

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, 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, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7408>

Jürgen Großmann · Michael Felderer
Fredrik Seehusen (Eds.)

Risk Assessment and Risk-Driven Quality Assurance

4th International Workshop, RISK 2016
Held in Conjunction with ICTSS 2016
Graz, Austria, October 18, 2016
Revised Selected Papers

Editors

Jürgen Großmann
Fraunhofer FOKUS CC SQC
Berlin
Germany

Fredrik Seehusen
SINTEF ICT
Oslo
Norway

Michael Felderer
Department of Computer Science
Universität Innsbruck
Innsbruck
Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-57857-6 ISBN 978-3-319-57858-3 (eBook)
DOI 10.1007/978-3-319-57858-3

Library of Congress Control Number: 2017938161

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Increased connectivity and software complexity lead to an ever-growing demand for techniques to ensure software quality, dependability, reliability, and security. The risks that software systems do not meet their intended level of quality can have a severe impact on vendors, customers, and even society at large. The precise understanding of risks has become one of the cornerstones of critical decision-making within complex social and technical environments.

Traditional approaches for ensuring system quality address risk implicitly rather than systematically. However, there is a growing interest in enhancing traditional approaches for ensuring system quality by taking risk systematically into account. For instance, in traditional test approaches, test planning and prioritization are often based on an implicit notion of risk; systems, functions, or modules, which are known to be critical, are tested more intensively than others. However, taking risk systematically into account allows for a more rigorous prioritization process that is better documented, less dependent on human guesswork, and more easily supported by tools.

The RISK Workshop series has emerged as a high-profile series of events that discusses innovative work in the areas of software risk assessment, testing, and the combination thereof. We have been able to look back on four successful years, in which we have been involved in different conferences and initiated a fruitful exchange between scientists from academia as well as from industry.

This volume contains the proceedings of the 4th International Workshop on Risk Assessment and Risk-Driven Quality Assurance (RISK 2016) held in October 2016 in Graz, Austria, in conjunction with the 28th International Conference on Testing Software and Systems (ICTSS). RISK 2016 brought together researchers from Europe who study, develop, and evaluate innovative techniques, tools, languages, and methods for risk assessment and risk-driven quality engineering. During the workshop, the participants discussed 11 peer-reviewed contributions tackling challenges of assessing and managing safety, security, and reliability risk, and in particular the intersection between these areas. The workshop was structured into three sessions on Security Risk Management, Security Risk Analysis as well as Risk-Based Testing.

We would like to take this opportunity to thank the people who have contributed to the RISK 2016 workshop and helped make it a success. We want to thank all authors and reviewers for their valuable contributions, and we wish them a successful continuation of their work in this area.

March 2017

Jürgen Großmann
Michael Felderer
Fredrik Seehusen

Organization

RISK 2016 was organized by Fraunhofer FOKUS, SINTEF Digital, and the University of Innsbruck.

Organizing Committee

Jürgen Großmann	Fraunhofer FOKUS, Germany
Michael Felderer	University of Innsbruck, Austria
Fredrik Seehusen	SINTEF Digital, Norway

Program Committee

Jürgen Großmann	Fraunhofer FOKUS, Germany
Fredrik Seehusen	SINTEF Digital, Norway
Michael Felderer	University of Innsbruck, Austria
Ina Schieferdecker	TU Berlin/Fraunhofer FOKUS, Germany
Ketil Stølen	SINTEF Digital, Norway
Ruth Breu	University of Innsbruck, Austria
Ron Kenett	KPA Ltd. and University of Turin, Italy
Sardar Muhammad Sulaman	Lund University, Sweden
Markus Schacher	KnowGravity Inc., Switzerland
Alessandra Bagnato	Softeam, France
Kenji Taguchi	AIST, Japan
Zhen Ru Dai	University of Applied Science Hamburg, Germany
Per Håkon Meland	SINTEF Digital, Norway
Luca Compagna	SAP Labs, France
Jörn Eichler	Fraunhofer AISEC, Germany
Bruno Legeard	Femto-ST, France
Xiaoying Bai	Tsinghua University, China

Contents

Security Risk Management

Business Driven ICT Risk Management in the Banking Domain with RACOMAT	3
<i>Johannes Viehmann</i>	
Towards Transparent Real-Time Privacy Risk Assessment of Intelligent Transport Systems.	11
<i>Gencer Erdogan, Aida Omerovic, Marit K. Natvig, and Isabelle C.R. Tardy</i>	
Check Your Blind Spot: A New Cyber-Security Metric for Measuring Incident Response Readiness	19
<i>Benjamin Aziz, Ali Malik, and Jeyong Jung</i>	

Security Risk Analysis

Quantitative Information Security Risk Estimation Using Probabilistic Attack Graphs	37
<i>Pontus Johnson, Alexandre Vernotte, Dan Gorton, Mathias Ekstedt, and Robert Lagerström</i>	
Fast and Optimal Countermeasure Selection for Attack Defence Trees.	53
<i>Steve Muller, Carlo Harpes, and Cédric Muller</i>	
An Assessment of Security Analysis Tools for Cyber-Physical Systems.	66
<i>Laurens Lemaire, Jan Vossaert, Bart De Decker, and Vincent Naessens</i>	
Supporting Risk Assessment with the Systematic Identification, Merging, and Validation of Security Goals.	82
<i>Daniel Angermeier, Alexander Nieding, and Jörn Eichler</i>	

Risk-Based Testing

Design Decisions in the Development of a Graphical Language for Risk-Driven Security Testing.	99
<i>Gencer Erdogan and Ketil Stølen</i>	
A Lightweight Approach for Estimating Probability in Risk-Based Software Testing.	115
<i>Rudolf Ramler, Michael Felderer, and Matthias Leitner</i>	

Gaining Certainty About Uncertainty: Testing Cyber-Physical Systems
in the Presence of Uncertainties at the Application Level 129
Martin A. Schneider, Marc-Florian Wendland, and Leon Bornemann

Risk Management During Software Development: Results of a Survey
in Software Houses from Germany, Austria and Switzerland 143
Michael Felderer, Florian Auer, and Johannes Bergsmann

Author Index 157