Preface

This volume contains the papers presented at the Eleventh NASA Formal Methods (NFM) Symposium held on May 7-9, 2019 at Rice University in Houston, Texas, USA.

The widespread use and increasing complexity of mission-critical and safety-critical systems at NASA and in the aerospace industry require advanced techniques that address these systems' specification, design, verification, validation, and certification requirements. The NASA Formal Methods Symposium (NFM) is a forum to foster collaboration between theoreticians and practitioners from NASA, academia, and industry. NFM's goals are to identify challenges and to provide solutions for achieving assurance for such critical systems.

New developments and emerging applications like autonomous software for uncrewed deep space human habitats, caretaker robotics, Unmanned Aerial Systems (UAS), UAS Traffic Management (UTM), and the need for system-wide fault detection, diagnosis, and prognostics provide new challenges for system specification, development, and verification approaches. The focus of these symposiums are on formal techniques and other approaches for software assurance, including their theory, current capabilities and limitations, as well as their potential application to aerospace, robotics, and other NASA-relevant safety-critical systems during all stages of the software life-cycle.

The NASA Formal Methods Symposium is an annual event organized by the NASA Formal Methods (NFM) Steering Committee, comprised of researchers spanning several NASA centers. NFM 2019 was co-hosted by Rice University and NASA-Johnson Space Center in Houston, TX. It was organized by a collaboration between Rice, NASA JSC, and Iowa State University.

NFM was created to highlight the state of the art in formal methods, both in theory and in practice. The series is a spinoff of the original Langley Formal Methods Workshop (LFM). LFM was held six times in 1990, 1992, 1995, 1997, 2000, and 2008 near NASA Langley in Virginia, USA. The 2008 reprisal of LFM led to the expansion to a NASA-wide conference. In 2009 the first NASA Formal Methods Symposium was organized at NASA Ames Research Center in Moffett Field, CA. In 2010, the Symposium was organized by NASA Langley Research Center and NASA Goddard Space Flight Center, and held at NASA Headquarters in Washington, D.C. The third NFM symposium was organized by the Laboratory for Reliable Software at the NASA Jet Propulsion Laboratory/California Institute of Technology, and held in Pasadena, CA in 2011. NFM returned to NASA Langley Research Center in 2012 in nearby Norfolk, Virginia. NASA Ames Research Center organized and hosted NFM 2013, the fifth Symposium in the series. NFM 2014 was organized via a collaboration between NASA Goddard Space Flight Center, NASA Johnson Space Center, and NASA Ames Research Center, and held at JSC. NASA JPL hosted the seventh NFM in 2015 in Pasadena, CA. In 2016, the eighth NFM Symposium visited the University of Minnesota, hosted by a collaboration between academia and NASA. 2017 brought the ninth NFM back to NASA Ames Research Center. NASA Langley hosted NFM's 10th anniversary edition in 2018.

NFM 2019 encouraged submissions on cross-cutting approaches that bring together formal methods and techniques from other domains such as probabilistic reasoning, machine learning, control theory, robotics, and quantum computing among others.The topics covered by the Symposium include but are not limited to: 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; correct-by-design controller synthesis; formal assurance methods to handle adaptive systems.

Two lengths of papers were considered: regular papers describing fully developed work and complete results, and two categories of short papers: (a) tool Papers describing novel, publicly-available tools; (b) case studies detailing complete applications of formal methods to real systems with publicly-available artifacts, or substantial work-in-progress describing results from designing a new technique for a new application, with appropriate available artifacts. Artifacts enabling reproducibility of the paper's major contributions were strongly encouraged and considered in PC evaluations. Artifacts may appear in online appendices; websites with additional artifacts, e.g., for reproducibility or additional correctness proofs, were encouraged.

The Symposium received 102 abstract submissions, 72 of which resulted in full papers: 54 regular papers, and 18 short papers (10 tool papers and 8 case studies) in total. Out of these, a total of 28 papers, 20 regular papers and 8 short papers, were accepted, giving an overall acceptance rate of 39% (a 37% rate for regular papers and a 44% rate for short papers). All submissions went through a rigorous reviewing process, where each paper was read by at least three (and on the average 3.8) reviewers.

In addition to the refereed papers, the symposium featured two invited talks and a NASA panel. Representing ONERA in France, Dr. Virginie Wiels delivered a keynote talk on "Integrating Formal Methods Into Industrial Processes." Professor Richard Murray from Caltech gave a keynote talk on "Safety-Critical Systems: Rapprochement Between Formal Methods and Control Theory." NFM 2019 included a NASA panel on "Challenges for Future Exploration" featuring four NASA civil servants: Dr. Kimberly Hambuchen, Space Technology Principle Technologist for Robotics; Emily Nelson, Deputy Chief, Flight Director Branch; Joe Caram, Gateway Systems Engineering and Integration Lead; Bill Othon, Gateway Verification and Validation Lead. The panel issued challenges to the formal methods research community as NASA pushes the state of the art in certifying the integrated systems required for human spaceflight, includ-

ing unprecedented requirements for autonomy and safe operation in uniquely challenging environments.

