

Lecture Notes in Computer Science

852

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

Advisory Board: W. Brauer D. Gries J. Stoer



Klaus Echte Dieter Hammer
David Powell (Eds.)

Dependable Computing – EDCC-1

First European Dependable Computing Conference
Berlin, Germany, October 4-6, 1994
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos

Universität Karlsruhe

Postfach 69 80, Vincenz-Priessnitz-Straße 1, D-76131 Karlsruhe, Germany

Juris Hartmanis

Department of Computer Science, Cornell University

4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen

Department of Computer Science, Utrecht University

Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editors

Klaus Echtle

Fachbereich Informatik

Universität Dortmund, Lehrstuhl IV

D-44221 Dortmund, Germany

Dieter Hammer

Humboldt-Universität zu Berlin

Fachbereich Informatik

D-10119 Berlin, Germany

David Powell

LAAS-CNRS

7 avenue du Colonel Roche, F-31077 Toulouse, France

CR Subject Classification (1991): B.1.3, B.2.3, B.3.4, B.4.5, C.3-4, D.2.4, D.2.8, D.4.5, E.4, J.7

ISBN 3-540-58426-9 Springer-Verlag Berlin Heidelberg New York

CIP data applied for

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 1994

Printed in Germany

Typesetting: Camera-ready by author

SPIN: 10478938

45/3140-543210 - Printed on acid-free paper

Foreword

The "First European Dependable Computing Conference" is both the start of a new European forum for dependable computing and the continuation of two former conference series – the "International Conference on Fault Tolerant Computing Systems" held in the Federal Republic of Germany until 1991 and the "International Conference on Fault-Tolerant Systems and Diagnostics" held in the countries of Eastern Europe until 1990.

Hardware and software reliability, safety and security, fault detection and tolerance, verification and validation are challenges newly arising for every computing system generation where high dependability requirements must be met in a practical and efficient way. Theoretical and experimental research form the scientific background to enable safety-critical applications.

The new series "European Dependable Computing Conference", EDCC will become a meeting point and enforce the exchange of ideas, models, designs and results from all over the world in a place where considerable contributions have been made. European industry spans the scope from highly available transaction processing applications to safety-critical areas such as railway signalling and aircraft control.

The work on dependability improvement is supported by interest groups in various European countries. They agreed to set up EDCC as their new common platform. The unification of their previous activities also reflects the political opening, which offers promising prospects to the scientific community. We wish all the best to the free cooperation among researchers and developers. It will certainly ease and promote their efforts.

The East West unification character of this conference is underlined by selecting Berlin as the location of the very first event, and by the composition of the program committee, the external referees, the session chairs – and the two co-chairs of EDCC-1 as well.

The conference would not be possible without the substantial contributions of many persons. First of all we express our thanks to the program committee, which performed excellent work under the chair of David Powell. By the willing help of the external referees an outstanding selection of papers was achieved. Our thanks is also directed to Erik Maehle who mainly contributed to EDCC's publicity and made it a well-known event.

The conference organisation was supported by the German interest group "Fault-Tolerant Computing Systems" and its chairman Ernst Schmitter, by LAAS-CNRS in Toulouse, and staff at University of Dortmund, Humboldt University of Berlin,

University of Paderborn, and Technical University of Cottbus. All their help is gratefully acknowledged.

We also express our thanks to Springer-Verlag for publishing the conference proceedings in the well-known series "Lecture Notes in Computer Science", and the Informationstechnische Gesellschaft ITG for arranging this conference.

We hope that EDCC-1 will be a successful start of the new conference series and that the participants will find its technical contribution interesting. We also hope that everyone enjoys the stay in Berlin.

July 1994

Klaus Echte, Dieter Hammer
Co-Chairs

Preface

Europe has been evolving quickly as we approach the end of the second millennium. In the 1980s, the advent of the European Community funding of technical research and development was a key factor in the creation of an international Western European Scientific Community, in particular in the field of computer science, thanks to the ESPRIT program. Now, in the 1990s, Europe is on the move again on a wider scale and our Community can grow further. This first European Dependable Computing Conference unites and expands two earlier series of conferences that were held in our formerly divided continent. It seems most fitting that Berlin should host this first united European conference and it has been my very great honour to chair its program committee.

Since this is the first conference of its sort, a major concern was to set high standards regarding both international representation on the program committee and the rigour of the paper selection process. A 30-strong committee was set up with representatives from 16 different European countries. Furthermore, to encourage submissions from outside Europe, two international liaison chairs kindly agreed to assist us. The committee was also ably assisted by 228 external referees from 23 different countries.

