Lecture Notes in Computer Science 6150

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

Holger Giese (Ed.)

Architecting Critical Systems

First International Symposium, ISARCS 2010
Prague, Czech Republic, June 23-25, 2010
Proceedings

Springer

Volume Editor

Holger Giese
Hasso Plattner Institute for Software Systems Engineering
Prof.-Dr.-Helmert-Str. 2-3, 14482 Potsdam, Germany
E-mail: Holger.Giese@hpi.uni-potsdam.de

Library of Congress Control Number: 2010928429

CR Subject Classification (1998): C.3, K.6.5, D.4.6, E.3, H.4, D.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-13555-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13555-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

Architecting critical systems has gained major importance in commercial, governmental and industrial sectors. Emerging software applications encompass criticalities that are associated with either the whole system or some of its components. Therefore, effective methods, techniques, and tools for constructing, testing, analyzing, and evaluating the architectures for critical systems are of major importance. Furthermore, these methods, techniques and tools must address issues of dependability and security, while focusing not only on the development, but also on the deployment and evolution of the architecture.

This newly established ISARCS symposium provided an exclusive forum for exchanging views on the theory and practice for architecting critical systems. Such systems are characterized by the perceived severity of consequences that faults or attacks may cause, and architecting them requires appropriate means to assure that they will fulfill their specified services in a dependable and secure manner.

The different attributes of dependability and security cannot be considered in isolation for today's critical systems, as architecting critical systems essentially means to find the right trade-off among these attributes and the various other requirements imposed on the system. This symposium therefore brought together the four communities working on dependability, safety, security and testing/analysis, each addressing to some extent the architecting of critical systems from their specific perspective. To this end the symposium united the following three former events:

- Workshop on Architecting Dependable Systems (WADS)
- Workshop on the Role of Software Architecture for Testing and Analysis (ROSATEA)
- Workshop on Views on Designing Complex Architectures. (VODCA)

The 27 submissions and 11 published papers of this first ISARCS instance in 2010 show that we brought together as planned expertise from the different communities and therefore were able to provide a first overarching view on the state of research on how to design, develop, deploy and evolve critical systems from the architectural perspective.

The selected papers addressed issues such as rigorous development, testing and analysis based on architecture, fault tolerance based on the architecture, safety-critical systems and architecture, secure systems and architecture, combined approaches and industrial needs.

In the symposium the design of critical systems was addressed looking at issues such as analyzing the trade-offs between security and performance, architectural design decisions for achieving reliable software systems, and the integration of fault-tolerance techniques into the design of critical systems. In addition, also more rigorous approaches to design were discussed.

The assurance of critical systems was discussed for approaches that employ formal methods and testing for applications as well as underlying software layers. In addition, a number of results that target specific domains such as military systems, safety-critical product lines and peer-to-peer control and data acquisition systems were presented. These papers provided a good introduction into the specific requirements of these domains and presented specific solutions for their domain. Furthermore, the interplay of architecture modeling and existing domain-specific safety standards was discussed in the context of automotive systems.

The program was completed by two keynotes that were shared with the other events of the federated CompArch conference. The first one was on a component-based approach for adaptive user-centric pervasive applications from Martin Wirsing from the Ludwig-Maximilians-Universität Munich, Germany, and the second addressed how to make the definition of evolution intrinsic to architecture descriptions, by Jeff Magee from the Imperial College, London, UK.

I thank the authors of all submitted papers, and the PC members and external referees who provided excellent reviews. I am in particular grateful to Frantisek Plasil and the whole team in Prague as well as Stefan Neumann and Edgar Nähter for their help and support concerning organizational issues. I furthermore thank the ISARCS SC members for their support throughout the whole process and their strong commitment to making ISARCS 2010 a success.

April 2010 Holger Giese

Organization

ISARCS 2010 was organized by the Faculty of Mathematics and Physics of the Charles University, Prague, Czech Republic as one event of the federated conference Component-Based Software Engineering and Software Architecture (CompArch 2010).

General Chair

Frantisek Plasil	Charles University, Prague, Czech Republic

Program Chair

Holger Giese	Hasso Plattner Institute at the University of Potsdam, Germany

Local Organization

Petr Hnětynka	Charles University, Prague, Czech Republic
Milena Zeithamlova	Action M Agency, Prague, Czech Republic

Steering Committee

Rogério de Lemos	University of Coimbra, Portugal)
Cristina Gacek	City University, London, UK
Fabio Gadducci	University of Pisa, Italy
Lars Grunske	Swinburne University of Technology, Australia
Henry Muccini	University of L'Aquila, Italy
Maurice ter Beek	ISTI-CNR, Pisa, Italy

Program Committee

Alessandro Aldini	University of Urbino, Italy
Aslan Askarov	Cornell University, USA
Brian Berenbach	Siemens Corporate Research, USA
Stefano Bistarelli	Università di Perugia, Italy
Michel R.V. Chaudron	Leiden University, The Netherlands
Betty H. C.Cheng	Michigan State University, USA
Nathan Clarke	University of Plymouth, UK
Ricardo Corin	Universidad Nacional de Cordoba (FAMAF), Argentina

Cas Cremers	ETH Zurich, Switzerland
Ivica Crnkovic	Mälardalen University, Sweden
Bojan Cukic	West Virginia University, USA
Eric Dashofy	The Aerospace Corporation, USA
Erik de Vink	Eindhoven University of Technology, The Netherlands
Heiko Dörr	Carmeq GmbH, Germany
Alexander Egyed	Johannes Kepler University, Austria
Sébastien Gérard	CEA LIST, France
Wolfgang Grieskamp	Microsoft Corporation, USA
Ethan Hadar	CA Inc., Israel
Paola Inverardi	University of L'Aquila, Italy
Valérie Issarny	INRIA, UR de Rocquencourt, France
Tim Kelly	University of York, UK
Marc-Olivier Killijian	LAAS-CNRS Toulouse, France
Philip Koopman	Carnegie Mellon University, USA
Patricia Lago	VU University Amsterdam, The Netherlands
Javier Lopez	University of Malaga, Spain
Nenad Medvidovic	University of Southern California, USA
Flavio Oquendo	European University of Brittany - UBS/VALORIA, France
Mauro Pezzè	University of Lugano, Switzerland
Ralf H. Reussner	Karlsruhe Institute of Technology / FZI, Germany
Roshanak Roshandel	Seattle University, USA
Ana-Elena Rugina	Astrium Satellites, France
Bradley Schmerl	Carnegie Mellon University, USA
Bran Selic	Malina Software, Canada
Judith Stafford	Tufts University, USA
Michael von der Beeck	BMW Group, Germany

External Referees

Rogério de Lemos
Lars Grunske
Aaron Kane
Giovanni Mainetto
Mohamad Reza Mousavi
Henry Muccini
Marinella Petrocchi
Justin Ray
Francesco Santini
Malcolm Taylor
Maurice H. ter Beek

Table of Contents

Design

Verification and Validation

Domain-Specific Results

Standards