The organizers are grateful to the authors for submitting their work to NFM 2019 and to the invited speakers and panelists for sharing their insights. NFM 2019 would not have been possible without the collaboration of the Steering Committee, Program Committee, our many external reviewers who pitched in during a U.S. Government shutdown, and the support of the NASA Formal Methods community. We are also grateful to our collaborators at Rice University's Computer Science Department, including for financial support and local organization. The NFM 2019 website can be found at https://robonaut.jsc.nasa.gov/R2/pages/nfm2019.html.

March, 2019
Houston, Texas, USA

Kristin Yvonne Rozier
Julia Badger

Table of Contents

Program Committee

Erika Abraham	RWTH Aachen University
Julia Badger	NASA
Dirk Beyer	LMU Munich, Germany
Armin Biere	Johannes Kepler University Linz
Nikolaj Bjorner	Microsoft
Sylvie Boldo	INRIA
Jonathan Bowen	London South Bank University
Gianfranco Ciardo	Iowa State University
Darren Cofer	Rockwell Collins
Frederic Dadeau	FEMTO-ST
Ewen Denney	NASA
Gilles Dowek	INRIA and ENS Paris-Saclay
Steven Drager	AFRL
Catherine Dubois	ENSIIE-Samovar
Alexandre Duret-Lutz	LRDE/EPITA
Aaron Dutle	NASA
Marco Gario	Siemens Corporate Technology
Alwyn Goodloe	NASA
Arie Gurfinkel	University of Waterloo
John Harrison	Amazon Web Services
Klaus Havelund	Jet Propulsion Laboratory
Constance Heitmeyer	Naval Research Laboratory, Washington DC 20375
Marieke Huisman	University of Twente
Shafagh Jafer	Embry-Riddle University
Xiaoqing Jin	Apple Inc.
Rajeev Joshi	Automated Reasoning Group, Amazon Web Services
Laura Kovacs	Vienna University of Technology
Hadas Kress-Gazit	Cornell University
Joe Leslie-Hurd	Intel
Panagiotis Manolios	Northeastern University
Cristian Mattarei	Stanford University
Stefan Mitsch	Carnegie Mellon University
Cesar Munoz	NASA
Anthony Narkawicz	Amazon Web Services
Necmiye Ozay	University of Michigan
Corina Pasareanu	CMU/NASA Ames Research Center
Lee Pike	Galois, Inc.
Kristin Yvonne Rozier	Iowa State University
Johann Schumann	NASA
Cristina Seceleanu	Mälardalen University
Bernhard Steffen	Univ Dortmund
Stefano Tonetta	FBK-irst

Ufuk Topcu	Uni of Texas at Austin
Christoph Torens	German Aerospace Center, Institute of Flight Systems
Michael Watson	NASA
Huan Xu	University of Maryland

Additional Reviewers

A
Al Ghazo, Alaa
Arechiga, Nikos
Asaadi, Erfan
B
Bainczyk, Alexander
Bharadwaj, Suda
Bonakdarpour, Borzoo
C
Chen, Xin
Chen, Yu-Ting
Cubuktepe, Murat
D
Devriendt, Jo
Dodds, Joey
Dureja, Rohit
E
Ehsan, Fauzia
Elliott, Trevor
Enoiu, Eduard Paul
F
Fedyukovich, Grigory
Filipovikj, Predrag
Foughali, Mohammed
Fried, Dror
Friedberger, Karlheinz
Frohme, Markus
G
Gallois-Wong, Diane
Garoche, Pierre-Loic
H
Haesaert, Sofie
Herlihy, Maurice
Heule, Marijn
I
Immler, Fabian
J
Jakobs, Marie-Christine
Jansen, Nils
Jeannin, Jean-Baptiste
Jiang, Shengbing
Jones, Benjamin

K
Kumar, Ankit
Kunnappilly, Ashalatha
L
Larus, James
Lathouwers, Sophie
Lemberger, Thomas
Li, Jianwen
Li, Meng
Liu, Zexiang
M
Mahmud, Nesredin
Melquiond, Guillaume
Micheli, Andrea
Moscato, Mariano
Müller, Andreas
N
Navas, Jorge A
Neider, Daniel
Nilsson, Petter
P
Peled, Doron
Perez, Ivan
R
Raju, Dhananjay
Ravitch, Tristan
Ren, Hao
Renault, Etienne
Rieu-Helft, Raphaël
Rüthing, Oliver
S
Schieweck, Alexander
Schirmer, Sebastian
Schupp, Stefan
Seidl, Martina
Sogokon, Andrew
Spießl, Martin
T
Tabajara, Lucas
U
Urban, Caterina
V
Vardi, Moshe
W
Walter, Andrew