

Janusz Górski (Ed.)

LNCS 4166

Computer Safety, Reliability, and Security

25th International Conference, SAFECOMP 2006
Gdansk, Poland, September 2006
Proceedings



Springer

Janusz Górski (Ed.)

Computer Safety, Reliability, and Security

25th International Conference, SAFECOMP 2006
Gdansk, Poland, September 27-29, 2006
Proceedings

 Springer

Volume Editor

Janusz Górski
Gdansk University of Technology
Department of Software Engineering
ul. Narutowicza 11/12, 80-952 Gdansk, Poland
E-mail: jango@pg.gda.pl

Library of Congress Control Number: 2006932795

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-45762-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-45762-6 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11875567 06/3142 5 4 3 2 1 0

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Preface

Welcome to SAFECOMP 2006, the 25th International Conference on Computer Safety, Security and Reliability, held in Gdansk, Poland. Since it was established in 1979 by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Safety, Reliability and Security (EWICS TC7), SAFECOMP has continuously contributed to the progress in high integrity applications of information technologies. The conference focuses on the state of the art, experience and new trends in the areas of safety, security and reliability of critical IT systems and applications and serves as a platform for knowledge and technology transfer for researchers, industry (suppliers, operators, users), regulators and certifiers of such systems. SAFECOMP provides ample opportunity to exchange insights and experiences on emerging methods, approaches and practical solutions to safety, security and reliability problems across the borders of different application domains and technologies.

The SAFECOMP 2006 program reflected in this book included 32 papers selected from 101 submissions of full texts. The submissions came from authors representing 26 different countries from Europe, Asia, and North and South America. The 32 accepted papers were prepared by experts representing 14 different countries. The above data confirm the broad and increasing interest in SAFECOMP and the topics addressed.

The program was supplemented by three keynote presentations by outstanding invited experts (not included in this book). The keynotes focused on interdisciplinary aspects of dependability of computer systems, practical aspects of application of safety standards and new challenges of information security research and development.

Preparation of the SAFECOMP 2006 program was a long and intensive process. Its success is the result of the hard work, involvement and support of the International Program Committee, the external reviewers, the keynote speakers, and most of all, the authors who submitted numerous excellent contributions. Selecting from them was by no means an easy task and in many cases some very good papers could not be accepted because of the program constraints.

I would like to thank all those who contributed to the preparation of the SAFECOMP 2006 program for their competence, dedication and sustainable support. I would also like to thank my colleagues from the Information Assurance Group of the Department of Software Engineering of Gdansk University of Technology for their organizational support. Special thanks are due to the National Organizing Committee, for its involvement in the preparation of the conference.

The next conference, SAFECOMP 2007, will take place in Nuremberg, Germany, and in the name of the organizers I am extending to you the invitation to

contribute to and attend this important event in the field of Computer Safety, Reliability and Security.

July 2006

Janusz Górski

Organization

Program Chair

Janusz Górski, Poland

EWICS Chair

Udo Voges, Germany

Organizing Committee

Janusz Górski (Co-chair)
Aleksander Jarzębowski (Co-chair)
Janusz Czaja
Grzegorz Gołaszewski
Alfreda Kortas
Jakub Miler
Marcin Olszewski

International Program Committee

Stuart Anderson, UK	Connie Heitmeyer, USA
Ramesh Bharadwaj, USA	Ming-Yuh Huang, USA
Andrzej Białas, Poland	Chris Johnson, UK
Robin Bloomfield, UK	Mohamed Kaâniche, France
Sandro Bologna, Italy	Karama Kanoun, France
Andrea Bondavalli, Italy	Floor Koornneef, Netherlands
Bettina Buth, Germany	Peter Ladkin, Germany
Tadeusz Cichocki, Poland	Jan Magott, Poland
Peter Daniel, UK	Marcelo Masera, Italy
Erland Jonsson, Sweden	Meine van der Meulen, UK
Wolfgang Ehrenberger, Germany	Odd Nordland, Norway
Massimo Felici, UK	Simone Pozzi, Italy
Robert Genser, Austria	Gerd Rabe, Germany
Chris Goring, UK	Felix Redmill, UK
Bjørn Axel Gran, Norway	Krzysztof Sacha, Poland
Wolfgang Grieskamp, USA	Francesca Saglietti, Germany
Wolfgang Halang, Germany	Erwin Schoitsch, Austria
Monika Heiner, Germany	Nicolas Sklavos, Greece
Maritta Heisel, Germany	Jeanine Souquières, France

