Table of Contents

Message from the General Chairs.............................................................................................................ix
Message from the Program Chairs............................................................................................................x
Organizing Committee................................................................................................................................xi
Program Committee...................................................................................................................................xii
Additional Reviewers................................................................................................................................xiv
Steering Committee...................................................................................................................................xv

Session 1A: Security I
Using Attack Surface Entry Points and Reachability Analysis to Assess the Risk of Software Vulnerability Exploitation .........................................................................................................................1
   Awad A. Younis, Yashwant K. Malaiya, and Indrajit Ray
Leveraging Variations in Event Sequences in Keystroke-Dynamics Authentication Systems ............................................................9
   Zahid Syed, Sean Banerjee, and Bojan Cukic
A Model-Based Intrusion Detection System for Smart Meters .................................................................................17
   Farid Molazem Tabrizi and Karthik Pattabiraman

Session 1B: Fault Analysis
Evaluating Distortion in Fault Injection Experiments ............................................................................................25
   Erik van der Kouwe, Cristiano Giuffrida, and Andrew S. Tanenbaum
A Practitioner’s Guide to Software-Based Soft-Error Mitigation Using AN-Codes ...............................................................33
   Martin Hoffmann, Peter Ulbrich, Christian Dietrich, Horst Schirmeier,
   Daniel Lohmann, and Wolfgang Schröder-Preikschat
ArCMAPE: A Software Product Line Infrastructure to Support Fault-Tolerant Composite Services ....................................................41
   Amanda S. Nascimento, Cecília M.F. Rubira, and Fernando Castor
Session 2A: Testing I

Fail-Safe Test Generation in Safety Critical Systems ..........................................................49
   Anneliese Andrews, Salwa Elakeili, and Salah Boukhris

Making an ALARP Decision of Sufficient Testing .............................................................57
   Mahnaz Malekzadeh and Iain Bate

Combinatorial Test Generation for Software Product Lines Using Minimum Invalid Tuples ..........................................................65
   Linbin Yu, Feng Duan, Yu Lei, Raghu N. Kacker, and D. Richard Kuhn

Session 2B: Formal Methods

Modeling and Verification of Humanoid Robot Task Coordination ....................................73
   Yujian Fu and Steven Drager

Temporal Verification of Simulink Diagrams ........................................................................81
   Jiri Barnat, Petr Bauch, and Vojtech Havel

Proving the Fidelity of Simulations of Event-B Models .....................................................89
   Faqing Yang, Jean-Pierre Jacquot, and Jeanine Souquières

Session 3A: Reliability

A Novel Framework of Software Reliability Evaluation with Software Reliability Growth Models and Software Metrics ..........................................................97
   Hiroyuki Okamura and Tadashi Dohi

Towards Comprehensive Modeling of Reliability for Smart Grids: Requirements and Challenges ..........................................................105
   Koosha Marashi and Sahra Sedigh Sarvestani

An Empirical Failure-Analysis of a Large-Scale Cloud Computing Environment ..............113
   Peter Garraghan, Paul Townend, and Jie Xu

Session 3B: Safety

Assuring Safety for Component Based Software Engineering ..........................................121
   Philippa Conmy and Iain Bate

Analysis of Critical Systems Certification .........................................................................129
   Panayiotis Steele and John Knight

Using Program Transformation, Annotation, and Reflection to Certify a Java Type Resolution Function ..........................................................137
   Victor L. Winter, Carl Reinke, and Jonathan Guerrero
### Session 4A: Invited Paper Session

Policy-Driven High Assurance Cyber Infrastructure-Based Systems ..................................................146  
*Abdulrahman Almutairi, Tawfeeq A. Shawly, Saleh M. Basalamah, and Arif Ghafoor*

Autonomous Decentralized High-Assurance Surveillance System for Air Traffic Control ..........................................................154  
*Tadashi Koga, Xiaodong Lu, and Kinji Mori*

Mobile Testing-as-a-Service (MTaaS) -- Infrastructures, Issues, Solutions and Needs ..........................................................158  
*Jerry Gao, Wei-Tek Tsai, Ray Paul, Xiaoying Bai, and Tadahiro Uehara*

### Session 4B: Testing II

UML-Based Modeling of Robustness Testing ..........................................................168  
*Regina Moraes, Hélène Waeselynck, and Jérémie Guiochet*

Testing of Memory Leak in Android Applications ..........................................................176  
*Hossain Shahrriar, Sarah North, and Edward Mawangi*

Trade-Off Analysis for Selective versus Brute-Force Regression Testing in FSMWeb ..........................................................184  
*Anneliese Andrews and Hyunsook Do*

### Session 5A: Security II

Hardware Implementation of Secure Shamir's Secret Sharing Scheme ..............................................193  
*Pei Luo, Andy Yu-Lun Lin, Zhen Wang, and Mark Karpovsky*

Security Driven Requirements Refinement and Exploration of Architecture with Multiple NFR Points of View ..........................................................201  
*Takao Okubo, Nobukazu Yoshioka, and Haruhiko Kaiya*

Clicksafe: Providing Security against Clickjacking Attacks ......................................................206  
*Jawwad A. Shamsi, Sufian Hameed, Waleed Rahman, Farooq Zuberi, Kaiser Altf, and Ammar Amjad*

Proactive Model-Based Performance Analysis and Security Tradeoffs in a Complex System ..........................................................211  
*Jesse Musgrove, Bojan Cukic, and Vittorio Cortellessa*

### Session 5B: Failure Analysis

On the Need for Training Failure Prediction Algorithms in Evolving Software Systems ..........................................................216  
*Ivano Irrera, Joao Duraes, and Marco Vieira*

Adaptive Testing of Nondeterministic Systems with FSM ......................................................224  
*Alexandre Petrenko and Nina Yevtushenko*
Verifying the Precedence Property Pattern Using the B Method .................................................. 229
   *Amel Mammar and Marc Frappier*

Using Flash to Tolerate Track Failures in RAID ................................................................. 234
   *Zheng Chen and Allen McBride*

**Session 6A: Privacy and Safety**

PriDaC: Privacy Preserving Data Collection in Sensor Enabled RFID Based Healthcare Services ............................................................... 236
   *Farzana Rahman, Drew Williams, Sheikh I. Ahamed, Ji-Jiang Yang, and Qing Wang*

Recommender Systems for Privacy Management: A Framework .................................................. 243
   *Curtis Rasmussen and Rozita Dara*

On the Nature and Content of Safety Contracts ...................................................................... 245
   *Patrick Graydon and Iain Bate*

Functional Alarms for Systems of Interoperable Medical Devices ........................................... 247
   *Krishna K. Venkatasubramanian, Eugene Y. Vasserman, Oleg Sokolsky, and Insup Lee*

**Session 6B: Model Analysis**

Inferring Approximated Models for Systems Engineering ....................................................... 249
   *Alexandre Petrenko, Keqin Li, Roland Groz, Karim Hossen, and Catherine Oriat*

Zero-Knowledge Evaluation of Service Performance Based on Simulation .............................. 254
   *Claudio A. Ardagna, Ernesto Damiani, Kouessi A.R. Sagbo, and Fulvio Frati*

Ordering Upgrade Changes for Highly Available Component Based Systems .......................... 259
   *Ali Davoudian, Ferhat Khendek, and Maria Toeroe*

Modeling the Interaction of Power Line and SCADA Networks ............................................. 261
   *Yuki Matsui, Hideharu Kojima, and Tatsuhiro Tsuchiya*

**Author Index** ........................................................................................................................ 263