Overall, 106 papers were submitted from 29 countries. For each paper, 3 committee members were asked to nominate 1 committee member referee and 2 external referees. With this data, each paper was finally allocated 2 committee member referees and 3 external referees. Assigning referees in this way gave very positive results since the rate of return of completed reviews was extremely good. Overall, 530 manuscripts and review forms were sent out and 472 completed reviews were returned (89%). Most papers (91.5%) received 4 or more reviews and all papers were reviewed by at least 3 referees.

The program committee met on April 11-13, 1994 at LAAS-CNRS, Toulouse, to select those papers that were judged to be of a sufficiently high standard to be presented at the conference and to be included in the proceedings. Of the 106 papers submitted, 24 met the committee's stringent requirements and were thus accepted outright. Another 10 papers were accepted on the condition that the authors carry out the modifications requested by the referees. These papers were re-checked before final acceptance. In all, 34 papers out of 106 were finally accepted, with authors from 13 different countries.

The selected papers cover many different areas of dependable computing, including fault avoidance and fault tolerance techniques, in both hardware and software, for dealing with a wide class of faults: physical faults, design faults, intrusions,... There

are also many interesting papers that deal with fault removal and fault forecasting aspects for validating dependable systems through testing and evaluation.

The technical program at the conference has been purposely organized in a single track so that attendees will have the opportunity to apprehend the basic concepts of dependability that are applicable over a wide range of viewpoints. Maybe the resulting cross-fertilization of ideas will provide inspiration for future research? I hope so.

I also hope that this first EDCC has laid firm foundations for a regular series of high-standard conferences that will periodically provide a respected European venue for researchers worldwide to present and discuss their results.

July 1994

David Powell
Program Chair

Organization Committee

Co-Chairs

Klaus Echtle
University of Dortmund
Germany

Dieter Hammer
WIP Berlin
Germany

Program Chair

David Powell
LAAS-CNRS, Toulouse
France

Publicity Chair

Erik Maehle
University of Paderborn
Germany

Finance Chair

Volker Schanz
ITG-VDE, Frankfurt
Germany

International Liaison Chairs

North America:
Jacob Abraham
University of Texas, Austin
USA

Asia:
Yoshiro Tohma
Tokyo Denki University
Japan

Program Committee

A. Avizienis (Lithuania)
D. Avresky (Bulgaria)
O. Babaoglu (Italy)
A. Costes (France)
P. J. Courtois (Belgium)
M. Dal Cin (Germany)
Y. Deswarte (France)
W. Görke (Germany)
B. Helvik (Norway)
J. Hlavicka (Czech Republic)
A. Hlawiczka (Poland)
H. Kirmann (Switzerland)
H. Kopetz (Austria)
C. Landrault (France)
J. C. Laprie (France)

J. McDermid (United Kingdom)
J. Nordahl (Denmark)
A. Pfitzmann (Germany)
J. J. Quisquater (Belgium)
B. Randell (United Kingdom)
E. Schmitter (Germany)
J. Silva (Portugal)
L. Simoncini (Italy)
B. Straube (Germany)
J. Sziray (Hungary)
J. Torin (Sweden)
R. Ubar (Estonia)
P. Verissimo (Portugal)
J. Vytopil (Netherlands)

External Referees

E. J. Aas	R. Cooper	K. Goseva-Popstojanova
L. Alvisi	D. Crestani	M. Gössel
T. Anderson	F. Cuppens	E. Gramatová
R. Anderson	R. Cuyvers	F. Grandoni
J. Arlat	B. d'Ausbourg	K. Großpietsch
P. Azéma	A. Dahbura	G. Grünsteidl
L. F. Bacellar	G. Dahll	H. Guillermain
K. Badzmirowksi	J. Devooght	K.M. Hansen
F. Balbach	F. Di Giandomenico	L. Heerink
G. Balbo	B. Dimke	K. D. Heidtmann
A. Balivada	A. Domenici	S. Hellebrand
M. Banâtre	L. Donatiello	M. Hildebrand
P. Banerjee	V. Dràbek	M. Hiltunen
H. Beilner	H. Dücker	W. Hohl
F. Belli	C. Dufaza	J. Hooman
T. Bemmerl	W. Dulz	G. Horvath
C. Bernardeschi	H. Edler	K. A. Iyoudou
Y. Bertrand	G. Eizenberg	J. Jacob
J. Biskup	R. Ernst	J. Jacobson
J. P. Blanquart	B. Eschermann	E. Jonsson
A. Bobbio	A. Fantechi	G. Juanole
A. Bode	G. Färber	M. Kaâniche
A. Boehm	B. Ferruccio	Y. Kakuda
A. Bondavalli	S. Fischer-Hübner	Z. Kalbarczyk
L. Breveglieri	G. Fohler	A. Kalendarev
E. Brinksma	D. Forslund	G. Kanawati
J. Bruck	P. Frankl	K. Kanoun
H. H. Brüggemann	K. Fuchs	H. Kantz
S. Budkowski	E. Fuchs	A. Kaposi
A. Burns	R. Gantenbein	J. Karlsson
L. Cacciari	W. Geisselhardt	J. P. Kelly
A. Canning	J. Gentina	P. Keresztes
J. Carrasco	J. Gerardin	K. Kim
S. Chabridon	R. Gerlich	Y. S. Kim
A. Ciuffoletti	P. Girard	Y. Koga
A. Clematis	M. Girault	M. Kotocová
J. Coenen	J. Goldberg	C. Koza

