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

Ritchie Lee · Susmit Jha · Anastasia Mavridou ·
Dimitra Giannakopoulou (Eds.)

NASA Formal Methods

12th International Symposium, NFM 2020
Moffett Field, CA, USA, May 11–15, 2020
Proceedings

Springer

Editors
Ritchie Lee
NASA Ames Research Center
Moffett Field, CA, USA

Susmit Jha
SRI International
Menlo Park, CA, USA

Anastasia Mavridou
KBR Inc., NASA Ames Research Center
Moffett Field, CA, USA

Dimitra Giannakopoulou
NASA Ames Research Center
Moffett Field, CA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-55753-9 ISBN 978-3-030-55754-6 (eBook)
https://doi.org/10.1007/978-3-030-55754-6

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

The sustained improvement in hardware performance, the rapid progress in software-based control, and the emergence of artificial intelligence with near-human performance have accelerated the adoption of cyber-physical systems and, in particular, autonomous or semi-autonomous systems. An immense increase in system complexity has accompanied this acceleration in adoption. The traditional abstraction layers have been broken by the rise in new enabling technologies such as hardware acceleration and big-data-driven models, as well as unique application needs such as energy efficiency, human-in-the-loop systems, and resilient distributed computing. These factors have widened the gap between what can be designed with acceptable average behavior and what can be analyzed for their worst-case behavior.

NASA and the aerospace industry are at the frontier of the effort to tame the growing complexity of systems with the development of formal analysis approaches to ensure system safety and certification. In recent years, new challenges have emerged for system specification, development, verification, and the need for system-wide fault detection, diagnosis, and prognostics. Systems such as autonomous on-board software for Unmanned Aerial Systems (UAS) and UAS Traffic Management (UTM) require rethinking traditional approaches to assurance. The NASA Formal Methods Symposium (NFM) is a forum to foster collaboration between theoreticians and practitioners from NASA, academia, and the industry to address these challenges. The goal is to facilitate the development of advanced techniques that address specification, design, verification, validation, and certification requirements. These techniques will facilitate the responsible adoption of these complex systems in mission-critical and safety-critical applications in aerospace as well as other industries such as automobiles, robotics, and medical equipment.

NFM is an annual event organized by the NFM Steering Committee, comprised of researchers spanning several NASA centers. The series began in 1990 as the Langley Formal Methods Workshop (LFM) at NASA Langley and later became the NASA Formal Methods Symposium starting in 2009 when it became an annual NASA-wide event. The symposium is hosted by a different NASA center each year. This year, NFM was hosted and organized by the NASA Ames Research Center.

This volume contains the papers presented at the 12th NASA Formal Methods Symposium (NFM 2020) held during May 11–15, 2020. The symposium was originally planned to be held physically at NASA Ames. However, due to the travel restrictions and shelter-in-place orders arising from COVID-19, the symposium was shifted to be completely online this year. The convenience of participating in a virtual event brought a record number of registrations. This year, we had 857 registered participants from 48 different countries around the world.

The main program contained two categories of papers: (1) regular papers, presenting fully developed work and complete results and (2) short papers, presenting tools or

experience reports on applications of formal methods to real systems. We encouraged, but did not require, that papers be accompanied by publicly-available artifacts.

We received 80 abstract submissions, which ultimately resulted in 62 paper submissions. The symposium accepted a total of 25 papers (20 regular, 5 short) to be presented, resulting in an overall acceptance rate of 40.3% (39.2% regular, 45.4% short). The papers were reviewed by an international Program Committee of 44 members from a mix of academia, government, and industry. All submissions went through a rigorous single-blind reviewing process overseen by the Program Committee chairs. Each submission was reviewed by at least three reviewers.

The main program also featured six invited talks covering all aspects of safety-critical systems. Professor Byron Cook from Amazon Web Services and University College London gave a keynote talk on formal methods for cloud services. Professor David Dill from Facebook Calibra and Stanford University gave a keynote talk about formal methods for blockchain. Dana Schulze from the National Transportation Safety Board (NTSB) gave a keynote talk about transportation accidents and safety. Professor Sanjit Seshia from UC Berkeley gave a keynote talk on formal methods for autonomous and cyberphysical systems. Dr. Vandi Verma from NASA JPL gave a keynote talk about Mars 2020 rover and challenges. Finally, Léonard Bouygues from Google Loon gave a keynote talk about safety and high-altitude balloon networks. The main program also included a special session introducing the SAE G-34/EUROCAE WG-114 Working Group, which is a standards development committee for AI certification.