VIII Organization

Werner Stephan, Germany
Mark Sujan, UK
Atoosa P.-J. Thunem, Norway
Jos Trienekens, Netherlands
Adolfo Villafiorita, Italy
Udo Voges, Germany
Andrzej Wardziński, Poland

Albrecht Weinert, Germany
Marc Wilikens, Italy
Rune Winther, Norway
Stefan Wittmann, Belgium
Eric Wong, USA
Zdzisław Żurkowski, Poland

External Reviewers

Lei Bu
Lassaad Cheikhrouhou
Silvano Chiaradonna
Sergio Contini
Lorenzo Falai
Igor Nai Fovino
Felicita Di Giandomenico
Jeremie Guiochet
Paweł Głuchowski
Tom Heijer
Hai Hu
Martin Gilje Jaatun
Bin Lei
Paolo Lollini

Thea Peacock
Yu Qi
Georg Rock
Marco Roveri
Peter Ryan
Holger Schmidt
Martin Skambraks
Paweł Skrobanek
Alberto Stefanini
Avinanta Tarigan
Roberto Tiella
I. Made Wiryana
Wei Zhang

Sponsoring Organizations

Organizing Institutions



Scientific Sponsors



Industrial Sponsors



Lecture Notes in Computer Science

For information about Vols. 1–4116

please contact your bookseller or Springer

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), *Modular Programming Languages*. X, 415 pages. 2006.

Vol. 4224: E. Corchado, H. Yin, V. Botti, C. Fyfe (Eds.), *Intelligent, Data Engineering and Automated Learning – IDEAL 2006*. XXVII, 1447 pages. 2006.

Vol. 4219: D. Zamboni, C. Kruegel (Eds.), *Recent Advances in Intrusion Detection*. XII, 331 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), *Personal Wireless Communications*. XV, 532 pages. 2006.

Vol. 4213: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), *Knowledge Discovery in Databases: PKDD 2006*. XXII, 660 pages. 2006. (Sublibrary LNAI).

Vol. 4212: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), *Machine Learning: ECML 2006*. XXIII, 851 pages. 2006. (Sublibrary LNAI).

Vol. 4208: M. Gerndt, D. Kranzlmüller (Eds.), *High Performance Computing and Communications*. XXII, 938 pages. 2006.

Vol. 4207: Z. Ésik (Ed.), *Computer Science Logic*. XII, 627 pages. 2006.

Vol. 4206: P. Dourish, A. Friday (Eds.), *UbiComp 2006: Ubiquitous Computing*. XIX, 526 pages. 2006.

Vol. 4205: G. Bourque, N. El-Mabrouk (Eds.), *Comparative Genomics*. X, 231 pages. 2006. (Sublibrary LNBI).

Vol. 4203: F. Esposito, Z.W. Ras, D. Malerba, G. Semeraro (Eds.), *Foundations of Intelligent Systems*. XVIII, 767 pages. 2006. (Sublibrary LNAI).

Vol. 4202: E. Asarin, P. Bouyer (Eds.), *Formal Modeling and Analysis of Timed Systems*. XI, 369 pages. 2006.

Vol. 4201: Y. Sakakibara, S. Kobayashi, K. Sato, T. Nishino, E. Tomita (Eds.), *Grammatical Inference: Algorithms and Applications*. XII, 359 pages. 2006. (Sublibrary LNAI).

Vol. 4197: M. Raubal, H.J. Miller, A.U. Frank, M.F. Goodchild (Eds.), *Geographic, Information Science*. XIII, 419 pages. 2006.

Vol. 4196: K. Fischer, E. André, I.J. Timm, N. Zhong (Eds.), *Multiagent System Technologies*. X, 185 pages. 2006. (Sublibrary LNAI).

Vol. 4194: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), *Computer Algebra in Scientific Computing*. XI, 313 pages. 2006.

