

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Frank Ortmeier Peter Daniel (Eds.)

Computer Safety, Reliability, and Security

SAFECOMP 2012 Workshops: Sassur, ASCoMS,
DESEC4LCCI, ERCIM/EWICS, IWDE
Magdeburg, Germany, September 25-28, 2012
Proceedings

Volume Editors

Frank Ortmeier

Otto-von-Guericke-Universität, Fakultät für Informatik
Institut für Technische und Betriebliche Informationssysteme (ITI)
Universitätsplatz 2, 39106 Magdeburg, Germany
E-mail: frank.ortmeier@ovgu.de

Peter Daniel

SELEX ELSAG, Liverpool Innovation Park
Edge Lane, Fairfield, Liverpool, L7 9NJ, UK
E-mail: ewicstc7@prdaniel.co.uk

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-33674-4

e-ISBN 978-3-642-33675-1

DOI 10.1007/978-3-642-33675-1

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012947423

CR Subject Classification (1998): K.6.5, D.2, C.2, F.3, H.4, D.3, I.2

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Safety, reliability, and security are becoming vital in almost all technical domains. The reason is that computer pervasion is steadily increasing and more and more systems are becoming networked. This often leads to the term of cyber-physical systems, i.e., systems influencing our environment that are connected by modern computer networks. Examples are smart traffic guidance, intelligent power lines, or autonomous vehicles. Despite the commonality in safety challenges, each domain has very specific stakeholders, requirements, standards, etc.

To account for this, we decided to give various domain experts a common meeting place in the form of domain-specific workshops at SAFECOMP. The common theme is safety and security. Bringing these experts together at one place and collecting their articles in one volume fosters collaboration and the exchange of ideas.

For SAFECOMP 2012, we accepted five domain-specific, high-quality workshops. Each workshop had well-known chairs and an international program committee. Altogether 69 researchers from 15 countries reviewed the following 44 articles.

Architecting safe collaborative mobile systems was the aim of the ASCoMS workshop (chairs: António Casimiro and Jörg Kaiser). Building autonomous mobile systems is already challenging. However, for transition from academia to real-world scenarios, safety guarantees are mandatory and a prerequisite for acceptance.

Our daily life heavily depends upon the correct functioning of many complex large-scale infrastructures such as communication, power, or water supply. The DESEC4LCCI workshop (chairs: Christian Esposito, Marco Platania, and Francesco Brancati) focused on dependable and secure computing for such systems. Until recently, security for such systems could be reduced to physical security (i.e., protecting the infrastructure by security personal). As systems become widely connected, this is no longer sufficient and new approaches must be developed.

The emergence of cyber-physical systems is speeding up exponentially. The ERCIM/EWICS/DECOS workshop (chairs: Erwin Schoitsch and Amund Skavhaug) brought together stakeholders from many major European research projects and programs to exchange ideas on making such systems safer and more reliable.

Design and operation of most technical systems is no longer only an engineering challenge. It requires the interaction of mechanical, electrical, and software engineers for digitally engineering such a system. The 3rd International Workshop on Digital Engineering – IWDE (chairs: Gunter Saake and Veit Köppen) brought together researchers from these domains, which share the common vision of jointly digitally engineering safe and secure systems.

Safety assurance and certification are amongst the most expensive and time-consuming tasks in the development of safety-critical systems. The SASSUR workshop (chairs: Alejandra Ruiz, Tim Kelly, Mehrdad Sabetzadeh, and Didier Van den Abeele) focused exactly on bridging this gap. It covered new methods, approaches, and tools on tackling this problem.

Summarizing, I have to say that correspondence and organization of these five workshops for SAFECOMP took a lot of my time. But when looking at the program now, I would like to express my deepest thanks to all workshop chairs. You did a fantastic job. The program was very tempting and a great extension to SAFECOMP 2012. I would also like to thank in particular Michael Lipaczewski, who did a great job in organizing this volume and collecting all the articles, introductions, copyright forms, etc.

I hope you are all enjoying this volume and are maybe even benefitting from some new ideas and achievements presented here.

