Lecture Notes in Computer Science 7612

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

Frank Ortmeier Peter Daniel (Eds.)

Computer Safety, Reliability, and Security

31st International Conference, SAFECOMP 2012
Magdeburg, Germany, September 25-28, 2012
Proceedings

Springer

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
European Workshop on Industrial Computer Systems Reliability,
Safety and Security, EWICS TC7
7 Lime Tree Grove, Heswall, Wirral CH60 1US, UK
E-mail: ewicstc7@prdaniel.co.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-33677-5 e-ISBN 978-3-642-33678-2
DOI 10.1007/978-3-642-33678-2
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012947537

CR Subject Classification (1998): K.6.5, C.2, D.2, H.3, D.4.6, E.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

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

Since 1979, when the first SAFECOMP conference was organized by the Technical Committee on Reliability, Safety and Security of the European Workshop on Industrial Computer Systems (EWICS TC7), the SAFECOMP conference series has always been a mirror of current trends and challenges in highly critical systems engineering.

The key theme of SAFECOMP 2012 was "virtually safe – making system safety traceable". This theme addresses two important aspects of critical systems. On the one hand, systems are always claimed to be virtually safe, which often means they are safe unless some very rare events happen. However, many recent accidents – like Fukushima, for example, – have shown that these assumptions often do not hold. As a consequence, we must reconsider what acceptable and residual risk shall be. The second aspect of the theme addresses the question of making system safety understandable. Safety case and arguments are often based on a deep understanding of the system and its behavior. Displaying such dynamic behavior in a visual way or even a virtual reality scenario might help in understanding the arguments better and finding flaws more easily.

SAFECOMP has always seen itself as a conference connecting industry and academia. To account for this, we introduced separate categories for industrial and academic papers. More than 70 submission from authors of 20 countries were reviewed and the best 33 papers were selected for presentation at the conference and publication in this volume. In addition, three invited talks given by Jürgen Leohold (CTO of Volkswagen), Marta Kwiatkowska (Oxford University), and Hans Hansson (Mälardalen University) were included in the conference program. Safety, security, and reliability is a very broad topic, which touches many different application domains. In 2012, we decided to co-locate five scientific workshops, which focus on different current topics ranging from critical infrastructures to dependable cyber-physical systems. The SAFECOMP workshops are not included in this volume but in a separate SAFECOMP LNCS volume.

As Program Chairs , we want to give a very warm thank you to all 60 members of the international Program Committee. The comprehensive reviews provided the basis for the productive discussions at the Program Committee meeting held in May in Munich, which was hosted by Siemens. We also want to thank the local organization team at the Otto-von-Guericke University Magdeburg (OVGU), the Local Chairs Gunter Saake, Michael Schenk, and Jana Dittmann, the Center for Digital Engineering (CDE), and the Virtual Development and Training Center (VDTC).

Finally, we hope you find, the papers in this volume interesting. On behalf of EWICS TC7, we also invite you to join the SAFECOMP community and hope you will be joining us at the 2013 SAFECOMP conference in Toulouse.

September 2012

Frank Ortmeier
Peter Daniel

Organization

Program Committee

Stuart Anderson	University of Edinburgh, UK
Tom Anderson	Newcastle University, UK
Friedemann Bitsch	Thales Transportation Systems, Stuttgart, Germany
Robin Bloomfield	CSR, City University London, UK
Sandro Bologna	Associazione Italiana Esperti in Infrastrutture Critiche, Italy
Andrea Bondavalli	University of Florence, Italy
Jens Braband	Siemens AG, Germany
Manfred Broy	TUM, Germany
Bettina Buth	HAW Hamburg, Germany
Werner Damm	OFFIS e.V., Germany
Peter Daniel	European Workshop on Industrial Computer Systems Reliability, Safety and Security, EWICS TC7, UK
Jana Dittmann	Otto-von-Guericke-University of Magdeburg, Germany
Wolfgang Ehrenberger	Fachhochschule Fulda, Germany
Massimo Felici	University of Edinburgh, UK
Francesco Flammini	Ansaldo STS Italy, University "Federico II" of Naples, Italy
Georg Frey	Saarland University, Germany
Holger Giese	Hasso Plattner Institute, Germany
Michael Glaß	University of Erlangen-Nuremberg, Germany
Janusz Gorski	Gdansk University of Technology, FETI, DSE, Poland
Lars Grunske	Swinburne University of Technology, Australia
Jérémie Guiochet	Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS, France
Peter Göhner	University of Stuttgart, Germany
Wolfgang Halang	Lehrgebiet Informationstechnik, Fernuniversität in Hagen, Germany
Maritta Heisel	University of Duisburg-Essen, Germany
Constance Heitmeyer	Naval Research Laboratory, Washington, USA
Chris Johnson	University of Glasgow, UK
Jan Jürjens	Technical University of Dortmund and Fraunhofer ISST, Germany
Mohamed Kaaniche	Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS, France

