Lecture Notes in Computer Science **11460**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Formal Methods

Subline of Lectures Notes in Computer Science

More information about this series at http://www.springer.com/series/7408

Julia M. Badger · Kristin Yvonne Rozier (Eds.)

NASA Formal Methods

11th International Symposium, NFM 2019 Houston, TX, USA, May 7–9, 2019 Proceedings

Springer

Editors
Julia M. Badger
NASA
Houston, TX, USA

Kristin Yvonne Rozier
Iowa State University
Ames, IA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-20651-2 ISBN 978-3-030-20652-9 (eBook)
https://doi.org/10.1007/978-3-030-20652-9

LNCS Sublibrary: SL2 – Programming and Software Engineering

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 11th NASA Formal Methods (NFM) Symposium held during 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, comprising 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. Then, 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; and 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 (ten tool papers and eight case studies) in total. Out of these, a total of 28 papers, 20 regular papers and eight 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 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, including 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, the 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

Kristin Yvonne Rozier
Julia Badger

Organization

Program Committee

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

Johann Schumann	NASA, USA
Cristina Seceleanu	Mälardalen University, Sweden
Bernhard Steffen	University of Dortmund, Germany
Stefano Tonetta	FBK-irst, Italy
Ufuk Topcu	University of Texas at Austin, USA
Christoph Torens	German Aerospace Center, Institute of Flight Systems, Germany
Michael Watson	NASA, USA
Huan Xu	University of Maryland, USA

Additional Reviewers

Al Ghazo, Alaa
Arechiga, Nikos
Asaadi, Erfan
Bainczyk, Alexander
Bharadwaj, Suda
Bonakdarpour, Borzoo
Chen, Xin
Chen, Yu-Ting
Cubuktepe, Murat
Devriendt, Jo
Dodds, Joey
Dureja, Rohit
Ehsan, Fauzia
Elliott, Trevor
Enoiu, Eduard Paul
Fedyukovich, Grigory
Filipovikj, Predrag
Foughali, Mohammed
Fried, Dror
Friedberger, Karlheinz
Frohme, Markus
Gallois-Wong, Diane
Garoche, Pierre-Loic
Haesaert, Sofie
Herlihy, Maurice
Heule, Marijn
Immler, Fabian
Jakobs, Marie-Christine
Jansen, Nils
Jeannin, Jean-Baptiste
Jiang, Shengbing
Jones, Benjamin
Kumar, Ankit
Kunnappilly, Ashalatha
Larus, James
Lathouwers, Sophie
Lemberger, Thomas
Li, Jianwen
Li, Meng
Liu, Zexiang
Mahmud, Nesredin
Melquiond, Guillaume
Micheli, Andrea
Moscato, Mariano
Müller, Andreas
Navas, Jorge A.
Neider, Daniel
Nilsson, Petter
Peled, Doron
Prez, Ivan
Raju, Dhananjay
Ravitch, Tristan
Ren, Hao
Renault, Etienne
Rieu-Helft, Raphaël
Rüthing, Oliver
Schieweck, Alexander
Schirmer, Sebastian
Schupp, Stefan
Seidl, Martina
Sogokon, Andrew
Spießl, Martin
Tabajara, Lucas
Urban, Caterina
Vardi, Moshe
Walter, Andrew
Xu, Zhe
Zhao, Ye
Zimmerman, Daniel M.

Challenges for Future Exploration (Panel Description)

A NASA Panel

NASA Johnson Space Center

Abstract. As NASA and the world look to exploration opportunities beyond low Earth orbit, several challenges have been identified. Spacecraft and other assets that will extend human presence beyond the vicinity of Earth will have unprecedented requirements for autonomy. These systems will be subject to new environments, latent and decreased communications bandwidth, sparse logistics support, and complex system requirements. New systems, such as vehicle system management, closed-loop environmental control and life support systems, and internal robotic caretakers, are proposed to close the technology gap between the current state of the art and future exploration needs. Current approaches to integration, testing, verification, and validation are likely to be insufficient to assure the operation of these vehicles and assets given their safety-critical functions. This panel will explore the challenges NASA is currently facing in the development of these systems, particularly from the standpoint of certifying the integrated system for human spaceflight.

