Preface

The NASA Formal Methods (NFM) Symposium is a forum to foster collaboration between theoreticians and practitioners from NASA, academia, and industry, with the goal of identifying challenges and providing solutions to achieving assurance in mission- and safety-critical systems. Examples of such systems include advanced separation assurance algorithms for aircraft, next-generation air transportation, autonomous rendezvous and docking for spacecraft, autonomous on-board software for unmanned aerial systems (UAS), UAS traffic management, autonomous robots, and systems for fault detection, diagnosis, and prognostics. The topics covered by the NASA Formal Methods Symposia include:

- Formal verification, including theorem proving, model checking, and static analysis
- Advances in automated theorem proving including SAT and SMT solving
- Use of formal methods in software and system testing
- Run-time verification
- Techniques and algorithms for scaling formal methods such as abstraction and symbolic methods, compositional techniques, as well as parallel and/or distributed techniques
- Code generation from formally verified models
- Safety cases and system safety
- Formal approaches to fault tolerance
- Theoretical advances and empirical evaluations of formal methods techniques for safety-critical systems, including hybrid and embedded systems
- Formal methods in systems engineering and model-based development
- Formalization of mathematics and physics

This volume contains the papers presented at NFM 2018, the 10th NASA Formal Methods Symposium, held during April 17–19, 2018 in Newport News, VA. NFM 2018 celebrated 30 years of formal methods research at NASA. Previous symposia were held in Moffett Field, CA (2017), Minneapolis, MN (2016), Pasadena, CA (2015), Houston, TX (2014), Moffett Field, CA (2013), Norfolk, VA (2012), Pasadena, CA (2011), Washington, DC (2010), and Moffett Field, CA (2009). The series started as the Langley Formal Methods Workshop, and was held under that name in 1990, 1992, 1995, 1997, 2000, and 2008.

Papers were solicited for NFM 2018 under two categories: regular papers describing fully developed work and complete results, and short papers describing tools, experience reports, or work in progress with preliminary results. The symposium received 92 submissions for review out of which 31 were accepted for publication. These submissions went through a rigorous reviewing process, where each paper was first independently reviewed by at least three reviewers and then subsequently discussed by the Program Committee. In addition to the refereed papers, the symposium featured
two invited presentations, one by Rick Butler of NASA Langley Research Center, USA, and one by Gilles Dowek of Inria, CNRS, and ENS Cachan, France.

The organizers are grateful to the authors for submitting their work to NFM 2018 and to the invited speakers for sharing their insights. NFM 2018 would not have been possible without the collaboration of the outstanding Program Committee and additional reviewers, the support of the Steering Committee, the efforts of the staff at the NASA Langley Research Center, and the general support of the NASA Formal Methods community. The NFM 2018 website can be found at: https://shemesh.larc.nasa.gov/NFM2018.