Vol. 4193: T.P. Runarsson, H.-G. Beyer, E. Burke, J.J. Merelo-Guervós, L. D. Whitley, X. Yao (Eds.), *Parallel Problem Solving from Nature - PPSN IX*. XIX, 1061 pages. 2006.

Vol. 4192: B. Mohr, J.L. Träff, J. Worringer, J. Dongarra (Eds.), *Recent Advances in Parallel Virtual Machine and Message Passing Interface*. XVI, 414 pages. 2006.

Vol. 4191: R. Larsen, M. Nielsen, J. Sparring (Eds.), *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2006, Part II*. XXXVIII, 981 pages. 2006.

Vol. 4190: R. Larsen, M. Nielsen, J. Sparring (Eds.), *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2006, Part I*. XXXVIII, 949 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), *Computer Security – ESORICS 2006*. XI, 548 pages. 2006.

Vol. 4188: P. Sojka, I. Kopeček, K. Pala (Eds.), *Text, Speech and Dialogue*. XIV, 721 pages. 2006. (Sublibrary LNAI).

Vol. 4187: J.J. Alferes, J. Bailey, W. May, U. Schwertel (Eds.), *Principles and Practice of Semantic Web Reasoning*. XI, 277 pages. 2006.

Vol. 4186: C. Jesshope, C. Egan (Eds.), *Advances in Computer Systems Architecture*. XIV, 605 pages. 2006.

Vol. 4185: R. Mizoguchi, Z. Shi, F. Giunchiglia (Eds.), *The Semantic Web – ASWC 2006*. XX, 778 pages. 2006.

Vol. 4184: M. Bravetti, M. Núñez, G. Zavattaro (Eds.), *Web Services and Formal Methods*. X, 289 pages. 2006.

Vol. 4183: J. Euzenat, J. Domingue (Eds.), *Artificial Intelligence: Methodology, Systems, and Applications*. XIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 4182: H.T. Ng, M.-K. Leong, M.-Y. Kan, D. Ji (Eds.), *Information Retrieval Technology*. XVI, 684 pages. 2006.

Vol. 4180: M. Kohlhase, *OMDoc – An Open Markup Format for Mathematical Documents [version 1.2]*. XIX, 428 pages. 2006. (Sublibrary LNAI).

Vol. 4179: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), *Advanced Concepts for Intelligent Vision Systems*. XXIV, 1224 pages. 2006.

Vol. 4178: A. Corradini, H. Ehrig, U. Montanari, L. Ribeiro, G. Rozenberg (Eds.), *Graph Transformations*. XII, 473 pages. 2006.

Vol. 4176: S.K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, B. Preneel (Eds.), *Information Security*. XIV, 548 pages. 2006.

Vol. 4175: P. Bücher, B.M.E. Moret (Eds.), *Algorithms in Bioinformatics*. XII, 402 pages. 2006. (Sublibrary LNBI).

Vol. 4174: K. Franke, K.-R. Müller, B. Nickolay, R. Schäfer (Eds.), *Pattern Recognition*. XX, 773 pages. 2006.

Vol. 4173: S. El Yacoubi, B. Chopard, S. Bandini (Eds.), *Cellular Automata*. XV, 734 pages. 2006.