August 2012

Frank Ortmeier

Organization

Next Generation of System Assurance Approaches for Safety-Critical Systems Workshop (Sassur 2012)

Chairs

Didier Van Den Abeele	Alstom Transport, France
Tim Kelly	University of York, UK
Alejandra Ruiz	Tecnalía, Spain
Mehrdad Sabetzadeh	Simula Research Laboratory, Norway

Steering Committee

Annie Combelles	Inspairit, France
Javier Díaz	University of Granada, Spain
Huascar Espinoza	TECNALIA, Spain
John Favaro	Intecs, Italy
Paolo Panaroni	Intecs, Italy
Fulvio Tagliabò	Centro Ricerche FIAT, Italy

Program Committee

Katrina Attwood	University of York, UK
Fabien Belmonte	Alstom, France
Ronald Blanrue	EADS/Eurocopter, France
Marc Born	ikv++ technologies ag, Germany
Sergio Campos	Tecnalía Research & Innovation, Spain
Daniela Cancilla	Atego, France
Cedric Chevrel	Thales Avionics, France
C. Michael Holloway	NASA Langley Research Center, USA
Olaf Kath	ikv++ technologies ag, Germany
Andreas Keis	EADS/Innovation Works, UK
Uwe Kremer	TÜV SÜD, Germany
Xabier Larrucea	TECNALIA, Spain
Mark Nicholson	University of York, UK
Jürgen Niehaus	Safetrans, Germany
Kenji Taguchi	AIST, Japan
Jose Luis De La Vara	Simula Research Laboratory, Norway
Harold Weffers	Eindhoven University of Technology, The Netherlands

Workshop on Architecting Safety in Collaborative Mobile Systems (ASCoMS 2012)

Chairs

António Casimiro	University of Lisbon, Portugal
Jörg Kaiser	Otto-von-Guericke-University of Magdeburg, Germany

Program Committee

Luis Almeida	FEUP, Portugal
Leandro Becker	UFSC, Brazil
Andrea Bondavalli	University of Florence, Italy
Thomas Fuhrman	GM, USA
Karl Goeschka	Vienna University of Technology, Austria
Rolf Johansson	SP, Sweden
Marcelo Lemes	EMBRAER, Brazil
Priya Narasimhan	Carnegie Mellon University, USA
Edgar Nett	Otto-von-Guericke-University of Magdeburg, Germany
Stefan Schemmer	RT Solutions, Germany
Elad Michael Schiller	Chalmers University of Technology, Sweden
Paulo Verissimo	University of Lisbon, Portugal

Workshop on Dependable and Secure Computing for Large-scale Complex Critical Infrastructures (DESEC4LCCI 2012)

Chairs

Francesco Brancati	Resiltech, Italy
Christian Esposito	Institute of High Performance Computing and Networking (ICAR), Italy
Marco Platania	Sapienza University of Rome, Italy

Program Committee

Angelo Corsaro	PrismTech, UK
Michele Colajanni	University of Modena, Italy
Bojan Cukic	West Virginia University, USA
Francesco Flammini	University “Federico II” of Naples, Italy
Felicita Di Giandomenico	ISTI-CNR, Italy

Abdelmajid Khelil	TU Darmstadt, Germany
Catello Di Martino	University of Illinois at Urbana-Champaign, USA
Edgar Nett	Otto-von-Guericke-University of Magdeburg, Germany
Ricardo Jimenez Peris	Universidad Politecnica de Madrid, Spain
Sara Tucci Piergiovanni	CEA LIST, Italy
Luigi Romano	Parthenope University of Naples, Italy
Nuno Silva	Critical Software SA, Portugal
Paulo Verissimo	University of Lisbon, Portugal
Marco Vieira	University of Coimbra, Portugal

ERCIM/EWICS/Cyberphysical Systems Workshop

Chairs

Erwin Schoitsch	Austrian Institute of Technology, Austria
Amund Skavhaug	NTNU, Trondheim, Norway

Program Committee

Friedemann Bitsch	Germany
Sandro Bologna	Italy
Wolfgang Ehrenberger	Germany
Francesco Flammini	Italy
Robert Genser	Austria
Janusz Gorski	Poland
Maritta Heisel	Germany
Floor Koornneef	The Netherlands
Peter Ladkin	Germany
Meine van der Meulen	Norway
Odd Nordland	Norway
Frank Ortmeier	Germany
Thomas Pfeiffenberger	Austria
Francesca Saglietti	Germany
Christoph Schmitz	Switzerland
Erwin Schoitsch	Austria
Rolf Schumacher	Germany
Amund Skavhaug	Norway

International Workshop on Digital Engineering (IWDE 2012)

Chairs

Veit Köppen	Otto-von-Guericke-University Magdeburg, Germany
Gunter Saake	Otto-von-Guericke-University Magdeburg, Germany

Program Committee

Abdel-Badeeh M. Salem	Ain Shams University, Egypt
Andreas Brenke	HS Niederrhein, Germany
Raimund Dachselt	TU Dresden, Germany
Matthias Güdemann	Inria, Grenoble, France
Frank Ortmeier	Otto-von-Guericke University Magdeburg, Germany
Dirk Reiners	University of Louisiana at Lafayette, USA
Hermann Rohling	TU Hamburg, Germany
Michael Schenk	FhG IFF Magdeburg, Germany
Gunter Saake	Otto-von-Guericke University Magdeburg, Germany