April 2018

Aaron Dutle
César Muñoz
Anthony Narkawicz
## Organization

### Program Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erika Ábrahám</td>
<td>RWTH Aachen University, Germany</td>
</tr>
<tr>
<td>Mauricio Ayala-Rincon</td>
<td>Universidade de Brasilia, Brazil</td>
</tr>
<tr>
<td>Julia Badger</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Dirk Beyer</td>
<td>LMU Munich, Germany</td>
</tr>
<tr>
<td>Nikolaj Bjørner</td>
<td>Microsoft, USA</td>
</tr>
<tr>
<td>Jasmin Blanchette</td>
<td>Vrije Universiteit Amsterdam, The Netherlands</td>
</tr>
<tr>
<td>Sylvie Boldo</td>
<td>Inria, France</td>
</tr>
<tr>
<td>Kalou Cabrera Castillos</td>
<td>LAAS-CNRS, France</td>
</tr>
<tr>
<td>Misty Davies</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Catherine Dubois</td>
<td>ENSIIE-Samovar, France</td>
</tr>
<tr>
<td>Aaron Dutle</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Stefania Gnesi</td>
<td>ISTI-CNR, Italy</td>
</tr>
<tr>
<td>Alberto Griggio</td>
<td>Fondazione Bruno Kessler, Italy</td>
</tr>
<tr>
<td>George Hagen</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>John Harrison</td>
<td>Intel, USA</td>
</tr>
<tr>
<td>Klaus Havelund</td>
<td>NASA Jet Propulsion Laboratory, USA</td>
</tr>
<tr>
<td>Ashlie Hocking</td>
<td>Dependable Computing, USA</td>
</tr>
<tr>
<td>Susmit Jha</td>
<td>SRI International, USA</td>
</tr>
<tr>
<td>Rajeev Joshi</td>
<td>NASA Jet Propulsion Laboratory, USA</td>
</tr>
<tr>
<td>Laura Kovacs</td>
<td>Vienna University of Technology, Austria</td>
</tr>
<tr>
<td>Michael Lowry</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Panagiotis Manolios</td>
<td>Northeastern University, USA</td>
</tr>
<tr>
<td>Shaun McWherter</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>César Muñoz</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Anthony Narkawicz</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Natasha Neogi</td>
<td>NASA, USA</td>
</tr>
<tr>
<td>Lee Pike</td>
<td>Groq, USA</td>
</tr>
<tr>
<td>Murali Rangarajan</td>
<td>The Boeing Company, USA</td>
</tr>
<tr>
<td>Elvinia Riccobene</td>
<td>University of Milan, Italy</td>
</tr>
<tr>
<td>Camilo Rocha</td>
<td>Pontificia Universidad Javeriana Cali, Colombia</td>
</tr>
<tr>
<td>Kristin Yvonne Rozier</td>
<td>Iowa State University, USA</td>
</tr>
<tr>
<td>Sriram</td>
<td>University of Colorado Boulder, USA</td>
</tr>
<tr>
<td>Sankaranarayanan</td>
<td></td>
</tr>
<tr>
<td>Johann Schumann</td>
<td>SGT, USA</td>
</tr>
<tr>
<td>Konrad Slind</td>
<td>Rockwell Collins, USA</td>
</tr>
<tr>
<td>Cesare Tinelli</td>
<td>The University of Iowa, USA</td>
</tr>
<tr>
<td>Laura Titolo</td>
<td>National Institute of Aerospace, USA</td>
</tr>
</tbody>
</table>
Additional Reviewers

Alves, Vander         Katz, Guy
Arcaimi, Paolo        Kremer, Gereon
Basile, Davide        Lammich, Peter
Bozzano, Marco        Larraz, Daniel
Braghin, Chiara       Lemberger, Thomas
Brotherston, James    Li, Jianwen
Byun, Taejoon         Lüdtke, Daniel
Chakarov, Aleksandar  Marché, Claude
Champion, Adrien      Marechal, Alexandre
Chen, Xin             Mazzanti, Franco
Chowdhury, Omar       Meel, Kuldeep S.
Cohen, Cyril          Merz, Stephan
Cox, Arlen            Moscato, Mariano
Cruanes, Simon        Nantes-Sobrinho, Daniele
Dangl, Matthias       Nigam, Vivek
Dodds, Mike           Panizo, Laura
Dureja, Rohit         Paskevich, Andrei
Fainekos, Georgios    Pérez, Jorge A.
Fantechi, Alessandro  Ravitch, Tristian
Feliú Gabaldon, Marco Rioboo, Renaud
Ferrari, Alessio      Roveri, Marco
Fleury, Mathias       Schirmer, Sebastian
Fokkink, Wan          Schopferer, Simon
Friedberger, Karlheinz Schupp, Stefan
Gallois-Wong, Diane   Stewart, Danielle
Ghassabani, Elaheh    Strub, Pierre-Yves
Goodloe, Alwyn        Tian, Chun
Hoxha, Bardh          Traytel, Dmitriy
Hussein, Soha         Weaver, Sean
Jakobs, Marie-Christine Wendler, Philipp
Jones, Benjamin       Weps, Benjamin
Katís, Andreas
Contents

Incremental Construction of Realizable Choreographies .......................... 1
Sarah Benyagoub, Meriem Ouederni, Yamine Aït-Ameur,
and Atif Mashkoor

Formal Assurance for Cooperative Intelligent Autonomous Agents ........... 20
Siddhartha Bhattacharyya, Thomas C. Eskridge, Natasha A. Neogi,
Marco Carvalho, and Milton Stafford

Ghosts for Lists: A Critical Module of Contiki Verified in Frama-C ......... 37
Allan Blanchard, Nikolai Kosmatov, and Frédéric Loulergue

An Executable Formal Framework for Safety-Critical Human Multitasking. . 54
Giovanna Broccia, Paolo Milazzo, and Peter Csaba Ölveczky

Simpler Specifications and Easier Proofs of Distributed Algorithms
Using History Variables ........................................................................... 70
Saksham Chand and Yanhong A. Liu