Hubert B. Keller	Karlsruhe Institute of Technology, Germany
Tim Kelly	University of York, UK
John Knight	University of Virginia, USA
Floor Koornneef	Technical University of Delft, The Netherlands
Peter Ladkin	University of Bielefeld, Germany
Jean-Jacques Lesage	ENS de Cachan, France
Peter Liggesmeyer	Technical University of Kaiserslautern, Germany
Søren Lindskov-Hansen	Nove Nordisk A/S, Denmark
Bev Littlewood	City University, UK
Juergen Mottok	University of Applied Sciences Regensburg, Germany
Odd Nordland	SINTEF, Norway
Frank Ortmeier	Otto-von-Guericke-University of Magdeburg, Germany
András Pataricza	Budapest University of Technology and Economics, Hungary
Thomas Pfeiffenberger	Salzburg Research Forschungsgesellschaft m.b.H, Austria
Wolfgang Reif	Augsburg University, Germany
Gerhard Rieger	TÜV Nord, Germany
Alexander Romanovsky	Newcastle University, UK
Martin Rothfelder	Siemens AG, Germany
Gunter Saake	Otto-von-Guericke-University of Magdeburg, Germany
Francesca Saglietti	University of Erlangen-Nuremberg, Germany
Bernhard Schaetz	Technical University of Munich, Germany
Michael Schenk	IFF Magdeburg, Germany
Christoph Schmitz	Zühlke, Zurich, Switzerland
Erwin Schoitsch	Austrian Institute of Technology, Austria
Wilhelm Schäfer	University of Paderborn, Germany
Sahra Sedigh	Missouri University of Science and Technology, USA
Amund Skavhaug	Norwegian University of Science and Technology, Norway
Mark-Alexander Sujan	University of Warwick, UK
Kishor Trivedi	Duke University, USA
Meine Van Der Meulen	Det Norske Veritas (DNV), Norway
Birgit Vogel-Heuser	Technical University of Munich, Germany

Sponsors

- EWICS TC7 - European Workshop on Industrial Computer Systems Reliability, Safety and Security
- OVGU - Otto von Guericke University of Magdeburg
- METOP - Mensch, Technik, Organisation und Planung
- CDE - Center for Digital Engineering
- VDTC - Virtual Development and Taining Centre
- Siemens
- TÜV Nord
- MES - Model Engineering Solutions
- Zühlke - empowering ideas
- GfSE - Gesellschaft für System Engineering e.V.
- GI - Gesellschaft für Informatik e.V.
- IEEE - Advancing Technology for Humanity
- OCG - Austrian Computer Society
- IFAC - International Federation of Accountants
- IFIP - International Federation for Information Processing
- ERCIM - European Research Consortium for Informatics and Mathematics
- ARTEMIS Austria
- ENCRESS - European Network of Clubs for Reliability and Safety of Software
- AIT - Austrian Institute of Technology
- CSE - Center for Digital Engineering
- ISOTEC - Institut für innovative Softwaretechnologie

Organizing Team

- Augustine, Marcus
- Fietz, Gabriele
- Gonschorek, Tim
- Güdemann, Matthias
- Köppen, Veit
- Lipaczewski, Michael
- Ortmeier, Frank
- Struck, Simon
- Weise, Jens

General Information on SAFECOMP

SAFECOMP is an annual event, which is internationally hosted around the world. Further information on previous and upcoming SAFECOMP events may be found at www.safecomp.org.