Panelists

- **Joe Caram** leads the Systems Engineering and Integration Team for concept maturation of the cislunar spacecraft - Gateway. His agency wide team is responsible for refining the overall concepts for the Gateway. His work includes defining the integrated system requirements, concept of operations, and element functional allocations that make up the Gateway spacecraft.
  Prior to his current assignment, Joe has held key leadership roles in various projects, programs, and organizations including the lead Flight Dynamics Officer for the X-38 Project, Aerothermodynamics Team lead for the Columbia Accident Investigation, the Systems Engineering and Integration Chief Engineer for the Space Shuttle Return to Flight, Manager of the Integrated Systems Performance Office in Constellation SE&I Office, held Deputy Manager positions in both the Systems Architecture and Integration Office and the Technical Integration Office in the JSC Engineering Directorate, and was the manager of the Exploration Mission Planning Office of the JSC Exploration Integration and Science Directorate. He is the author or co-author of 24 technical papers.
- **Dr. Kimberly Hambuchen** is currently the NASA Space Technology Mission Directorate's (STMD) Principal Technologist for Robotics. As Principal Technologist, she serves as the STMD technical expert and advocate for robotics across all

NASA centers for STMD programs. Prior to this, she was the project manager for the Human Robotic Systems project, which focused on developing and advancing technologies to integrate robotics into human exploration missions.
As a robotics engineer in the Robotics Systems Technology branch of the Software, Robotics and Simulation division of engineering at NASA Johnson Space Center, Dr. Hambuchen developed expertise in novel methods for remote supervision of space robots over intermediate time delays and has proven the validity of these methods on various NASA robots, including JSC's Robonaut and Centaur robots. She participated in the development of NASA's Space Exploration Vehicle (SEV) and bipedal humanoid, Valkyrie (R5), to which she extended her work developing human interfaces for robot operations.

- **Emily Nelson** came to JSC as an employee of United Space Alliance (USA) in September of 1998 as an International Space Station (ISS) Thermal Operations and Resources Flight Controller (ThOR). She supported on-orbit operations in ISS Expeditions 0-15, and supported ISS assembly missions ISS 2A.2A (STS-101), ISS 4A (STS-97), ISS 5A (STS-98), ISS 6A (STS-100), ISS 7A.1 (STS-105) and ISS 11A (STS-113). Emily served as lead ThOR for ISS Expeditions 3, 5, 7 and 8 and the ISS 9A (STS-112) and ISS 12A.1 (STS-116) assembly flights. In 2004 she was hired by NASA and continued to support the ISS program as a ThOR and the Constellation program as a leader in information architecture development until May, 2007.
  In May of 2007, Emily was selected as a Flight Director and began ISS support with Expedition 16 in December 2007. Emily served as an ISS Flight Director in Houston's Mission Control during the ISS 1J (STS-124), ISS ULF2 (STS-126) and ISS ULF3 (STS-129) missions of the Space Shuttle to ISS. She also supported the ISS 1JA (STS-123) and ISS 2JA (STS-127) missions as an International Partner Liaison Flight Director from the Japanese Space Agency's SSIPC Control Center in Tsukuba, Japan. Emily served as lead Flight Director for ISS Expeditions 18, 27, 33, 46 and 49 and the lead ISS Flight Director for STS-132/ISS ULF4 and the third mission of the Orbital-ATK Cygnus vehicle (the OA-2 mission).
  Emily is currently serving as Deputy Chief of the Flight Director Office, is also the lead Flight Director for a series of spacewalks to repair the Alpha Magnetic Spectrometer research platform 2019, and continues to support continuous ISS operations in Mission Control Houston.

  Team Name Each NASA Flight Director chooses a symbol/color to represent his or her team. Ms. Nelson has chosen Peridot as the symbol for her flight control team because in addition to being a lovely stone, it's a gemstone known to be found in meteorites. This "space stone" represents all of the extraordinary things, familiar and unfamiliar, we're bound to find as we pursue exploration further and further from our beautiful blue planet.