A. Krasniewski	O. Novàk	J. Sifakis
H. Krawczyk	J. O'Connell	L. M. Silva
U. Krieger	C. O'Halloran	A. Skavhaug
T. Krol	P. Olivo	P. Slaba
H. Krumm	A. Pataricza	J. Sosnowski
M. Labarrère	S. Perl	N. Speirs
X. Lai	B. Pfitzmann	T. Stålhane
J. Lala	A. Pluhàcek	F. Stanischewski
G. Leber	P. Poechmueller	F. Stassen
P. Lee	I. Pomeranz	A. Steininger
R. Lepold	D. K. Pradhan	A. Stopp
R. Leveugle	S. Pravossoudovitch	L. Strigini
B. Littlewood	P. Puschner	M. Svěda
D. Logothetis	A. P. Ravn	A. Szegi
T. Lovric	M. Raynal	S. Tao
T. Lunt	J. Richier	P. Thévenod
C. Macnish	A. Robinson	K. Tilly
H. Madeira	L. Rodrigues	J. Toetenel
E. Maehle	A. Romanovsky	S. Tritsolev
P. Maestrini	R. A. Rueppel	K. Trivedi
V. Mainkar	J. Rushby	G. Tsudik
N. Malvache	J. Rutkowski	P. D. V. van der Stok
R. Marie	H. Rzehak	M. Vanneschi
R. Maxion	F. Saglietti	H. Vanthiena
C. Meadows	J. Santucci	H. Veit
S. Metge	K. Sapiecha	H. T. Vierhaus
J. F. Meyer	G. Saucier	C. Viho
F. Meyer	A. Schedl	U. Voges
S. Miller	H. Schepers	A. Vrchoticky
M. Millinque	A. Schiper	H. Waeselynck
I. Mitrani	R. Schlatterbeck	M. Waidner
M. Morganti	R. Schlichting	A. Wellings
C. Morin	W. G. Schneeweiß	H. Wunderlich
G. Muller	W. Seidel	J. Xu
R. Needham	E. Selényi	V. Yodaiken
R. Negrini	N. S. Sendrier	L. T. Young
J. Nehmer	B. Sericola	H. Zhu
M. Nicolaïdis	E. Shokri	C. Ziegler
H. Niederreitter	D. P. Siewiorek	J. Zwiers

Table of Contents

Session 1: Fault-Tolerance Techniques	1
<i>Chair: Winfried Görke, University of Karlsruhe, Germany</i>	
A Model for Adaptive Fault-Tolerant Systems	3
<i>M. A. Hiltunen, R. D. Schlichting (University of Arizona, Tucson, USA)</i>	
Designing Secure and Reliable Applications using Fragmentation- Redundancy-Scattering: An Object-Oriented Approach.....	21
<i>J.-C. Fabre, Y. Deswartes (LAAS-CNRS, Toulouse, France), B. Randell (University of Newcastle-upon-Tyne, United Kingdom)</i>	
A Fault-Tolerant Mechanism for Simple Controllers	39
<i>J. G. Silva, L. M. Silva, H. Madeira, J. Bernardino (University of Coimbra, Portugal)</i>	
Session 2: Formal Methods	57
<i>Chair: John McDermit, University of York, United Kingdom</i>	
Formal Semantics for Ward & Mellor's Transformation Schemas and the Specification of Fault-Tolerant Systems.....	59
<i>C. Petersohn, W.-P. de Roever (Christian-Albrechts-University of Kiel, Germany), C. Huizing (Eindhoven University of Technology, The Netherlands), J. Peleska (DST GmbH, Kiel, Germany)</i>	
Formal Reasoning on Fault Coverage of Fault Tolerant Techniques: a Case Study	77
<i>C. Bernardeschi, A. Fantechi, L. Simoncini (University of Pisa, Italy)</i>	
Session 3: Evaluation	95
<i>Chair: Bjarne Helvik, DELAB, Trondheim, Norway</i>	
On Performability Modeling and Evaluation of Software Fault Tolerance Structures.....	97
<i>S. Chiaradonna, A. Bondavalli (CNUCE/CNR, Pisa, Italy), L. Strigini (IEI/CNR, Pisa, Italy)</i>	
Optimal Design of Fault-Tolerant Soft-Real-Time Systems with Imprecise Computations.....	115
<i>C. Antonelli (Tor Vergata University of Rome, Italy), V. Grassi (University of Perugia, Italy)</i>	

