

2016 IEEE/ACM 4th FME Workshop on Formal Methods in Software Engineering (FormaliSE 2016)

**Austin, Texas, USA
15 May 2016**



**IEEE Catalog Number: CFP16ZAP-POD
ISBN: 978-1-5090-2202-1**

**Copyright © 2016, Association for Computing Machinery
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:	CFP16ZAP-POD
ISBN (Print-On-Demand):	978-1-5090-2202-1
ISBN (Online):	978-1-4503-4159-2

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
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

4th FME Workshop on Formal Methods in Software Engineering (FormaliSE 2016)

Table of Contents

Message from the Workshop Chairs.....	vii
Committees and Reviewers	viii
Sponsors and Supporters	x

Session 1

Deductive Evaluation: Formal Code Analysis with Low User Burden	1
<i>Ben L. Di Vito</i>	
— NASA Langley Research Center, USA	

Session 2

Undertaking the Tokeneer Challenge in Event-B	8
<i>Víctor Rivera, Sukriti Bhattacharya, and Néstor Cataño</i>	
— Innopolis University, Russian Federation; University College London (UCL), United Kingdom	
Simple Synthesis of Reactive Systems with Tolerance for Unexpected Environmental Behavior	15
<i>Shigeki Hagihara, Atsushi Ueno, Takashi Tomita, Masaya Shimakawa,</i>	
<i>and Naoki Yonezaki</i>	
— Tokyo Institute of Technology, Japan; Japan Advanced Institute of Science and Technology, Japan	
Download Malware? No, Thanks. How Formal Methods Can Block Update Attacks	22
<i>Francesco Mercaldo, Vittoria Nardone, Antonella Santone, and Corrado Aaron Visaggio</i>	
— University of Sannio, Italy	
Validating Formal Specifications Using Testing-Based Specification Animation.....	29
<i>Shaoying Liu</i>	
— Hosei University, Japan	

Session 3

Towards Synthesis from Assume-Guarantee Contracts involving Infinite Theories: A Preliminary Report.....	36
<i>Andreas Katis, Andrew Gacek, and Michael W. Whalen</i>	
— University of Minnesota, USA; Rockwell Collins, USA	

Session 4

Toward Rigorous Design of Domain-Specific Distributed Systems	42
<i>Mohammed Al-Mahfoudh, Ganesh Gopalakrishnan, and Ryan Stutsman</i>	
<i>— The University of Utah, USA</i>	

Author Index	49
--------------------	----