Francesca Saglietti
Norbert Oster (Eds.)

LNCS 4680

Computer Safety, Reliability, and Security

26th International Conference, SAFECOMP 2007
Nuremberg, Germany, September 2007
Proceedings

Springer

Francesca Saglietti Norbert Oster (Eds.)

Computer Safety, Reliability, and Security

26th International Conference, SAFECOMP 2007
Nuremberg, Germany, September 18-21, 2007
Proceedings

Springer

Volume Editors

Francesca Saglietti
Department of Software Engineering
University of Erlangen-Nuremberg
Germany
E-mail: saglietti@informatik.uni-erlangen.de

Norbert Oster
Department of Software Engineering
University of Erlangen-Nuremberg
Germany
E-mail: oster@informatik.uni-erlangen.de

Library of Congress Control Number: 2007934754

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 3-540-75100-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75100-7 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12161898 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4680

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

Since 1979, when it was first established by the Technical Committee on Reliability, Safety and Security of the European Workshop on Industrial Computer Systems (EWICS TC7), the SAFECOMP Conference series has regularly and continuously contributed to improving the state of the art of highly dependable computer-based systems, since then increasingly applied to safety-relevant industrial domains.

In this expanding technical field SAFECOMP offers a platform for knowledge and technology transfer between academia, industry, research and licensing institutions, providing ample opportunities for exchanging insights, experiences and trends in the areas of safety, reliability and security regarding critical computer applications. In accordance with the growing spread of critical infrastructures involving both safety and security threats, this year's SAFECOMP program included a considerable number of contributions addressing technical problems and engineering solutions across the border between safety-related and security-related concerns.

The reaction to our call for papers was particularly gratifying and impressive, including 136 full papers submitted by authors representing 29 countries from Europe, Asia, North and South America as well as Australia. The selection of 33 full papers and 16 short papers for presentation and publication was a challenging task requiring a huge amount of reviewing and organizational effort. In view of the particularly high number of articles submitted, obvious practical constraints led – to our regret – to the rejection of a considerable amount of high-quality work. To all authors, invited speakers, members of the International Program Committee and external reviewers go our heartfelt thanks!

The local organization of SAFECOMP 2007, hosted in Nuremberg, is also gratefully acknowledged. The intensive preparatory activities demanded year-long dedication from the members of the Department of Software Engineering at the University of Erlangen-Nuremberg, which co-organized the event in co-operation with the German Computer Society (Gesellschaft für Informatik). Particular thanks are due to all colleagues and friends from the Organizing Committee, whose support we regard as crucial for the success of this conference.

We are confident that – when reading the present volume of the *Lecture Notes in Computer Science* – you will find its contents interesting enough to consider joining the SAFECOMP community. In the name of EWICS TC7 and of the future organizers we welcome you and invite you to attend future SAFECOMP conferences – among them SAFECOMP 2008 in Newcastle upon Tyne (UK) – and to contribute actively to their technical program.

July 2007

Francesca Saglietti
Norbert Oster

Organization

Program Chair

Francesca Saglietti (Germany)

EWICS Chair

Udo Voges (Germany)

International Program Committee

Stuart Anderson (UK)
Robin Bloomfield (UK)
Sandro Bologna (Italy)
Jens Braband (Germany)
Inga Bratteby-Ribbing (SE)
Bettina Buth (Germany)
Peter Daniel (UK)
Christian Diedrich (Germany)
Jana Dittmann (Germany)
Wolfgang Ehrenberger (Germany)
Massimo Felici (UK)
Robert Genser (Austria)
Bjorn Axel Gran (Norway)
Karl-Erwin Großpietsch (Germany)
Wolfgang Halang (Germany)
Monika Heiner (Germany)
Maritta Heisel (Germany)
Constance Heitmeyer (USA)
Janusz Gorski (Poland)
Karl-Heinz John (Germany)
Karama Kanoun (France)
Floor Koornneef (The Netherlands)
Peter B. Ladkin (Germany)
Søren Lindskov Hansen (Denmark)
Bev Littlewood (UK)
Vic Maggioli (USA)
Odd Nordland (Norway)
Gerd Rabe (Germany)
Felix Redmill (UK)
Martin Rothfelder (Germany)
Krzysztof Sacha (Poland)
Erwin Schoitsch (Austria)
Werner Stephan (Germany)
Mark Sujan (UK)
Pascal Traverse (France)
Jos Trienekens (The Netherlands)
Meine Van der Meulen
(The Netherlands)
Udo Voges (Germany)
Albrecht Weinert (Germany)
Rune Winther (Norway)
Stefan Wittmann (Belgium)
Zdzislaw Zurakowski (Poland)