In addition to the main program, the symposium also had two affiliated workshops: Workshop on AI Safety and Workshop on Formal Methods for Cryptographic Proofs.

We gratefully thank the authors for submitting and presenting their work at NFM 2020. We thank the invited speakers, Steering Committee, session chairs, Program Committee and external reviewers, and support staff, all of whom have contributed to make the virtual symposium successful. Finally, we thank our sponsor UTRC and everyone who attended NFM this year. The NFM 2020 website can be found at https://ti.arc.nasa.gov/events/nfm-2020/.

May 2020

Ritchie Lee
Susmit Jha
Anastasia Mavridou
Dimitra Giannakopoulou

The original version of the book was revised: a forgotten volume editor was added. The correction to the book is available at https://doi.org/10.1007/978-3-030-55754-6_26

Organization

General Chairs

Dimitra Giannakopoulou	NASA Ames Research Center, USA
Anastasia Mavridou	NASA Ames Research Center and KBR, USA

Program Committee Chairs

Ritchie Lee	NASA Ames Research Center, USA
Susmit Jha	SRI International, USA

Steering Committee

Julia Badger	NASA Johnson, USA
Aaron Dutle	NASA Langley, USA
Klaus Havelund	NASA JPL, USA
Michael R. Lowry	NASA Ames, USA
Kristin Y. Rozier	Iowa State University, USA
Johann Schumann	NASA Ames and KBR, USA

Program Committee

Aaron Dutle	NASA Langley, USA
Ahmed Irfan	Stanford University, USA
Alessandro Cimatti	Fondazione Bruno Kessler (FBK), Italy
Alwyn Goodloe	NASA Langley, USA
Arie Gurfinkel	University of Waterloo, Canada
Arnaud Venet	Facebook, USA
Ashlie Hocking	Dependable Computing, USA
Brian Jalaian	Army Research Laboratory, USA
Catherine Dubois	ENSIIE, France
Cesar Munoz	NASA Langley, USA
Christoph Torens	German Aerospace Center (DLR), Germany
Constance Heitmeyer	Naval Research Laboratory, USA
Corina Pasareanu	NASA Ames and Carnegie Mellon University, USA
Cormac Flanagan	UC Santa Cruz, USA
Cristina Seceleanu	Malardalen University, Sweden
Daniel Genin	Johns Hopkins University APL, USA
Erika Ábrahám	RWTH Aachen University, Germany
Ewen Denney	NASA Ames and KBR, USA
Falk Howar	Dortmund University, Germany
Huafeng Yu	Boeing, USA

J. Aaron Pendergrass	Johns Hopkins University APL, USA
Jean-Baptiste Jeannin	University of Michigan, USA
Johann Schumann	NASA Ames and KBR, USA
Klaus Haveland	NASA JPL, USA
Konrad Slind	Rockwell Collins, USA
Kristin Rozier	Iowa State University, USA
Laura Kovacs	TU Wien, Austria
Laura Titolo	NASA Langley and NIA, USA
Marielle Stoelinga	University of Twente and Radboud University, The Netherlands
Michael Lowry	NASA Ames, USA
Michael Whalen	Amazon Web Services, USA
Natasha Neogi	NASA Langley, USA
S. Ramesh	General Motors, USA
Shaun McWherter	NASA Armstrong, USA
Simon Bliudze	Inria, France
Stavros Tripakis	Northeastern University, USA
Stefan Mitsch	Carnegie Mellon University, USA
Stefania Gnesi	ISTI, Italy
Steven Drager	Air Force Research Laboratory, USA
Taylor Johnson	Vanderbilt University, USA
Ufuk Topcu	The University of Texas at Austin, USA
Virginie Wiels	ONERA, France
Willem Visser	Stellenbosch University, South Africa
Xiaoqing Jin	Apple, USA

Additional Reviewers

Peter Backeman
Davide Basile
Steven Carr
Esther Conrad
Thao Dang
Jyotirmoy Deshmukh
Florian Faissole
Alessandro Fantechi
Lu Feng
Predrag Filipovikj
Jie Fu
Georgios Giantamidis
Stephen Giguere
Rong Gu
Arnd Hartmanns
Fabian Immler
Brian Kempa
Rom Langerak
Nham Le
Makai Mann
Omer Nguena Timo
Melkior Ornik
Ivan Perez
Arnau Prat i Sala
Swarn Priya
John Rushby
Sebastian Schirmer
Stefan Schupp
Maximilian Schwenger
Tanner Slagel
Hari Govind Vediramana Krishnan
Abhinav Verma
Haoze Wu
Djurre van der Wal

Abstracts of Invited Talks

Automated Reasoning at Amazon

Byron Cook

Amazon Web Services, University College London
b.cook@cs.ucl.ac.uk

Abstract. This talk will discuss the development and use of formal verification tools within Amazon Web Services (AWS) to increase the assurance of its cloud infrastructure and to help customers help themselves build correct cloud-based systems. I will also discuss some open challenges that could inspire future research in the community.