- Vol. 4172: J. Gonzalo, C. Thanos, M. F. Verdejo, R.C. Carrasco (Eds.), *Research and Advanced Technology for Digital Libraries*. XVII, 569 pages. 2006.
- Vol. 4169: H.L. Bodlaender, M.A. Langston (Eds.), *Parameterized and Exact Computation*. XI, 279 pages. 2006.
- Vol. 4168: Y. Azar, T. Erlebach (Eds.), *Algorithms – ESA 2006*. XVIII, 843 pages. 2006.
- Vol. 4167: S. Dolev (Ed.), *Distributed Computing*. XV, 576 pages. 2006.
- Vol. 4166: J. Górski (Ed.), *Computer Safety, Reliability, and Security*. XIV, 440 pages. 2006.
- Vol. 4165: W. Jonker, M. Petković (Eds.), *Secure, Data Management*. X, 185 pages. 2006.
- Vol. 4163: H. Bersini, J. Carneiro (Eds.), *Artificial Immune Systems*. XII, 460 pages. 2006.
- Vol. 4162: R. Kráľovič, P. Urzyczyn (Eds.), *Mathematical Foundations of Computer Science 2006*. XV, 814 pages. 2006.
- Vol. 4161: R. Harper, M. Rauterberg, M. Combetto (Eds.), *Entertainment Computing - ICEC 2006*. XXVII, 417 pages. 2006.
- Vol. 4160: M. Fisher, W.v.d. Hoek, B. Konev, A. Lisitsa (Eds.), *Logics in Artificial Intelligence*. XII, 516 pages. 2006. (Sublibrary LNAI).
- Vol. 4159: J. Ma, H. Jin, L.T. Yang, J.J.-P. Tsai (Eds.), *Ubiquitous Intelligence and Computing*. XXII, 1190 pages. 2006.
- Vol. 4158: L.T. Yang, H. Jin, J. Ma, T. Ungerer (Eds.), *Autonomic and Trusted Computing*. XIV, 613 pages. 2006.
- Vol. 4156: S. Amer-Yahia, Z. Bellahsene, E. Hunt, R. Unland, J.X. Yu (Eds.), *Database and XML Technologies*. IX, 123 pages. 2006.
- Vol. 4155: O. Stock, M. Schaerf (Eds.), *Reasoning, Action and Interaction in AI Theories and Systems*. XVIII, 343 pages. 2006. (Sublibrary LNAI).
- Vol. 4154: Y.A. Dimitriadis, I. Zigurs, E. Gómez-Sánchez (Eds.), *Groupware: Design, Implementation, and Use*. XIV, 438 pages. 2006.
- Vol. 4153: N. Zheng, X. Jiang, X. Lan (Eds.), *Advances in Machine Vision, Image Processing, and Pattern Analysis*. XIII, 506 pages. 2006.
- Vol. 4152: Y. Manolopoulos, J. Pokorný, T. Sellis (Eds.), *Advances in Databases and Information Systems*. XV, 448 pages. 2006.
- Vol. 4151: A. Iglesias, N. Takayama (Eds.), *Mathematical Software - ICMS 2006*. XVII, 452 pages. 2006.
- Vol. 4150: M. Dorigo, L.M. Gambardella, M. Birattari, A. Martinoli, R. Poli, T. Stützle (Eds.), *Ant Colony Optimization and Swarm Intelligence*. XVI, 526 pages. 2006.
- Vol. 4149: M. Klusch, M. Rovatsos, T.R. Payne (Eds.), *Cooperative Information Agents X*. XII, 477 pages. 2006. (Sublibrary LNAI).
- Vol. 4148: J. Vounckx, N. Azemard, P. Maurine (Eds.), *Integrated Circuit and System Design*. XVI, 677 pages. 2006.
- Vol. 4146: J.C. Rajapakse, L. Wong, R. Acharya (Eds.), *Pattern Recognition in Bioinformatics*. XIV, 186 pages. 2006. (Sublibrary LNBI).
- Vol. 4144: T. Ball, R.B. Jones (Eds.), *Computer Aided Verification*. XV, 564 pages. 2006.
- Vol. 4142: A. Campilho, M. Kamel (Eds.), *Image Analysis and Recognition, Part II*. XXVII, 923 pages. 2006.
- Vol. 4141: A. Campilho, M. Kamel (Eds.), *Image Analysis and Recognition, Part I*. XXVIII, 939 pages. 2006.
- Vol. 4139: T. Salakoski, F. Ginter, S. Pyysalo, T. Pahikkala, *Advances in Natural Language Processing*. XVI, 771 pages. 2006. (Sublibrary LNAI).
- Vol. 4138: X. Cheng, W. Li, T. Znati (Eds.), *Wireless Algorithms, Systems, and Applications*. XVI, 709 pages. 2006.
- Vol. 4137: C. Baier, H. Hermanns (Eds.), *CONCUR 2006 – Concurrency Theory*. XIII, 525 pages. 2006.
- Vol. 4136: R.A. Schmidt (Ed.), *Relations and Kleene Algebra in Computer Science*. XI, 433 pages. 2006.
- Vol. 4135: C.S. Calude, M.J. Dinneen, G. Păun, G. Rozenberg, S. Stepney (Eds.), *Unconventional Computation*. X, 267 pages. 2006.
- Vol. 4134: K. Yi (Ed.), *Static Analysis*. XIII, 443 pages. 2006.
- Vol. 4133: J. Gratch, M. Young, R. Aylett, D. Ballin, P. Olivier (Eds.), *Intelligent Virtual Agents*. XIV, 472 pages. 2006. (Sublibrary LNAI).
- Vol. 4132: S. Kollias, A. Stafylopatis, W. Duch, E. Oja (Eds.), *Artificial Neural Networks – ICANN 2006, Part II*. XXXIV, 1028 pages. 2006.
- Vol. 4131: S. Kollias, A. Stafylopatis, W. Duch, E. Oja (Eds.), *Artificial Neural Networks – ICANN 2006, Part I*. XXXIV, 1008 pages. 2006.
- Vol. 4130: U. Furbach, N. Shankar (Eds.), *Automated Reasoning*. XV, 680 pages. 2006. (Sublibrary LNAI).
- Vol. 4129: D. McGookin, S. Brewster (Eds.), *Haptic and Audio Interaction Design*. XII, 167 pages. 2006.
- Vol. 4128: W.E. Nagel, W.V. Walter, W. Lehner (Eds.), *Euro-Par 2006 Parallel Processing*. XXXIII, 1221 pages. 2006.
- Vol. 4127: E. Damiani, P. Liu (Eds.), *Data and Applications Security XX*. X, 319 pages. 2006.
- Vol. 4126: P. Barahona, F. Bry, E. Franconi, N. Henze, U. Sattler, *Reasoning Web*. XII, 269 pages. 2006.
- Vol. 4124: H. de Meer, J.P. G. Sterbenz (Eds.), *Self-Organizing Systems*. XIV, 261 pages. 2006.
- Vol. 4121: A. Biere, C.P. Gomes (Eds.), *Theory and Applications of Satisfiability Testing - SAT 2006*. XII, 438 pages. 2006.
- Vol. 4120: J. Calmet, T. Ida, D. Wang (Eds.), *Artificial Intelligence and Symbolic Computation*. XIII, 269 pages. 2006. (Sublibrary LNAI).
- Vol. 4119: C. Dony, J.L. Knudsen, A. Romanovsky, A. Tripathi (Eds.), *Advanced Topics in Exception Handling Components*. X, 302 pages. 2006.
- Vol. 4117: C. Dwork (Ed.), *Advances in Cryptology - CRYPTO 2006*. XIII, 621 pages. 2006.