Organizing Committee

Francesca Saglietti (Co-chair)
Wolfgang Ehrenberger (Co-chair)
Norbert Oster
Jutta Radke
Gerd Schober
Sven Söhnlein

External Reviewers

Myla Archer
Lassaad Cheikhrouhou
DeJiu Chen
Yves Crouzet
Håkan Edler
Jonas Elmqvist
Denis Hatebur
Tobias Hoppe
Ralph D. Jeffords
Björn Johansson
Johan Karlsson
Stefan Kiltz
Andreas Lang
Bruno Langenstein
Tiejun Ma
Oliver Meyer
M. Oliver Möller
Simin Nadjm-Tehrani
Vincent Nicomette
Andreas Nonnengart
Andrea Oermann
Ulf Olsson
Norbert Oster
Christian Raspotnig
Ronny Richter
Georg Rock
Jan Sanders
Thomas Santen
Tobias Scheidat
Holger Schmidt
Bernd Schomburg
Martin Schwarick
Dirk Seifert
Sven Söhnlein
Marc Spisländer
Mirco Tribastone
Arno Wacker
Dirk Wischermann

Scientific Sponsor

EWICS – European Workshop on Industrial Computer Systems
TC7 – Technical Committee on Reliability, Safety and Security

in collaboration with the following **Scientific Co-sponsors**:

IFAC
International Federation of Automatic Control

IFIP
International Federation for Information Processing

ENCRESS
European Network of Clubs for Reliability
and Safety of Software-Intensive Systems

SCSC
The Safety-Critical Systems Club

SRMC
The Software Reliability & Metrics Club

[redacted]

OCG
Austrian Computer Society

DECOS
Dependable Embedded Components and Systems

SAFECOMP 2007 Organizers

SWE
Department of Software Engineering
University of Erlangen-Nuremberg

GI
Gesellschaft für Informatik e.V.

Lecture Notes in Computer Science

Sublibrary 2: Programming and Software Engineering

For information about Vols. 1–4044
please contact your bookseller or Springer

Vol. 4749: B.J. Krämer, K.-J. Lin, P. Narasimhan (Eds.), Service-Oriented Computing – ICSOC 2007. XIX, 629 pages. 2007.

Vol. 4741: C. Bessiere (Ed.), Principles and Practice of Constraint Programming – CP 2007. XV, 890 pages. 2007.

Vol. 4680: F. Saglietti, N. Oster (Eds.), Computer Safety, Reliability, and Security. XV, 548 pages. 2007.

Vol. 4670: V. Dahl, I. Niemelä (Eds.), Logic Programming. XII, 470 pages. 2007.

Vol. 4634: H.R. Nielson, G. Filé (Eds.), Static Analysis. XI, 469 pages. 2007.

Vol. 4615: R. de Lemos, C. Gacek, A. Romanovsky (Eds.), Architecting Dependable Systems IV. XIV, 435 pages. 2007.

Vol. 4610: B. Xiao, L.T. Yang, J. Ma, C. Muller-Schloer, Y. Hua (Eds.), Autonomic and Trusted Computing. XVIII, 571 pages. 2007.

Vol. 4609: E. Ernst (Ed.), ECOOP 2007 – Object-Oriented Programming. XIII, 625 pages. 2007.