Table of Contents

Next Generation of System Assurance Approaches for Safety-Critical Systems Workshop (Sassur 2012)	
Introduction to Sassur 2012	3
<i>Alejandra Ruiz, Tim P. Kelly, Mehrdad Sabetzadeh, and Didier Van Den Abeele</i>	
AdvoCATE: An Assurance Case Automation Toolset	8
<i>Ewen Denney, Ganesh Pai, and Josef Pohl</i>	
Towards a Case-Based Reasoning Approach for Safety Assurance Reuse	22
<i>Alejandra Ruiz, Ibrahim Habli, and Huáscar Espinoza</i>	
Modeling for Safety in a Synthesis-Centric Systems Engineering Framework	36
<i>Jasen Markovski and J.M. van de Mortel-Fronczak</i>	
A Model Based Approach for Safety Analysis	50
<i>Fabien Belmonte and Elie Soubiran</i>	
Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards	64
<i>Jose Luis de la Vara, Sunil Nair, Eric Verhulst, Janusz Studzizba, Piotr Pepek, Jerome Lambourg, and Mehrdad Sabetzadeh</i>	
A New Approach to Assessment of Confidence in Assurance Cases	79
<i>Xingyu Zhao, Dajian Zhang, Minyan Lu, and Fuping Zeng</i>	
An Unified Meta-model for Trustworthy Systems Engineering	92
<i>Eric Verhulst and Bernhard H.C. Spath</i>	
A Preliminary Fault Injection Framework for Evaluating Multicore Systems	106
<i>Anna Lanzaro, Antonio Pecchia, Marcello Cinque, Domenico Cotroneo, Ricardo Barbosa, and Nuno Silva</i>	
Meeting Real-Time Requirements with Multi-core Processors	117
<i>Daniel Kästner, Marc Schlickling, Markus Pister, Christoph Cullmann, Gernot Gebhard, Reinhold Heckmann, and Christian Ferdinand</i>	
Assessing Software Interference Management When Modifying Safety-Related Software	132
<i>Patrick J. Graydon and Tim P. Kelly</i>	

Workshop on Architecting Safety in Collaborative Mobile Systems (ASCoMS 2012)

Introduction to ASCoMS 2012 149
António Casimiro and Jörg Kaiser

Towards Dependable and Stable Perception in Smart Environments with Timing and Value Faults 151
Luís Marques and António Casimiro

An Approach Supporting Fault-Propagation Analysis for Smart Sensor Systems 162
Sebastian Zug, Tino Brade, Jörg Kaiser, and Sasanka Potluri

Use of Quality Metrics for Functional Safety in Systems of Cooperative Vehicles 174
Kenneth Östberg and Rolf Johansson

From Autonomous Vehicles to Safer Cars: Selected Challenges for the Software Engineering 180
Christian Berger

Modelling of Safety-Related Timing Constraints for Automotive Embedded Systems 190
Oscar Ljungkrantz, Henrik Lönn, Hans Blom, Cecilia Ekelin, and Daniel Karlsson

Workshop on Dependable and Secure Computing for Large-Scale Complex Critical Infrastructures (DESEC4LCCI 2012)

Introduction to DESEC4LCCI 2012 205
Christian Esposito, Marco Platania, and Francesco Brancati

Quantitative Security Evaluation of a Multi-biometric Authentication System 209
Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli, and Ernesto La Mattina

Protecting the WSN Zones of a Critical Infrastructure via Enhanced SIEM Technology 222
Luigi Romano, Salvatore D'Antonio, Valerio Formicola, and Luigi Coppolino

On Securing Communications among Federated Health Information Systems 235
Mario Ciampi, Giuseppe De Pietro, Christian Esposito, Mario Sicuranza, Paolo Mori, Abraham Gebrehiwot, and Paolo Donzelli