Table of Contents

Systems of Systems

System of Systems Hazard Analysis Using Simulation and Machine Learning	1
<i>Robert Alexander, Dimitar Kazakov, Tim Kelly</i>	
Through the Description of Attacks: A Multidimensional View	15
<i>Igor Nai Fovino, Marcelo Masera</i>	
On Certain Behavior of Scale-Free Networks Under Malicious Attacks	29
<i>Tomasz Gierszewski, Wojciech Molisz, Jacek Rak</i>	

Security and Survivability Analysis

Verifying a Chipcard-Based Biometric Identification Protocol in VSE	42
<i>Lassaad Cheikhrouhou, Georg Rock, Werner Stephan, Matthias Schwan, Gunter Lassmann</i>	
Exploring Resilience Towards Risks in eOperations in the Oil and Gas Industry	57
<i>Felicjan Rydzak, Lars S. Breistrand, Finn Olav Sveen, Ying Qian, Jose J. Gonzalez</i>	
Computer System Survivability Modelling by Using Stochastic Activity Network	71
<i>Eimantas Garsva</i>	

Nuclear Safety and Application of Standards

Software Safety Lifecycles and the Methods of a Programmable Electronic Safety System for a Nuclear Power Plant	85
<i>Jang-Soo Lee, Arndt Lindner, Jong-Gyun Choi, Horst Miedl, Kee-Choon Kwon</i>	
Regulatory Software Configuration Management System Design	99
<i>I-Hsin Chou, Chin-Feng Fan</i>	