Vol. 4608: H.W. Schmidt, I. Crnkovic, G.T. Heineman, J.A. Stafford (Eds.), Component-Based Software Engineering. XII, 283 pages. 2007.

Vol. 4591: J. Davies, J. Gibbons (Eds.), Integrated Formal Methods. IX, 660 pages. 2007.

Vol. 4589: J. Münch, P. Abrahamsson (Eds.), Product-Focused Software Process Improvement. XII, 414 pages. 2007.

Vol. 4574: J. Derrick, J. Vain (Eds.), Formal Techniques for Networked and Distributed Systems – FORTE 2007. XI, 375 pages. 2007.

Vol. 4556: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part III. XXII, 1020 pages. 2007.

Vol. 4555: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part II. XXII, 1066 pages. 2007.

Vol. 4554: C. Stephanidis (Ed.), Universal Acess in Human Computer Interaction, Part I. XXII, 1054 pages. 2007.

Vol. 4553: J.A. Jacko (Ed.), Human-Computer Interaction, Part IV. XXIV, 1225 pages. 2007.

Vol. 4552: J.A. Jacko (Ed.), Human-Computer Interaction, Part III. XXI, 1038 pages. 2007.

Vol. 4551: J.A. Jacko (Ed.), Human-Computer Interaction, Part II. XXIII, 1253 pages. 2007.

Vol. 4550: J.A. Jacko (Ed.), Human-Computer Interaction, Part I. XXIII, 1240 pages. 2007.

Vol. 4542: P. Sawyer, B. Paech, P. Heymans (Eds.), Requirements Engineering: Foundation for Software Quality. IX, 384 pages. 2007.

Vol. 4536: G. Concas, E. Damiani, M. Scotto, G. Succi (Eds.), Agile Processes in Software Engineering and Extreme Programming. XV, 276 pages. 2007.

Vol. 4530: D.H. Akehurst, R. Vogel, R.F. Paige (Eds.), Model Driven Architecture - Foundations and Applications. X, 219 pages. 2007.

Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y.W. Park, L.T. Yang, S.W. Kim (Eds.), Embedded Software and Systems. XIX, 829 pages. 2007.

Vol. 4498: N. Abdennahder, F. Kordon (Eds.), Reliable Software Technologies - Ada-Europe 2007. XII, 247 pages. 2007.

Vol. 4486: M. Bernardo, J. Hillston (Eds.), Formal Methods for Performance Evaluation. VII, 469 pages. 2007.

Vol. 4470: Q. Wang, D. Pfahl, D.M. Raffo (Eds.), Software Process Dynamics and Agility. XI, 346 pages. 2007.

Vol. 4468: M.M. Bonsangue, E.B. Johnsen (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 317 pages. 2007.

Vol. 4467: A.L. Murphy, J. Vitek (Eds.), Coordination Models and Languages. X, 325 pages. 2007.

Vol. 4454: Y. Gurevich, B. Meyer (Eds.), Tests and Proofs. IX, 217 pages. 2007.

Vol. 4444: T. Reps, M. Sagiv, J. Bauer (Eds.), Program Analysis and Compilation, Theory and Practice. X, 361 pages. 2007.

Vol. 4440: B. Liblit, Cooperative Bug Isolation. XV, 101 pages. 2007.

Vol. 4408: R. Choren, A. Garcia, H. Giese, H.-f. Leung, C. Lucena, A. Romanovsky (Eds.), Software Engineering for Multi-Agent Systems V. XII, 233 pages. 2007.

Vol. 4406: W. De Meuter (Ed.), Advances in Smalltalk. VII, 157 pages. 2007.

Vol. 4405: L. Padgham, F. Zambonelli (Eds.), Agent-Oriented Software Engineering VII. XII, 225 pages. 2007.

Vol. 4401: N. Guelfi, D. Buchs (Eds.), Rapid Integration of Software Engineering Techniques. IX, 177 pages. 2007.