Don’t Miss the End: Preventing Unsafe End-of-File Comparisons ............ 87
Charles Zhuo Chen and Werner Dietl

An Efficient Rewriting Framework for Trace Coverage
of Symmetric Systems ............................................................................. 95
Flavio M. De Paula, Arvind Haran, and Brad Bingham

Verification of Fault-Tolerant Protocols with Sally ............................... 113
Bruno Dutertre, Dejan Jovanović, and Jorge A. Navas

Output Range Analysis for Deep Feedforward Neural Networks ............ 121
Souradeep Dutta, Susmit Jha, Sriram Sankaranarayanan,
and Ashish Tiwari

Formal Dynamic Fault Trees Analysis Using an Integration
of Theorem Proving and Model Checking ................................................ 139
Yassmeen Elderhalli, Osman Hasan, Waqar Ahmad, and Sofiène Tahar

Twenty Percent and a Few Days – Optimising a Bitcoin Majority Attack. . . 157
Ansgar Fehnker and Kaylash Chaudhary

An Even Better Approach – Improving the B.A.T.M.A.N. Protocol
Through Formal Modelling and Analysis ................................................ 164
Ansgar Fehnker, Kaylash Chaudhary, and Vinay Mehta
Towards a Formal Safety Framework for Trajectories ................................. 179
  Marco A. Feliú and Mariano M. Moscato

Static Value Analysis of Python Programs by Abstract Interpretation ............. 185
  Aymeric Fromherz, Abdelraouf Ouadjaout, and Antoine Miné

Model-Based Testing for General Stochastic Time .................................. 203
  Marcus Gerhold, Arnd Hartmanns, and Mariëlle Stoelinga

Strategy Synthesis for Autonomous Agents Using PRISM ............................ 220
  Ruben Giaquinta, Ruth Hoffmann, Murray Ireland, Alice Miller,
  and Gethin Norman

The Use of Automated Theory Formation in Support of Hazard Analysis ........ 237
  Andrew Ireland, Maria Teresa Llano, and Simon Colton

Distributed Model Checking Using ProB .................................................. 244
  Philipp Körner and Jens Bendisposto

Optimal Storage of Combinatorial State Spaces ..................................... 261
  Alfons Laarman

Stubborn Transaction Reduction ......................................................... 280
  Alfons Laarman

Certified Foata Normalization for Generalized Traces .............................. 299
  Hendrik Maarand and Tarmo Uustalu

On the Timed Analysis of Big-Data Applications .................................. 315
  Francesco Marconi, Giovanni Quattrocchi, Luciano Baresi,
  Marcello M. Bersani, and Matteo Rossi

Tuning Permissiveness of Active Safety Monitors for Autonomous Systems ...... 333
  Lola Masson, Jérémie Guiochet, Hélène Waeselynck,
  Kalou Cabrera, Sofia Cassel, and Martin Törngren

Sound Black-Box Checking in the LearnLib ......................................... 349
  Jeroen Meijer and Jaco van de Pol

Model-Checking Task Parallel Programs for Data-Race ........................... 367
  Radha Nakade, Eric Mercer, Peter Aldous, and Jay McCarthy

Consistency of Property Specification Patterns with Boolean and Constrained
  Numerical Signals ............................................................................... 383
  Massimo Narizzano, Luca Pulina, Armando Tacchella,
  and Simone Vuotto
Automatic Generation of DO-178 Test Procedures

César Ochoa Escudero, Rémi Delmas, Thomas Bochot, Matthieu David, and Virginie Wiels

Using Test Ranges to Improve Symbolic Execution.

Rui Qiu, Sarfraz Khurshid, Corina S. Păsăreanu, Junye Wen, and Guowei Yang

Symbolic Execution and Reachability Analysis Using Rewriting Modulo SMT for Spatial Concurrent Constraint Systems with Extrusion

Miguel Romero and Camilo Rocha

Experience Report: Application of Falsification Methods on the UxAS System

Cumhur Erkan Tuncali, Bardh Hoxha, Guohui Ding, Georgios Fainekos, and Sriram Sankaranarayanan

MoDeS3: Model-Based Demonstrator for Smart and Safe Cyber-Physical Systems

András Vörös, Márton Búr, István Réth, Ákos Horváth, Zoltán Micskei, László Balogh, Bálint Hegyi, Benedek Horváth, Zsolt Mázló, and Dániel Varró

Author Index