Computational Restrictions for SPN with Generally Distributed Transition Times.....	131
<i>A. Bobbio (University of Brescia, Italy), M. Telek (Technical University of Budapest, Hungary)</i>	
Session 4: Hardware Testing	149
<i>Chair: Bernd Straube, Fraunhofer – EAS, Dresden, Germany</i>	
Test Generation for Digital Systems Based on Alternative Graphs	151
<i>R. Ubar (Technical University of Tallinn, Estonia)</i>	
The Configuration Ratio: A Model for Simulating CMOS Intra-Gate Bridge with Variable Logic Thresholds.....	165
<i>M. Renovell, P. Huc, Y. Bertrand (University of Montpellier II, France)</i>	
Coverage of Delay Faults: When 13% and 99% Mean the Same	178
<i>A. Krásniewski, L. B. Wroński (Warsaw University of Technology, Poland)</i>	
Session 5: Fault Injection	197
<i>Chair: Jean Arlat, LAAS-CNRS, Toulouse, France</i>	
RIFLE: A General Purpose Pin-level Fault Injector.....	199
<i>H. Madeira, M. Rela, F. Moreira, J. G. Silva (University of Coimbra, Portugal)</i>	
On Single Event Upset Error Manifestation.....	217
<i>R. Johansson (Chalmers University of Technology, Göteborg, Sweden)</i>	
Session 6: Software Testing	233
<i>Chair: Pierre-Jacques Courtois, AIB-Vincotte Nuclear, Brussels, Belgium</i>	
Injecting Faults into Environment Simulators for Testing Safety Critical Software.....	235
<i>H. Zhu, P. A. V. Hall, J. H. R. May (The Open University, Milton Keynes, United Kingdom), T. Cockram (Rolls Royce plc., United Kingdom)</i>	
On Statistical Structural Testing of Synchronous Data Flow Programs.....	250
<i>P. Thévenod-Fosse, C. Mazuet, Y. Crouzet (LAAS-CNRS, Toulouse, France)</i>	
Session 7: Built-In Self Test	269
<i>Chair: Andrzej Hlawiczka, Technical University of Gliwice, Poland</i>	
Hierarchical Test Analysis of VLSI Circuits for Random BIST.....	271
<i>G. Masseboeuf (Laboratoire d'Automatique de Grenoble, France), J. Pulou, J. L. Rainard (CNET, Meylan, France)</i>	
Zero Aliasing Compression Based on Groups of Weakly Independent Outputs in Circuits with High Complexity for Two Fault Models.....	289
<i>P. Böhlau (University of Potsdam, Germany)</i>	

Session 8: Software Diversity

307

*Chair: Hubert Kirmann, ASEA Brown Boveri AG, Baden-Dätwil,
Switzerland*

Systematic and Design Diversity – Software Techniques for Hardware Fault Detection.....	309
<i>T. Lovric (University of Dortmund, Germany)</i>	

Detection of Permanent Hardware Faults of a Floating Point Adder by Pseudoduplication.....	327
<i>S. Gerber, M. Gössel (University of Potsdam, Germany)</i>	

MLDD (Multi-Layered Design Diversity) Architecture for Achieving High Design Fault Tolerance Capabilities.....	336
<i>A. Watanabe, K. Sakamura (University of Tokyo, Japan)</i>	

Session 9: Parallel Systems

351

Chair: Paulo Veríssimo, INESC, Lisbon, Portugal

Reconfiguration and Checkpointing in Massively Parallel Systems.....	353
<i>B. Bieker, E. Maehle (University of Paderborn, Germany), G. Deconinck, J. Vounckx (Catholic University of Leuven, Belgium)</i>	