- **Bill Othon** is the acting lead of Verification and Validation for the Gateway Program. Bill's team is responsible for verifying the performance of the integrated Gateway vehicle, assembled in cis-lunar space over a number of missions and with contributions from US and international partners.

Bill is also the lead for Ground Testing for the NextSTEP cis-lunar habitat activity in the AES program. The team will conduct evaluations on a number of ground habitat prototypes developed by US Industry partners, in preparation for exploration missions in the Proving Ground of cis-lunar space.

Bill has been at JSC for over 30 years, and involved in both spacecraft operations and technology development projects. Bill has a Bachelors in Aerospace Engineering from the University of Texas at Austin and a Masters in Computer Science from the University of Houston Clear Lake.

Abstracts of Invited Talks

Safety-Critical Systems: Rapprochement Between Formal Methods and Control Theory

Richard Murray

California Institute of Technology, USA
murray@cds.caltech.edu

Abstract. In computer science, formal methods provide a set of mathematically-based techniques for the specification, development, and verification of software and hardware systems. The field of control provides the principles and methods used to design engineering systems that maintain desirable performance by automatically adapting to changes in the environment. It turns out that both of these fields have been solving similar problems using different mathematical languages for the past 50 years or so. In this talk I will discuss how a convergent set of ideas from control theory and formal methods are coming together to provide useful frameworks for reasoning about the safety of these systems, motivated by applications in aerospace systems and self-driving cars.

Biography

Richard M. Murray received the B.S. degree in Electrical Engineering from California Institute of Technology in 1985 and the M.S. and Ph.D. degrees in Electrical Engineering and Computer Sciences from the University of California, Berkeley, in 1988 and 1991, respectively. He joined the faculty at Caltech in 1991 in Mechanical Engineering and helped found the Control and Dynamical Systems program in 1993.

In 1998–1999, Professor Murray took a sabbatical leave and served as the Director of Mechatronic Systems at the United Technologies Research Center in Hartford, CT. Upon returning to Caltech, Murray served as the Division Chair (dean) of Engineering and Applied Science at Caltech from 2000–2005, the Director for Information Science and Technology (IST) from 2006–2009, and interim Division Chair from 2008–2009. He is currently the Thomas E. and Doris Everhart Professor of Control & Dynamical Systems and Bioengineering at Caltech and an elected member of the National Academy of Engineering (2013).

Murray's research is in the application of feedback and control to networked systems, with applications in biology and autonomy. Current projects include analysis and design biomolecular feedback circuits, synthesis of discrete decision-making protocols for reactive systems, and design of highly resilient architectures for autonomous systems. Murray is a co-founder of Tierra Biosciences, a cell-free synthetic biology company, and a member of the Defense Innovation Board.

Integrating Formal Methods into Industrial Processes

Virginie Wiels

ONERA, France
Virginie.Wiels@onera.fr

Abstract. Formal techniques and tools have made significant progress for the last twenty years. However, industrial adoption of these techniques is still slow, despite some prominent successes. In this talk, I will identify missing bridges between formal verification research and potential industrial deployment, such as certification constraints or progressive shift between test and formal verification, and present work done at ONERA on these subjects.

Biography

Virginie Wiels is Director of the Information Processing and Systems Department (DTIS) at ONERA, the French aerospace laboratory. DTIS conducts study and research related to methods and tools for certification, autonomy, multidisciplinary design, systems of systems, intelligence and surveillance, applied mathematics. It gathers 300 persons including 80 PhD students. Virginie Wiels received her PhD in Computer Science from ISAE in 1997. Her expertise and research interest is on formal verification of critical systems and software, and the use of formal methods for the certification of avionics software.

She has served as principal investigator on government-sponsored research programs but also on industry-sponsored research programs (particularly in collaboration with Airbus). She served on EUROCAE committee WG-71 developing new certification guidance for airborne software (DO-178C/ED-12C) with significant contributions on the Formal Methods Supplement (DO-333/ED-216).

Contents