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

Springer
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
   Johannes Viehmann

Towards Transparent Real-Time Privacy Risk Assessment of Intelligent
Transport Systems ............................................................ 11
   Gencer Erdogan, Aida Omerovic, Marit K. Natvig,
   and Isabelle C.R. Tardy

Check Your Blind Spot: A New Cyber-Security Metric for Measuring
Incident Response Readiness ............................................ 19
   Benjamin Aziz, Ali Malik, and Jeyong Jung

Security Risk Analysis

Quantitative Information Security Risk Estimation Using Probabilistic
Attack Graphs ................................................................. 37
   Pontus Johnson, Alexandre Vernotte, Dan Gorton, Mathias Ekstedt,
   and Robert Lagerström

Fast and Optimal Countermeasure Selection for Attack Defence Trees ...... 53
   Steve Muller, Carlo Harpes, and Cédric Muller

An Assessment of Security Analysis Tools for Cyber-Physical Systems ...... 66
   Laurens Lemaire, Jan Vossaert, Bart De Decker, and Vincent Naessens

Supporting Risk Assessment with the Systematic Identification, Merging,
and Validation of Security Goals ........................................ 82
   Daniel Angermeier, Alexander Nieding, and Jörn Eichler

Risk-Based Testing

Design Decisions in the Development of a Graphical Language
for Risk-Driven Security Testing ......................................... 99
   Gencer Erdogan and Ketil Stølen

A Lightweight Approach for Estimating Probability in Risk-Based
Software Testing .............................................................. 115
   Rudolf Ramler, Michael Felderer, and Matthias Leitner
<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaining Certainty About Uncertainty: Testing Cyber-Physical Systems</td>
<td>129</td>
</tr>
<tr>
<td>in the Presence of Uncertainties at the Application Level</td>
<td></td>
</tr>
<tr>
<td><em>Martin A. Schneider, Marc-Florian Wendland, and Leon Bornemann</em></td>
<td></td>
</tr>
<tr>
<td>Risk Management During Software Development: Results of a Survey in</td>
<td>143</td>
</tr>
<tr>
<td>Software Houses from Germany, Austria and Switzerland</td>
<td></td>
</tr>
<tr>
<td><em>Michael Felderer, Florian Auer, and Johannes Bergsmann</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>157</td>
</tr>
</tbody>
</table>