

2014 IEEE 15th International Symposium on High-Assurance Systems Engineering

(HASE 2014)

**Miami Beach, Florida, USA
9 – 11 January 2014**



**IEEE Catalog Number: CFP14072-POD
ISBN: 978-1-4799-3467-6**

2014 IEEE 15th International Symposium on High-Assurance Systems Engineering

HASE 2014

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 Exploitability	1
<i>Awad A. Younis, Yashwant K. Malaiya, and Indrajit Ray</i>	
Leveraging Variations in Event Sequences in Keystroke-Dynamics Authentication Systems	9
<i>Zahid Syed, Sean Banerjee, and Bojan Cukic</i>	
A Model-Based Intrusion Detection System for Smart Meters	17
<i>Farid Molazem Tabrizi and Karthik Pattabiraman</i>	

Session 1B: Fault Analysis

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

Session 2A: Testing I

Fail-Safe Test Generation in Safety Critical Systems	49
<i>Anneliese Andrews, Salwa Elakeili, and Salah Boukhris</i>	
Making an ALARP Decision of Sufficient Testing	57
<i>Mahnaz Malekzadeh and Iain Bate</i>	
Combinatorial Test Generation for Software Product Lines Using Minimum Invalid Tuples	65
<i>Linbin Yu, Feng Duan, Yu Lei, Raghu N. Kacker, and D. Richard Kuhn</i>	

Session 2B: Formal Methods

Modeling and Verification of Humanoid Robot Task Coordination	73
<i>Yujian Fu and Steven Drager</i>	
Temporal Verification of Simulink Diagrams	81
<i>Jiri Barnat, Petr Bauch, and Vojtech Havel</i>	
Proving the Fidelity of Simulations of Event-B Models	89
<i>Faqing Yang, Jean-Pierre Jacquot, and Jeanine Souquières</i>	

Session 3A: Reliability

A Novel Framework of Software Reliability Evaluation with Software Reliability Growth Models and Software Metrics	97
<i>Hiroyuki Okamura and Tadashi Dohi</i>	
Towards Comprehensive Modeling of Reliability for Smart Grids: Requirements and Challenges	105
<i>Koosha Marashi and Sahra Sedigh Sarvestani</i>	
An Empirical Failure-Analysis of a Large-Scale Cloud Computing Environment	113
<i>Peter Garraghan, Paul Townend, and Jie Xu</i>	

Session 3B: Safety

Assuring Safety for Component Based Software Engineering	121
<i>Philippa Conmy and Iain Bate</i>	
Analysis of Critical Systems Certification	129
<i>Panayiotis Steele and John Knight</i>	
Using Program Transformation, Annotation, and Reflection to Certify a Java Type Resolution Function	137
<i>Victor L. Winter, Carl Reinke, and Jonathan Guerrero</i>	

Session 4A: Invited Paper Session

Policy-Driven High Assurance Cyber Infrastructure-Based Systems	146
<i>Abdulrahman Almutairi, Tawfeeq A. Shawly, Saleh M. Basalamah, and Arif Ghafoor</i>	
Autonomous Decentralized High-Assurance Surveillance System for Air Traffic Control	154
<i>Tadashi Koga, Xiaodong Lu, and Kinji Mori</i>	
Mobile Testing-as-a-Service (MTaaS) -- Infrastructures, Issues, Solutions and Needs	158
<i>Jerry Gao, Wei-Tek Tsai, Ray Paul, Xiaoying Bai, and Tadahiro Uehara</i>	

Session 4B: Testing II

UML-Based Modeling of Robustness Testing	168
<i>Regina Moraes, H�el�ene Waeselynck, and J�er�emie Guiochet</i>	
Testing of Memory Leak in Android Applications	176
<i>Hossain Shahriar, Sarah North, and Edward Mawangi</i>	
Trade-Off Analysis for Selective versus Brute-Force Regression Testing in FSMWeb	184
<i>Anneliese Andrews and Hyunsook Do</i>	

Session 5A: Security II

Hardware Implementation of Secure Shamir's Secret Sharing Scheme	193
<i>Pei Luo, Andy Yu-Lun Lin, Zhen Wang, and Mark Karpovsky</i>	
Security Driven Requirements Refinement and Exploration of Architecture with Multiple NFR Points of View	201
<i>Takao Okubo, Nobukazu Yoshioka, and Haruhiko Kaiya</i>	
Clicksafe: Providing Security against Clickjacking Attacks	206
<i>Jawwad A. Shamsi, Sufian Hameed, Waleed Rahman, Farooq Zuberi, Kaiser Altaf, and Ammar Amjad</i>	
Proactive Model-Based Performance Analysis and Security Tradeoffs in a Complex System	211
<i>Jesse Musgrove, Bojan Cukic, and Vittorio Cortellessa</i>	

Session 5B: Failure Analysis

On the Need for Training Failure Prediction Algorithms in Evolving Software Systems	216
<i>Ivano Irrera, Joao Duraes, and Marco Vieira</i>	
Adaptive Testing of Nondeterministic Systems with FSM	224
<i>Alexandre Petrenko and Nina Yevtushenko</i>	

Verifying the Precedence Property Pattern Using the B Method	229
<i>Amel Mammam and Marc Frappier</i>	

Using Flash to Tolerate Track Failures in RAID	234
<i>Zheng Chen and Allen McBride</i>	

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
<i>Curtis Rasmussen and Rozita Dara</i>	

On the Nature and Content of Safety Contracts	245
<i>Patrick Graydon and Iain Bate</i>	

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

Session 6B: Model Analysis

Inferring Approximated Models for Systems Engineering	249
<i>Alexandre Petrenko, Keqin Li, Roland Groz, Karim Hossen, and Catherine Oriat</i>	

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

Ordering Upgrade Changes for Highly Available Component Based Systems	259
<i>Ali Davoudian, Ferhat Khendek, and Maria Toeroe</i>	

Modeling the Interaction of Power Line and SCADA Networks	261
<i>Yuki Matsui, Hideharu Kojima, and Tatsuhiro Tsuchiya</i>	

Author Index	263
---------------------------	-----