Gaining Confidence in the Software Development Process Using Expert Systems 113
Mario Brito, John May

Formal Approaches

Retrenchment, and the Generation of Fault Trees for Static, Dynamic and Cyclic Systems 127
Richard Banach, Marco Bozzano

Stepwise Development of Secure Systems 142
Thomas Santen

Component-Based Hazard Analysis: Optimal Designs, Product Lines, and Online-Reconfiguration 156
Holger Giese, Matthias Tichy

Networks Dependability

New VoIP Traffic Security Scheme with Digital Watermarking 170
Wojciech Mazurczyk, Zbigniew Kotulski

Towards Filtering and Alerting Rule Rewriting on Single-Component Policies 182
Joaquín García-Alfaro, Frédéric Cuppens, Nora Cuppens-Bouahia

Using Group Overlapping to Protect Server from Attack in Grid Computing 195
Byungryong Kim

Coping with Change and Mobility

The Role of Situation Awareness in Assuring Safety of Autonomous Vehicles 205
Andrzej Wardziński

Demonstration of Safety in Healthcare Organisations 219
Mark-Alexander Sujan, Michael D. Harrison, Alison Steven, Pauline H. Pearson, Susan J. Vernon

Healthcare System Architecture, Economic Value, and Policy Models in Large-Scale Wireless Sensor Networks 233
Won Jay Song, Moon Kyo Cho, Im Sook Ha, Mun Kee Choi

Safety Analysis and Assessment

Assessment of Hazard Identification Methods for the Automotive Domain	247
<i>Fredrik Törner, Per Johannessen, Peter Öhman</i>	
A Tool for Databus Safety Analysis Using Fault Injection	261
<i>Dawid Trawczynski, Janusz Sosnowski, Janusz Zalewski</i>	
Towards a Unified Model-Based Safety Assessment	275
<i>Thomas Peikenkamp, Antonella Cavallo, Laura Valacca, Eckard Böde, Matthias Pretzer, E. Moritz Hahn</i>	

Poster Session

Reliability Analysis of Resilient Packet Rings	289
<i>Piotr Chotda, Jerzy Domżał, Andrzej Jajszczyk, Krzysztof Wajda</i>	
Experiences with the Design of a Run-Time Check	302
<i>Meine J.P. van der Meulen, Miguel A. Revilla</i>	
Development of an Integrated, Risk-Based Platform for Information and E-Services Security	316
<i>Andrzej Białas</i>	
Using Agent-Based Modelling Approaches to Support the Development of Safety Policy for Systems of Systems	330
<i>Martin Hall-May, Tim Kelly</i>	
Verification of Automatic Train Protection Systems with RTCP-Nets	344
<i>Marcin Szyrka, Tomasz Szmuc</i>	

6th FP Integrated Project DECOS

Checking SCADE Models for Correct Usage of Physical Units	358
<i>Rupert Schlick, Wolfgang Herzner, Thierry Le Sergent</i>	
Validation and Certification of Safety-Critical Embedded Systems - The DECOS Test Bench	372
<i>Erwin Schoitsch, Egbert Althammer, Henrik Eriksson, Jonny Vinter, Laszlo Gönczy, Andras Pataricza, György Csertan</i>	

Encapsulating Application Subsystems Using the DECOS Core OS 386
*Martin Schlager, Wolfgang Herzner, Andreas Wolf,
Oliver Gründonner, Maximilian Rosenblattl, Erwin Erkingner*

Modelling

Modeling the Railway Control Domain Rigorously with a
UML 2.0 Profile 398
Kirsten Berkenkötter, Ulrich Hannemann

Access Control Coherence of Information Systems Based on Security
Constraints 412
Aneta Poniszewska-Marańda

Automatic Test Data Generation by Multi-objective Optimisation 426
Norbert Oster, Francesca Saglietti

Author Index 439

System of Systems Hazard Analysis Using Simulation and Machine Learning

Robert Alexander, Dimitar Kazakov, and Tim Kelly

Department of Computer Science
University of York, York, YO10 5DD, UK

{robert.alexander, dimitar.kazakov, tim.kelly}@cs.york.ac.uk

Abstract. In the operation of safety-critical systems, the sequences by which failures can lead to accidents can be many and complex. This is particularly true for the emerging class of systems known as systems of systems, as they are composed of many distributed, heterogenous and autonomous components. Performing hazard analysis on such systems is challenging, in part because it is difficult to know in advance which of the many observable or measurable features of the system are important for maintaining system safety. Hence there is a need for effective techniques to find causal relationships within these systems. This paper explores the use of machine learning techniques to extract potential causal relationships from simulation models. This is illustrated with a case study of a military system of systems.