Towards Composable Safety (Invited Talk)

Prof. Hans Hansson

Märdalen University, Västerås, Sweden

Increased levels of complexity of safety-relevant systems bring increased responsibility on the system developers in terms of quality demands from the legal perspectives as well as company reputation. Component based development of software systems provides a viable and cost-effective alternative in this context provided one can address the quality and safety certification demands in an efficient manner. This keynote targets component-based development and composable safety-argumentation for safety-relevant systems. Our overarching objective is to increase efficiency and reuse in development and certification of safety-relevant embedded systems by providing process and technology that enable composable qualification and certification, i.e. qualification/certification of systems/subsystems based on reuse of already established arguments for and properties of their parts. The keynote is based on on-going research in two larger research efforts; the EU/ARTEMIS project SafeCer and the Swedish national project SYNOPSIS. Both projects started in 2011 and will end 2015. SafeCer includes more than 30 partners in six different countries, and aims at adapting processes, developing tools, and demonstrating applicability of composable certification within the domains: Automotive, Avionics, Construction Equipment, Healthcare, and Rail, as well as addressing cross-domain reuse of safety-relevant components. SYNOPSIS is a project at Mälardalen University sharing the SafeCer objective of composable certification, but emphasizing more the scientific basis than industrial deployment.

Our research is motivated by several important and clearly perceivable trends: (1) The increase in software based solutions which has led to new legal directives in several application domains as well as a growth in safety certification standards. (2) The need for more information to increase the efficiency of production, reduce the cost of maintaining sufficient inventory, and enhance the safety of personnel. (3) The rapid increase in complexity of software controlled products and production systems, mainly due to the flexibility and ease of adding new functions made possible by the software. As a result the costs for certification-related activities increase rapidly. (4) Modular safety arguments and safety argument contracts have in recent years been developed to support the needs of incremental certification. (5) Component-Based Development (CBD) approaches, by which systems are built from pre-developed components, have been introduced to improve both reuse and the maintainability of systems. CBD has been in the research focus for some time and is gaining industrial acceptance, though few approaches are targeting the complex requirements of the embedded domain.

Our aim is to enhance existing CBD frameworks by extending them to include dependability aspects so that the design and the certification of systems can be addressed together more efficiently. This would allow reasoning about the design and safety aspects of parts of the systems (components) in relative isolation, without consideration of their interfaces and emergent behaviour, and then deal with these remaining issues in a more structured manner without having to revert to the current holistic practices. The majority of research on such compositional aspects has concentrated on the functional properties of systems with a few efforts dealing with timing properties. However, much less work has considered non-functional properties, including dependability properties such as safety, reliability and availability.

This keynote provides an introduction to component-based software development and how it can be applied to development of safety-relevant embedded systems, together with an overview and motivation of the research being performed in the SafeCer and SYNOPSIS projects. Key verification and safety argumentation challenges will be presented and solutions outlined.

Sensing Everywhere: Towards Safer and More Reliable Sensor-Enabled Devices (Invited Talk)

Marta Kwiatkowska

Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Abstract. In this age of ubiquitous computing we are witnessing ever increasing dependence on sensing technologies. Sensor-enabled smart devices are used in a broad range of applications, from environmental monitoring, where the main purpose is information gathering and appropriate response, through smartphones capable of autonomous function and localisation, to integrated and sometimes invasive control of physical processes. The latter group includes, for example, self-parking and self-driving cars, as well as implantable devices such as glucose monitors and cardiac pacemakers [1, 2]. Future potential developments in this area are endless, with nanotechnology and molecular sensing devices already envisaged [3].