How Secure Is ERTMS?	247
<i>Richard Bloomfield, Robin Bloomfield, Ilir Gashi, and Robert Stroud</i>	
International Cooperation Experiences: Results Achieved, Lessons Learned, and Way Ahead	259
<i>Craig Gibson, Matteo Melideo, Luigi Romano, and Salvatore D'Antonio</i>	
A Federated Simulation Framework with ATN Fault Injection Module for Reliability Analysis of UAVs in Non-controlled Airspace	271
<i>Magali Andreia Rossi, Jorge Rady de Almeida Junior, Andrea Bondavalli, and Paolo Lollini</i>	
HSIENA: A Hybrid Publish/Subscribe System	282
<i>Fabio Petroni and Leonardo Querzoni</i>	
WSDM-Enabled Autonomic Augmentation of Classical Multi-version Software Fault-Tolerance Mechanisms	294
<i>Roeland Dillen, Jonas Buys, Vincenzo De Florio, and Chris Blondia</i>	
Formal Verification of a Safety Argumentation and Application to a Complex UAV System	307
<i>Julien Brunel and Jacques Cazin</i>	
Electronic Reliability Estimation: How Reliable Are the Results?	319
<i>Nuno Silva and Rui Lopes</i>	
Model-Based Assessment of Multi-region Electric Power Systems Showing Heterogeneous Characteristics	328
<i>Silvano Chiaradonna, Felicita Di Giandomenico, and Nicola Nostro</i>	
ERCIM/EWICS/Cyberphysical Systems Workshop	
Introduction to the ERCIM/EWICS Cyberphysical Systems Workshop 2012	343
<i>Erwin Schoitsch and Amund Skavhaug</i>	
The Cyber-Physical Attacker	347
<i>Roberto Vigo</i>	
Dependable and Secure Embedded Node Demonstrator	357
<i>Przemysław Osocha, João Carlos Cunha, and Fabio Giovagnini</i>	
Towards Secure Time-Triggered Systems	365
<i>Florian Skopik, Albert Treytl, Arjan Geven, Bernd Hirschler, Thomas Bleier, Andreas Eckel, Christian El-Salloum, and Armin Wasicek</i>	

Towards a Framework for Simulation Based Design, Validation and Performance Analysis of Electronic Control Systems	373
<i>Alexander Hanzlik and Erwin Kristen</i>	
Compiling for Time Predictability	382
<i>Peter Puschner, Raimund Kirner, Benedikt Huber, and Daniel Prokesch</i>	
Towards the Automated Qualification of Tool Chain Design	392
<i>Fredrik Asplund, Matthias Biehl, and Frédéric Loiret</i>	
A Systematic Elaboration of Safety Requirements in the Avionic Domain	400
<i>Antoaneta Kondeva, Martin Wassmuth, and Andreas Mitschke</i>	
Parallel NuSMV: A NuSMV Extension for the Verification of Complex Embedded Systems	409
<i>Orlando Ferrante, Luca Benvenuti, Leonardo Mangeruca, Christos Sofronis, and Alberto Ferrari</i>	
Supporting Assurance by Evidence-Based Argument Services	417
<i>Janusz Górski, Aleksander Jarzębowski, Jakub Miler, Michał Witkiewicz, Jakub Czyżnikiewicz, and Patryk Jar</i>	
Towards Composable Robotics: The R3-COP Knowledge-Base Driven Technology Platform	427
<i>Erwin Schoitsch, Wolfgang Herzner, Carmen Alonso-Montes, P. Chmelar, and Lars Dalgaard</i>	
Addressing the Needs of an Aging Population: An Experiment for Monitoring Behaviour in a Domestic Environment	436
<i>Marte E.B. Skjønsvjell, Aslak R. Normann, Dag Sjong, and Amund Skavhaug</i>	
International Workshop on Digital Engineering (IWDE 2012)	
Introduction to IWDE 2012	449
<i>Veit Köppen and Gunter Saake</i>	
Modeling the Effects of Software on Safety and Reliability in Complex Embedded Systems	454
<i>Max Steiner, Patric Keller, and Peter Liggesmeyer</i>	
Towards Artificial Perception	466
<i>André Dietrich, Sebastian Zug, and Jörg Kaiser</i>	

A Case Study of Radio-Based Monitoring System for Enhanced Safety of Logistics Processes	477
<i>Michael Soffner, Mykhaylo Nykolaychuk, Friederike Adler, and Klaus Richter</i>	
Visual Approach Facilitating the Importance Analysis of Component Fault Trees	486
<i>Yi Yang, Patric Keller, and Peter Liggesmeyer</i>	
Simulation of Structural Effects in Embedded Systems and Visualization of Dependencies According to an Intended Attack or Manipulation	498
<i>Sven Kuhlmann, Jana Fruth, Tobias Hoppe, and Jana Dittmann</i>	
From Discrete Event Simulation to Virtual Reality Environments	508
<i>Sebastian Nielebock, Frank Ortmeier, Marco Schumann, and André Winge</i>	
Program Comprehension in Preprocessor-Based Software	517
<i>Janet Siegmund, Norbert Siegmund, Jana Fruth, Sven Kuhlmann, Jana Dittmann, and Gunter Saake</i>	
Author Index	529