An Approach for Hierarchical System Level Diagnosis of Massively Parallel Computers Combined with a Simulation-Based Method for Dependability Analysis.....	371
<i>J. Altmann, F. Balbach, A. Hein (University of Erlangen-Nürnberg, Germany)</i>	

Hierarchical Checking of Multiprocessors Using Watchdog Processors.....	386
<i>I. Majzik, A. Pataricza (Technical University of Budapest, Hungary), M. Dal Cin, W. Hohl, J. Hönig, V. Sieh (University of Erlangen-Nürnberg, Germany)</i>	

Panel Discussion: Future Directions in Dependable Computing

405

Moderator: Jean-Claude Laprie, LAAS-CNRS, Toulouse, France

Dependability: The Challenge for the Future of Computing and Communication Technologies.....	407
<i>J.-C. Laprie (LAAS-CNRS, Toulouse, France)</i>	

Position Paper.....	409
<i>A. Avizienis (University of California, Los Angeles, USA)</i>	

Position Paper.....	411
<i>J. Hlavicka (Czech Technical University, Prague, Czech Republic)</i>	

Position Paper.....	412
<i>M. Morganti (ITALTEL Central Research Labs, Milano, Italy)</i>	

Some Lessons from the SW2000 Workshop.....	414
<i>B. Randell (University of Newcastle-upon-Tyne, United Kingdom)</i>	
Dependable Computing and its Industrial Use.....	417
<i>E. Schmitter (Siemens AG, Munich, Germany)</i>	
Session 10: Fault Tolerance in VLSI	419
<i>Chair: József Sziray, Computer Research and Innovation Center, Budapest, Hungary</i>	
An Effective Reconfiguration Process for Fault-Tolerant VLSI/WSI Array Processors.....	421
<i>Y.-Y. Chen, C.-H. Cheng, Y.-C. Chou (Chung-Hua Polytechnic Institute Hsin-Chu, Taiwan)</i>	
Concurrent Error Detection in Fast FNT Networks	439
<i>J. M. Tahir, S. S. Dlay, R. N. Gorgui-Naguib, O. R. Hinton (University of Newcastle-upon-Tyne, United Kingdom)</i>	
Feasible Regions Quantify the Configuration Power of Arrays with Multiple Fault Types.....	453
<i>L. E. LaForge (University of Nevada, Reno, USA)</i>	
Session 11: Measurement	471
<i>Chair: Taschko Nikolov, Technical University of Sofia, Bulgaria</i>	
Software Reliability Analysis of Three Successive Generations of a Switching System.....	473
<i>M. Kaâniche, K. Kanoun, M. Cukier (LAAS-CNRS, Toulouse, France), M. Bastos Martini (CpQD-Telebras, Brazil)</i>	
Performance of Consistent Checkpointing in a Modular Operating System: Results of the FTM Experiment	491
<i>G. Muller (IRISA/INRIA, Rennes, France), M. Hue, N. Peyrouze (Bull Research, France)</i>	
Session 12: Switching Networks and Hypercubes	509
<i>Chair: K. Iyoudou, Moscow Aviation Institute, Russia</i>	
Ring-Banyan Network: A Fault Tolerant Multistage Interconnection Network and its Fault Diagnosis	511
<i>J.-H. Park, H.-K. Lee (Korea Advanced Institute of Science and Technology, Taejon, Korea), J.-H. Cho (Electronics and Telecommunications Research Institute, Taejon, Korea)</i>	
Reconfiguration of Faulty Hypercubes	529
<i>D. R. Avresky, K. M. Al-Tawil (Texas A&M University, College Station, Texas)</i>	

Fault-Tolerance on Boolean n-Cube Architectures	546
<i>C.-S. Yang (National Sun Yat-Sen University, Kaohsiung, Taiwan),</i>	
<i>S.-Y. Wu (Chinese Military Academy, Kaohsiung, Taiwan)</i>	
Session 13: Distributed Systems	561
<i>Chair: Jan Torin, Chalmers University of Technology, Göteborg, Sweden</i>	
Relative Signatures for Fault Tolerance and their Implementation.....	563
<i>M. Leu (University of Dortmund, Germany)</i>	
GATOSTAR: A Fault Tolerant Load Sharing Facility for Parallel Applications.....	581
<i>B. Folliot, P. Sens (MASI Laboratory, Paris, France)</i>	
A Hierarchical Membership Protocol for Synchronous Distributed Systems.....	599
<i>P. D. V. van der Stok, M. M. M. P. J. Claessen, D. Alstein</i>	
<i>(Eindhoven University of Technology, The Netherlands)</i>	
Author Index	617