Biography

Byron Cook is Professor of Computer Science at University College London (UCL) and Senior Principal Scientist at Amazon. Byron's interests include computer/network security, program analysis/verification, programming languages, theorem proving, logic, hardware design, operating systems, and biological systems.

A Formal Verifier for the Libra Blockchain Move Language

David Dill

Facebook Inc., Stanford University
dill@cs.stanford.edu

Abstract. The Libra blockchain, which was initiated last year by Facebook, includes a novel programming language called Move for implementing smart contracts. We plan for the Libra blockchain to host massive amounts of assets, and all transactions are mediated by Move programs, and smart contracts on other blockchains have had devastating bugs resulting in major losses of assets, so we consider the correctness of Move programs to be critical. The Move language is designed to be as safe as we can make it, and it is accompanied by a formal specification and automatic verification tool, called the Move Prover. Our aspiration is that every Move program will be thoroughly specified and verified before being deployed on the blockchain.

Biography

David L. Dill is a Lead Researcher at Facebook, working on the Libra blockchain project. He is also Donald E. Knuth Professor, Emeritus, in the School of Engineering at Stanford University. He was on the faculty in the Department of Computer Science at Stanford from 1987 until going emeritus in 2017, and starting his current position at Facebook in 2018. Prof. Dill's research interests include formal verification of software, hardware, and protocols, with a focus on automated techniques, as well as voting technology and computational biology. He is an IEEE Fellow, an ACM Fellow, a member of the National Academy of Engineering, and the American Academy of Arts and Sciences. He received an EFF Pioneer Award for his work in voting technology and is the founder of VerifiedVoting.org.

Improving Design Assurance Through Accident/Incident Lessons Learned

Dana Schulze

National Transportation Safety Board (NTSB)
dana.schulze@ntsb.gov

Abstract. The NTSB has investigated or participated in the investigation of numerous accidents and incidents involving the failure of complex aircraft systems. While accidents involving these types of failures are quite rare, their occurrence offers lessons learned for the design and certification communities. Findings in several cases suggest that these malfunctions are not typically the result of software production deficiencies but rather system or software requirements deficiencies. Case studies involving two NTSB investigations will be discussed and used to introduce the broader set of design issues that accident and incident investigations have revealed, which could be useful in understanding the improvements needed in design assurance methods and their implementation to improve complex system certification outcomes.

Biography

Dana Schulze, Director of the Office of Aviation Safety, has been with the National Transportation Safety Board since 2002. She began her career with the Safety Board as an Aircraft System Safety Engineer in the Aviation Engineering Division and served as a Group Chairman and investigator on numerous major domestic and international airline accident investigations, including Alaska Airlines flight 261, Pinnacle Airlines flight 3701, and American Airlines flight 587. In 2006, Ms. Schulze became Chief of the Aviation Engineering Division, which is responsible for investigating the airworthiness of aircraft involved in major aviation accidents and serious incidents. Ms. Schulze later served as the Chief of the Major Investigations Division where she oversaw more than a dozen major airline accident investigations, including the investigation of US Airways flight 1549 in Weehawken, New Jersey, and Colgan Air flight 3407 in Clarence Center, New York, and subsequently as Deputy Director, leading the organization's execution of air carrier investigations and safety initiatives as well as the development of emergent programs for unmanned aircraft systems and commercial space accident investigation. In 2018, she was named the Acting Director of the Office of Aviation Safety and moved into the Director role in 2019. Prior to joining the NTSB, Ms. Schulze worked in the commercial aerospace industry in staff engineering and engineering management roles related to design, system safety, reliability, and quality. She received her Bachelor of Science degree in Space Sciences and Mechanical Engineering from the Florida Institute of Technology and Master of Science degree in Mechanical Engineering from the State University of New York.

Ms. Schulze is also a recipient of the Distinguished Presidential Rank Award, which recognizes a select group of career members of the United States Government Senior Executive Service (SES) for sustained extraordinary accomplishments on a national or international level.