1 Introduction

Large-scale military and transport Systems of Systems (SoS) present many challenges for safety. The term ‘SoS’ is somewhat controversial — attempts at definitions can be found in [1] and [2]. It is easy, however, to identify uncontroversial examples, Air Traffic Control and Network Centric Warfare being the most prominent. These examples feature mobile components distributed over large areas, such as regions, counties or entire continents. Their components frequently interact with each other in an ad-hoc fashion, and have the potential to cause large-scale destruction and injury.

It follows that for SoS that are being designed and procured now, safety has a high priority. This is particularly true for SoS incorporating new kinds of autonomous component systems, such as Unmanned Aerial Vehicles (UAVs).

This paper is concerned with one aspect of the safety process for SoS, specifically hazard analysis. This is an important first step in any risk-based safety process. Unfortunately, performing hazard analysis on SoS is not easy. Quite apart from the novelty of these systems, and the commensurate lack of examples to work from, the characteristics of SoS raise serious difficulties. For example, ad hoc communications mean that information errors can propagate through the system by many, and unpredictable, routes.

The following section describes the problems faced in SoS hazard analysis, then section 3 proposes multi-agent simulation as a possible solution. An approach to performing hazard analysis, using simulation combined with machine learning, is outlined

in section 4, and the results of a case study are presented in section 5. Section 6 compares the work with existing applications of simulation in safety and section 7 discusses the issue of model fidelity.

2 The Problem of SoS Hazard Analysis

A definition of the term ‘SoS hazard’ was given by the authors in [3] as “*Condition of an SoS configuration, physical or otherwise, that can lead to an accident.*” It follows that SoS hazard analysis is the process of finding those conditions that can lead to accidents.

The problems faced by safety analysts when attempting to perform hazard analysis on SoS fall into two key categories: the immediate issue of failure effect propagation, and the more pernicious category of ‘System Accidents’. It has been noted by Kelly and Wilkinson, in [4], that these problems are present in conventional systems, too, but the characteristics of SoS exacerbate them.

2.1 Deriving the Effects of a Failure

In a conventional system, such as a single vehicle or a chemical plant, the system boundary is well-defined and the components within that boundary can be enumerated. When a safety analyst postulates some failure of a component, the effect of that failure can be propagated through the system to reveal whether or not the failure results in a hazard. This is not always easy, because of the complexity of possible interactions and variability of system state, hence the need for systematic analysis techniques, automated analysis tools, and system designs that minimise possible interactions. To make the task more tractable, most existing hazard analysis techniques (such as FFA and HAZOP) deal with only a single failure at a time; coincident failures are rarely considered.

In an SoS, this problem is considerably worse. The system boundary is not well defined, and the set of entities within that boundary can vary over time, either as part of normal operation (a new aircraft enters a controlled airspace region) or as part of evolutionary development (a military unit receives a new air-defence system). Conventional tactics to minimise interactions may be ineffective, because the system consists of component entities that are individually mobile. In some cases, particularly military systems, the entities may be designed (for performance purposes) to form ad-hoc groupings amongst themselves. Conventional techniques may be inadequate for determining whether or not some failure in some entity is hazardous in the context of the SoS as a whole.

2.2 System Accidents

Perrow, in [5], discusses what he calls ‘normal accidents’ in the context of complex systems. His ‘Normal Accident Theory’ holds that any complex, tightly-coupled system has the potential for catastrophic failure stemming from simultaneous minor failures. Similarly, Leveson, in [6] notes that many accidents have multiple necessary causes. In such cases it follows that an investigation of any one cause *prior to the accident* (i.e. without the benefit of hindsight) would not have shown the accident to be plausible.