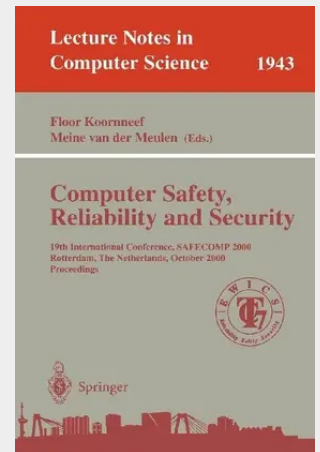


Computer Safety, Reliability, and Security

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

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 among 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. VI Preface 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 Kaaniche, Jean-Claude Laprie and Jean-Paul Blanquart VIII Table of Contents 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 M'ehaut and Pierre Mor`ere A Safety Licensable PES for SIL4 Applications. 141 Wolfgang A. Halang, Peter Vogrin and Matja`z Colnari`c Safety and Security Issues in Electric Power Industry. 151 ? Zdzislaw Zurkowski Dependability of Computer Control Systems in Power Plants. 165 Cl´audia Almeida, Alberto Arazo, Yves Crouzet and Karama Kanoun A Method of Analysis of Fault Trees with Time Dependencies. 176 Jan Magott and Paweł Skrobaneck 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 Problems in Education. 198 Thierry Scheurer Formal Methods Discussion: Past Lessons and Future Prospects. 211 R. Bloomfield, D. Craigen, F. Koob, M. Ullmann and S. Wittmann Invited Paper SafeTech: 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 Table of Contents IX Hardware Aspects An Approach to Software Assisted Recovery



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540411864
Medium: Buch
ISBN: 978-3-540-41186-4
Verlag: Springer
Erscheinungstermin: 11.10.2000
Sprache(n): Englisch
Auflage: 2000
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1380 g
Seiten: 438
Format (B x H): 155 x 235 mm