Vol. 4385: K. Coninx, K. Luyten, K.A. Schneider (Eds.), Task Models and Diagrams for Users Interface Design. XI, 355 pages. 2007.

Vol. 4383: E. Bin, A. Ziv, S. Ur (Eds.), Hardware and Software, Verification and Testing. XII, 235 pages. 2007.

Vol. 4379: M. Südholt, C. Consel (Eds.), Object-Oriented Technology. VIII, 157 pages. 2007.

Vol. 4364: T. Kühne (Ed.), Models in Software Engineering. XI, 332 pages. 2007.

Vol. 4355: J. Julliand, O. Kouchnarenko (Eds.), B 2007: Formal Specification and Development in B. XIII, 293 pages. 2006.

Vol. 4354: M. Hanus (Ed.), Practical Aspects of Declarative Languages. X, 335 pages. 2006.

Vol. 4350: M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, C. Talcott, All About Maude - A High-Performance Logical Framework. XXII, 797 pages. 2007.

Vol. 4348: S.T. Taft, R.A. Duff, R.L. Brukardt, E. Ploedereder, P. Leroy, Ada 2005 Reference Manual. XXII, 765 pages. 2006.

Vol. 4346: L. Brim, B. Haverkort, M. Leucker, J. van de Pol (Eds.), Formal Methods: Applications and Technology. X, 363 pages. 2007.

Vol. 4344: V. Gruhn, F. Oquendo (Eds.), Software Architecture. X, 245 pages. 2006.

Vol. 4340: R. Prodan, T. Fahringer, Grid Computing. XXIII, 317 pages. 2007.

Vol. 4336: V.R. Basili, D. Rombach, K. Schneider, B. Kitchenham, D. Pfahl, R.W. Selby (Eds.), Empirical Software Engineering Issues. XVII, 193 pages. 2007.

Vol. 4326: S. Göbel, R. Malkewitz, I. Iurgel (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. X, 384 pages. 2006.

Vol. 4323: G. Doherty, A. Blandford (Eds.), Interactive Systems. XI, 269 pages. 2007.

Vol. 4322: F. Kordon, J. Sztipanovits (Eds.), Reliable Systems on Unreliable Networked Platforms. XIV, 317 pages. 2007.

Vol. 4309: P. Inverardi, M. Jazayeri (Eds.), Software Engineering Education in the Modern Age. VIII, 207 pages. 2006.

Vol. 4294: A. Dan, W. Lamersdorf (Eds.), Service-Oriented Computing – ICSOC 2006. XIX, 653 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4262: K. Havelund, M. Núñez, G. Roşu, B. Wolff (Eds.), Formal Approaches to Software Testing and Runtime Verification. VIII, 255 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4242: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development II. IX, 289 pages. 2006.

Vol. 4229: E. Najm, J.F. Pradat-Peyre, V.V. Donzeau-Gouge (Eds.), Formal Techniques for Networked and Distributed Systems - FORTE 2006. X, 486 pages. 2006.

Vol. 4227: W. Nejdl, K. Tochtermann (Eds.), Innovative Approaches for Learning and Knowledge Sharing. XVII, 721 pages. 2006.

Vol. 4218: S. Graf, W. Zhang (Eds.), Automated Technology for Verification and Analysis. XIV, 540 pages. 2006.

Vol. 4214: C. Hofmeister, I. Crnkovic, R. Reussner (Eds.), Quality of Software Architectures. X, 215 pages. 2006.

Vol. 4204: F. Benhamou (Ed.), Principles and Practice of Constraint Programming - CP 2006. XVIII, 774 pages. 2006.

Vol. 4199: O. Nierstrasz, J. Whittle, D. Harel, G. Reggio (Eds.), Model Driven Engineering Languages and Systems. XVI, 798 pages. 2006.

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

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

Vol. 4166: J. Górski (Ed.), Computer Safety, Reliability, and Security. XIV, 440 pages. 2006.

