

# **2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE 2016)**

**Orlando, Florida, USA  
7-9 January 2016**



**IEEE Catalog Number: CFP16072-POD  
ISBN: 978-1-4673-9914-2**

**Copyright © 2016 by the Institute of Electrical and Electronic Engineers, Inc  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\*This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16072-POD
ISBN (Print-On-Demand):	978-1-4673-9914-2
ISBN (Online):	978-1-4673-9913-5
ISSN:	1530-2059

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2016 IEEE 17th International Symposium on High Assurance Systems Engineering

## HASE 2016

### Table of Contents

A Word from the General Chairs.....	x
Message from the Program Chairs.....	xi
Organizing Committee.....	xii
Program Committee.....	xiii
Additional Reviewers.....	xvi

---

#### Session 1A: Cybersecurity I

Game Theory with Learning for Cyber Security Monitoring .....	1
<i>Keywhan Chung, Charles A. Kamhoua, Kevin A. Kwiat, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer</i>	
Empirical Techniques to Detect and Mitigate the Effects of Irrevocably Evolving User Profiles in Touch-Based Authentication Systems .....	9
<i>Nikhil Palaskar, Zahid Syed, Sean Banerjee, and Charlotte Tang</i>	
Design Diversity for Mitigating Monoculture Induced Threats .....	17
<i>Qi Cheng, Kevin Kwiat, and Charles A. Kamhoua</i>	
Securing a Connected Mobile System for Healthcare .....	19
<i>Eric Reinsmidt, David Schwab, and Li Yang</i>	

#### Session 1B: Adaptive Systems

Using Models to Validate Unanticipated, Fine-Grained Adaptations at Runtime .....	23
<i>Mohammed Al-Refai, Walter Cazzola, Sudipto Ghosh, and Robert France</i>	
Correct Instantiation of a System Reconfiguration Pattern: A Proof and Refinement-Based Approach .....	31
<i>Guillaume Babin, Yamine Ait-Ameur, and Marc Pantel</i>	
The Cost of Formal Verification in Adaptive CPS. An Example of a Virtualized Server Node .....	39
<i>Marcello M. Bersani and Marisol García-Valls</i>	

## **Session 2A: Testing and Quality Assurance**

An Extension of Category Partition Testing for Highly Constrained Systems .....	47
<i>Sunint Kaur Khalsa and Yvan Labiche</i>	
Software Defect Prediction Using Exception Handling Call Graphs: A Case Study .....	55
<i>Puntitra Sawadpong and Edward B. Allen</i>	
Task Characterization for an Effective Worker Targeting in Crowdsourcing .....	63
<i>Tarek Awwad, Nadia Bennani, Lionel Brunie, David Coquil, Harald Kosch, and Veronika Rehn-Sonigo</i>	
World Model for Testing Autonomous Systems Using Petri Nets .....	65
<i>Anneliese Andrews, Mahmoud Abdelgawad, and Ahmed Gario</i>	

## **Session 2B: Safety-Critical Systems**

Formal Analysis of Railway Signalling Data .....	70
<i>Alexei Iliasov and Alexander Romanovsky</i>	
Safe Multi-objective Planning with a Posteriori Preferences .....	78
<i>Ralph Eastwood, Rob Alexander, and Tim Kelly</i>	
Representation of Confidence in Assurance Cases Using the Beta Distribution .....	86
<i>Lian Duan, Sanjai Rayadurgam, Mats Heimdahl, Oleg Sokolsky, and Insup Lee</i>	

## **Session 3A: System Resilience and Survivability**

Engineering Adaptive Fault-Tolerance Mechanisms for Resilient Computing on ROS .....	94
<i>Michael Lauer, Matthieu Amy, Jean-Charles Fabre, Matthieu Roy, William Excoffon, and Miruna Stoicescu</i>	
Runtime Adjustment of Configuration Models for Consistency Preservation .....	102
<i>Azadeh Jahanbanifar, Ferhat Khendek, and Maria Toeroe</i>	
CSRS: Cyber Survive and Recover Simulator .....	110
<i>Swastik Brahma, Kevin Kwiat, Pramod K. Varshney, and Charles A. Kamhoua</i>	

## **Session 3B: Software Analysis**

Synthesis of Logic Interpretations .....	114
<i>Jian Xiang, John Knight, and Kevin Sullivan</i>	
Feature-Based Software Customization: Preliminary Analysis, Formalization, and Methods .....	122
<i>Yufei Jiang, Can Zhang, Dinghao Wu, and Peng Liu</i>	
Comparative Modeling and Verification of Pthreads and Dthreads .....	132
<i>Yuan Fei, Huibiao Zhu, Xi Wu, and Huixing Fang</i>	