Verified Artificial Intelligence and Autonomy

Sanjit Seshia

UC Berkeley
sseshia@berkeley.edu

Abstract. Verified artificial intelligence (AI) is the goal of designing AI-based systems that have strong, verified assurances of correctness with respect to mathematically-specified requirements. This goal is particularly important for autonomous and semi-autonomous systems. In this talk, I will consider Verified AI from a formal methods perspective and with a special focus on autonomy. I will describe the challenges for and recent progress towards attaining Verified AI, with examples from the domain of intelligent cyber-physical systems, with a particular focus on autonomous vehicles and aerospace systems.

Biography

Sanjit A. Seshia is a Professor in the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. He received a Masters and PhD in Computer Science from Carnegie Mellon University, and a Bachelor in Computer Science and Engineering from the Indian Institute of Technology, Bombay. His research interests are in formal methods for dependable and secure computing, with a current focus on the areas of cyber-physical systems, computer security, machine learning, and robotics. He has made pioneering contributions to the areas of satisfiability modulo theories (SMT), SMT-based verification, and inductive program synthesis. He is co-author of a widely-used textbook on embedded, cyber-physical systems and has led the development of technologies for cyber-physical systems education based on formal methods. His awards and honors include a Presidential Early Career Award for Scientists and Engineers (PECASE), an Alfred P. Sloan Research Fellowship, the Frederick Emmons Terman Award for contributions to electrical engineering and computer science education, the Donald O. Pederson Best Paper Award for the IEEE Transactions on CAD, and the IEEE Technical Committee on Cyber-Physical Systems (TCCPS) Mid-Career Award. He is a Fellow of the IEEE.

Operable NASA Robots on Mars and Beyond

Vandi Verma

NASA Jet Propulsion Laboratory (JPL)
vandana.verma@jpl.nasa.gov

Abstract. The talk will provide an overview of Mars rovers and the challenges with developing operable space robots.

Biography

Vandi Verma leads the Operable Robotics group in the Mobility and Robotic Systems Section at NASA Jet Propulsion Laboratory. She has developed software for and operated multiple rovers on Mars and has worked on research rovers deployed in the Arctic, Antarctic, and the Atacama. Vandi's interests include space robotics, autonomy, and operability. She is currently working on robotic arm and sample caching algorithms, flight software for the Mars 2020 Perseverance rover, and is the software architect for the Europa Lander advanced autonomy prototype. She has a PhD in Robotics from Carnegie Mellon University.

Evolving Airspace Regulations and Systems to Enable Large Scale, Highly Automated Operations in the Stratosphere

Léonard Bouygues

Google Loon
leonardb@loon.com

Abstract. Loon is a network of stratospheric vehicles that provide connectivity to thousands of people living in underserved regions around the world. With over 350k flight hours in 2019 and over one million flight hours total, it is the world's first large-scale automated fleet of unmanned vehicles.

Aviation regulations, concepts of operations, and aviation systems need to evolve to enable new technologies like Loon. Loon is partnering with regulators, the entire community of stratospheric operators, and research organizations to cooperatively evolve this airspace. 1) Develop collaborative traffic management concepts that are necessary to handle the unique vehicle performance characteristics and the dynamic ecosystem. 2) Develop new risk and performance-based safety frameworks needed to ensure a safe environment in which technologies and designs can evolve rapidly. 3) Develop new validation methods for modern software development techniques and a rapidly evolving software ecosystem. 4) Propose adaptations to roles and responsibilities of humans in the context of large-scale automated systems.

Biography

Léonard is currently Head of Aviation Strategy at Loon. Loon is a network of high-altitude balloons that provide telecommunications access to unserved and underserved populations. It is the first large-scale automated fleet of unmanned vehicles and has already surpassed one million flight hours.

In this role, Léonard is responsible for the development of innovative aviation concepts. He currently leads industry players in the development of the "Collaborative Traffic Management in the Stratosphere" CONOPs. He is also a key contributing author of the initial paper that he presented at Drone Enable 2019. Additionally, Léonard is currently working in partnerships with NASA, MITRE, academia, and research organizations to evolve safety frameworks within FAA's safety continuum, in particular for in-time safety management, risk budgeting, and human-automation teaming for the supervision of large autonomous fleets.

After joining Loon in 2015, Léonard led Loon's Flight Operations from 2017–2019. In this position, he built and managed the company's Operation Control Center, enabling Loon to supervise a fleet of hundreds of autonomous vehicles. In this effort,

Léonard's team also developed technology for live risk computation of Loon operations.

Léonard started at Google's European headquarters as an Analytical Lead, before joining the Mountain View office to work as a Product Lead in the advertising division. Léonard holds a Master's in Aeronautical Engineering from Imperial College London, a Master of Science in Management of Technology and Innovation form MIT, and a Master of Science in management from HEC Paris.

Contents