These trends have naturally prompted a surge of interest in methodologies for ensuring safety and reliability of sensor-based devices. Device recalls [4] have added another dimension of safety concerns, leading FDA to tighten its oversight of medical devices. In seeking safety and reliability assurance, developers employ techniques to answer to queries such as "the smartphone will never disclose the bank account PIN number to unauthorised parties", "the blood glucose level returns to a normal range in at most 3 hours" and "the probability of failure to raise alarm if the levels of airborne pollutant are unacceptably high is tolerably low". Model-based design and automated verification technologies offer a number of advantages, particularly with regard to embedded software controllers: they enable rigorous software engineering methods such as automated verification in addition to testing, and have the potential to reduce the development effort through code generation and software reuse via product lines.

Automated verification has made great progress in recent years, resulting in a variety of software tools now integrated within software development environments. Models can be extracted from high-level design notations or even source code, represented as finite-state abstractions, and systematically analysed to establish if, e.g., the executions never violate a given temporal logic property. In cases where the focus is on safety, reliability and performance, it is necessary to include in the models quantitative aspects such as probability, time and energy usage. The preferred technique here is quantitative verification [5], which employs variants of Markov chains, annotated with reward structures, as models

and aims establish quantitative properties, for example, calculating the probability or expectation of a given event. Tools such as the probabilistic model checker PRISM [6] are widely used to analyse safety, dependability and performability of system models in several application domains, including communication protocols, sensor networks and biological systems.

The lecture will give an overview of current research directions in automated verification for sensor-enabled devices. This will include software verification for TinyOS [7], aimed at improving the reliability of embedded software written in nesC; as well as analysis of sensor network protocols for collective decision making, where the increased levels of autonomy demand a stochastic games approach [8]. We will outline the promise and future challenges of the methods, including emerging applications at the molecular level [9] that are already attracting attention from the software engineering community [10].

Acknowledgement. This research has been supported in part by ERC grant VERIWARE and Oxford Martin School.

References

1. Sankaranarayanan, S., Fainekos, G.: Simulating insulin infusion pump risks by in-silico modeling of the insulin-glucose regulatory system. In: Proc. CMSB 2012. LNCS. Springer, Heidelberg (to appear, 2012)
2. Jiang, Z., Pajic, M., Moarref, S., Alur, R., Mangharam, R.: Modeling and Verification of a Dual Chamber Implantable Pacemaker. In: Flanagan, C., König, B. (eds.) TACAS 2012. LNCS, vol. 7214, pp. 188–203. Springer, Heidelberg (2012)
3. Kroeker, K.L.: The rise of molecular machines. Commun. ACM 54(12), 11–13 (2011)
4. Food, U.: Drug Admin. (List of Device Recalls).
5. Kwiatkowska, M.: Quantitative verification: Models, techniques and tools. In: Proc. 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE), pp. 449–458. ACM Press, New York (2007)
6. Kwiatkowska, M., Norman, G., Parker, D.: PRISM 4.0: Verification of Probabilistic Real-Time Systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 585–591. Springer, Heidelberg (2011)
7. Bucur, D., Kwiatkowska, M.: On software verification for TinyOS. Journal of Software and Systems 84(10), 1693–1707 (2011)
8. Chen, T., Forejt, V., Kwiatkowska, M., Parker, D., Simaitis, A.: Automatic Verification of Competitive Stochastic Systems. In: Flanagan, C., König, B. (eds.) TACAS 2012. LNCS, vol. 7214, pp. 315–330. Springer, Heidelberg (2012)
9. Lakin, M., Parker, D., Cardelli, L., Kwiatkowska, M., Phillips, A.: Design and analysis of DNA strand displacement devices using probabilistic model checking. Journal of the Royal Society Interface 9(72), 1470–1485 (2012)
10. Lutz, R.R., Lutz, J.H., Lathrop, J.I., Klinge, T., Henderson, E., Mathur, D., Sheasha, D.A.: Engineering and verifying requirements for programmable self-assembling nanomachines. In: ICSE, pp. 1361–1364. IEEE (2012)

Table of Contents

Session I: Tools

Session II: Risk Analysis

Session III: Testing

Session IV: Quantitative Analysis

Session V: Security

Session VI: Formal Methods 1

Session VII: Aeronautic

Session VIII: Automotive

Session IX: Formal Methods 2

Session X: Process

Session XI: Case Studies