

2020 IEEE/ACM 8th International Conference on Formal Methods in Software Engineering (FormalISE 2020)

**Seoul, South Korea
13 July 2020**



**IEEE Catalog Number: CFP20ZAP-POD
ISBN: 978-1-7281-9843-9**

**Copyright © 2020, Association for Computing Machinery (ACM)
All Rights Reserved**

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

IEEE Catalog Number:	CFP20ZAP-POD
ISBN (Print-On-Demand):	978-1-7281-9843-9
ISBN (Online):	978-1-4503-7071-4
ISSN:	2380-873X

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

2020 IEEE/ACM 8th International Conference on Formal Methods in Software Engineering (FormaliSE) **FormaliSE 2020**

Table of Contents

Message from General Chairs	vii
Organizing Committee	ix
Program Committee	x
Subreviewers	xi

Regular Papers

Active Learning of Decomposable Systems	1
<i>Omar al Duhaiby (Eindhoven University of Technology) and Jan Friso Grooten (Eindhoven University of Technology)</i>	
Formal Model-Based Assurance Cases in Isabelle/SACM: An Autonomous Underwater Vehicle Case Study	11
<i>Simon Foster (University of York, United Kingdom), Yakoub Nemouchi (University of York, United Kingdom), Colin O'Halloran (D-RisQ Software Systems, United Kingdom), Karen Stephenson (D-RisQ Software Systems, United Kingdom), and Nick Tudor (D-RisQ Software Systems, United Kingdom)</i>	
Haiq: Synthesis of Software Design Spaces with Structural and Probabilistic Guarantees	22
<i>Javier Camara (University of York)</i>	
Impact Analysis of Cyber-Physical Attacks on a Water Tank System via Statistical Model Checking	34
<i>Andrei Munteanu (University of Verona, Italy), Michele Pasqua (University of Verona, Italy), and Massimo Merro (University of Verona, Italy)</i>	
Lattice-Based Information Flow Control-by-Construction for Security-by-Design	44
<i>Tobias Runge (TU Braunschweig, Germany), Alexander Knüppel (TU Braunschweig, Germany), Thomas Thüm (University of Ulm, Germany), and Ina Schaefer (TU Braunschweig, Germany)</i>	
Mind the Gap: Robotic Mission Planning Meets Software Engineering	55
<i>Mehrnoosh Askarpour (Politecnico di Milano), Claudio Menghi (University of Luxembourg), Gabriele Belli (Alten), Marcello M. Bersani (Politecnico di Milano), and Patrizio Pelliccione (Chalmers, University of Gothenburg and University of L'Aquila)</i>	

Minimal Assumptions Refinement for Realizable Specifications	66
<i>Davide G. Cavezza (Imperial College London, United Kingdom), Dalal Alrajeh (Imperial College London, United Kingdom), and András György (DeepMind, United Kingdom)</i>	
Relational Test Tables: A Practical Specification Language for Evolution and Security	77
<i>Alexander Weigl (Karlsruhe Institute of Technology), Mattias Ulbrich (Karlsruhe Institute of Technology), Suhyun Cha (Technical University of Munich), Bernhard Beckert (Karlsruhe Institute of Technology), and Birgit Vogel-Heuser (Technical University of Munich)</i>	
Rule-Based Word Equation Solving	87
<i>Joel D. Day (Loughborough University, UK), Mitja Kulczynski (Kiel University, Germany), Florin Manea (University of Göttingen, Germany), Dirk Nowotka (Kiel University, Germany), and Danny Bøgsted Poulsen (Aalborg University, Denmark)</i>	
Security Verification of Industrial Control Systems Using Partial Model Checking	98
<i>Tomas Kulik (Aarhus University), Jalil Boudjadar (Aarhus University), and Peter W. V. Tran-Jørgensen (Aarhus University)</i>	
Semantic-Based Architecture Smell Analysis	109
<i>Nacha Chondamrongkul (University of Auckland), Jing Sun (University of Auckland), Ian Warren (University of Auckland), and Scott Uk-Jin Lee (University of Auckland)</i>	
Towards Formally Verified Key Management for Industrial Control Systems	119
<i>Tomas Kulik (Aarhus University), Jalil Boudjadar (Aarhus University), and Diego F. Aranha (Aarhus University)</i>	
UML Consistency Rules: A Case Study with Open-Source UML Models	130
<i>Damiano Torre (University of Luxembourg), Yvan Labiche (Carleton University), Marcela Genero (University of Castilla-La Mancha), Maged Elaasar (Carleton University), and Claudio Menghi (University of Luxembourg)</i>	
Verification of Privacy-Enhanced Collaborations	141
<i>Sara Belluccini (IMT Lucca School for Advanced Studies, Italy), Rocco De Nicola (IMT Lucca School for Advanced Studies, Italy), Marlon Dumas (University of Tartu, Estonia), Pille Pullonen (Cybernetica AS, Estonia), Barbara Re (University of Camerino, Italy), and Francesco Tiezzi (University of Camerino, Italy)</i>	
Author Index	153