Vol. 4158: L.T. Yang, H. Jin, J. Ma, T. Ungerer (Eds.), Autonomic and Trusted Computing. XIV, 613 pages. 2006.

Vol. 4157: M. Butler, C. Jones, A. Romanovsky, E. Troubitsyna (Eds.), Rigorous Development of Complex Fault-Tolerant Systems. X, 403 pages. 2006.

Vol. 4143: R. Lämmel, J. Saraiva, J. Visser (Eds.), Generative and Transformational Techniques in Software Engineering. X, 471 pages. 2006.

Vol. 4134: K. Yi (Ed.), Static Analysis. XIII, 443 pages. 2006.

Vol. 4119: C. Dony, J.L. Knudsen, A. Romanovsky, A. Tripathi (Eds.), Advanced Topics in Exception Handling Techniques. X, 302 pages. 2006.

Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 447 pages. 2006.

Vol. 4089: W. Löwe, M. Südholt (Eds.), Software Composition. X, 339 pages. 2006.

Vol. 4085: J. Misra, T. Nipkow, E. Sekerinski (Eds.), FM 2006: Formal Methods. XV, 620 pages. 2006.

Vol. 4079: S. Etalle, M. Truszczyński (Eds.), Logic Programming. XIV, 474 pages. 2006.

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4066: A. Rensink, J. Warmer (Eds.), Model Driven Architecture – Foundations and Applications. XII, 392 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

¥732.00元

Table of Contents

Safety Cases

Impact of Security on Safety

Poster Session 1

Fault Tree Analysis

Safety Analysis

Security Aspects

Poster Session 2

Verification and Validation

Platform Reliability

Reliability Evaluation

Poster Session 3

Formal Methods

Static Code Analysis

Safety-Related Architectures

Establishing Evidence for Safety Cases in Automotive Systems – A Case Study

Willem Ridderhof[1], Hans-Gerhard Gross[2], and Heiko Doerr[3]

[1] ISPS Medical Software, Rotterdamseweg 145, 2628 AL Delft
willem.ridderhof@isps-medical-software.nl
[2] Embedded Software Laboratory, Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands
h.g.gross@tudelft.nl
[3] CARMEQ GmbH, Carnotstr. 4, 10587 Berlin, Germany
heiko.doerr@carmeq.com

Abstract. The upcoming safety standard ISO/WD 26262 that has been derived from the more general IEC 61508 and adapted for the automotive industry, introduces the concept of a safety case, a scheme that has already been successfully applied in other sectors of industry such as nuclear, defense, aerospace, and railway. A safety case communicates a clear, comprehensive and defensible argument that a system is acceptably safe in its operating context. Although, the standard prescribes that there should be a safety argument, it does not establish detailed guidelines on how such an argument should be organized and implemented, or which artifacts should be provided.

In this paper, we introduce a methodology and a tool chain for establishing a safety argument, plus the evidence to prove the argument, as a concrete reference realization of the ISO/WD 26262 for automotive systems. We use the Goal-Structuring-Notation to decompose and refine safety claims of an emergency braking system (EBS) for trucks into sub-claims until they can be proven by evidence. The evidence comes from tracing the safety requirements of the system into their respective development artifacts in which they are realized.

1 Introduction

Safety critical systems have to fulfill safety requirements in addition to functional requirements. Safety requirements describe the characteristics that a system must have in order to be safe [12]. This involves the identification of all hazards that can take place, and that may harm people or the environment. Safety-related issues are often captured in standards describing products and processes to be considered throughout the life-cycle of a safety critical system. The upcoming safety standard ISO/WD 26262 [2] is an implementation of the more general IEC 61508 standard that addresses safety issues in the automotive industry. The objective of the automotive standard is to take the specific constraints of automotive embedded systems and their development processes

F. Saglietti and N. Oster (Eds.): SAFECOMP 2007, LNCS 4680, pp. 1–13, 2007.