## **Session 4A: Cybersecurity II**

An Investigation into the Response of a Water Treatment System to Cyber Attacks .....	141
<i>Sridhar Adepur and Aditya Mathur</i>	
Characterization of Cyberattacks Aimed at Integrated Industrial Control and Enterprise Systems: A Case Study .....	149
<i>Raymond C. Borges Hink and Katerina Goseva-Popstojanova</i>	
FCFraud: Fighting Click-Fraud from the User Side .....	157
<i>Md. Shahrear Iqbal, Md. Zulkernine, Fehmi Jaafar, and Yuan Gu</i>	

## **Session 4B: Formal Development**

Formalisation-Driven Development of Safety-Critical Systems .....	165
<i>Alexei Iliasov, Alexander Romanovsky, Elena Troubitsyna, and Linas Laibinis</i>	
Formal Development of a Secure Access Control Filter .....	173
<i>Amel Mammur, Thi Mai Nguyen, and Régine Laleau</i>	
Incremental Formal Methods Based Design Approach Demonstrated on a Coupled Tanks Control System .....	181
<i>Kerianne H. Gross, Aaron W. Ficarek, and Jonathan A. Hoffman</i>	

## **Session 5A: Analysis of Design Models**

Proving Critical Properties of Simulink Models .....	189
<i>Ashlie B. Hocking, M. Anthony Aiello, John C. Knight, and Nikos Aréchiga</i>	
Statistical Model Checking for SystemC Models .....	197
<i>Van Chan Ngo, Axel Legay, and Jean Quilbeuf</i>	
Compositional Architecture Design for Fuel Tank Thermal Systems .....	205
<i>Sean J. S. Regisford, Brian K. Hulbert, and Aaron W. Ficarek</i>	

## **Session 5B: Networked Systems**

Using Network Topology to Supplement High Assurance Systems .....	213
<i>Paul Hyden, Ira S. Moskowitz, and Stephen Russell</i>	
Integrating a Calculus with Mobility and Quality for Wireless Sensor Networks .....	220
<i>Xi Wu, Yongxin Zhao, and Huibiao Zhu</i>	
Presenting the Proper Data to the Crisis Management Operator: A Relevance Labelling Strategy .....	228
<i>Tommaso Zoppi, Andrea Ceccarelli, Paolo Lollini, Andrea Bondavalli, Francesco Lo Piccolo, Gabriele Giunta, and Vito Morreale</i>	

## **Session 6A: Work in Progress – Software**

Modeling Negative User Stories is Risky Business .....	236
<i>Pankaj Kamthan and Nazlie Shahmir</i>	
High-Integrity Multitasking in SPARK: Static Detection of Data Races and Locking Cycles .....	238
<i>S. Tucker Taft, Florian Schanda, and Yannick Moy</i>	
Towards a MARTE Extension to Address Adaptation Mechanisms .....	240
<i>Mohamed Naija, Jean-Michel Bruel, and Samir Ben Ahmed</i>	

## **Session 6B: Work in Progress – System**

Model Checking for the Fault Tolerance of Collaborative AUVs .....	244
<i>Hong Liu, Tianyu Yang, and Jing Wang</i>	
An Analysis Platform for Execution-Based Model Generation .....	246
<i>Jaime C. Acosta and Salamah Salamah</i>	
Empirical Assessment of Methods to Detect Cyber Attacks on a Robot .....	248
<i>Giedre Sabaliauskaite, Geok See Ng, Justin Ruths, and Aditya P. Mathur</i>	

## **Session 7A: Cloud Services**

D <sup>2</sup> PS: A Dependable Data Provisioning Service in Multi-tenant Cloud Environment .....	252
<i>Renyu Yang, Tianyu Wo, Chunming Hu, Jie Xu, and Mingming Zhang</i>	
Generating Threat Profiles for Cloud Service Certification Systems .....	260
<i>Philipp Stephanow, Christian Banse, and Julian Schütte</i>	
CLOUBEX: A Cloud-Based Security Analysis Framework for Browser Extensions .....	268
<i>Saikat Das and Mohammad Zulkernine</i>	

## **Session 7B: Smart Grid and Cyber-Physical Systems**

A Holistic Viewpoint-Based SysML Profile to Design Systems-of-Systems .....	276
<i>Marco Mori, Andrea Ceccarelli, Paolo Lollini, Andrea Bondavalli, and Bernhard Frömel</i>	
Quantification of the Effectiveness of Medium Voltage Control Policies in Smart Grids .....	284
<i>Silvano Chiaradonna, Felicita Di Giandomenico, and Jun Xiao</i>	
Preventing and Unifying Threats in Cyberphysical Systems .....	292
<i>Eduardo B. Fernandez</i>	
High Assurance Smart Metering .....	294
<i>Sara Cleemput, Mustafa A. Mustafa, and Bart Preneel</i>	

**Author Index** .....298