

2023 IEEE International Conference on Assured Autonomy (ICAA 2023)

**Laurel, Maryland, USA
6-8 June 2023**



**IEEE Catalog Number: CFP23AH3-POD
ISBN: 979-8-3503-2602-4**

**Copyright © 2023 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. 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:	CFP23AH3-POD
ISBN (Print-On-Demand):	979-8-3503-2602-4
ISBN (Online):	979-8-3503-2601-7

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

2023 IEEE International Conference on Assured Autonomy (ICAA) ICAA 2023

Table of Contents

Preface	viii
Committees	ix
Sponsors	xi
Keynotes	xii

Session 1: Addressing Novelty for Trained Components

Causal Repair of Learning-Enabled Cyber-Physical Systems	1
<i>Pengyuan Lu (University of Pennsylvania, USA), Ivan Ruchkin (University of Florida, USA), Matthew Cleaveland (University of Pennsylvania, USA), Oleg Sokolsky (University of Pennsylvania, USA), and Insup Lee (University of Pennsylvania, USA)</i>	
Novelty Detection in Network Traffic: Using Survival Analysis for Feature Identification	11
<i>Taylor Bradley (Johns Hopkins University), Elie Alhajjar (Army Cyber Institute), and Nathaniel Bastian (Army Cyber Institute)</i>	
Predicting Out-of-Distribution Performance of Deep Neural Networks Using Model Conformance. 19	
<i>Ramneet Kaur (University of Pennsylvania), Susmit Jha (SRI International), Anirban Roy (SRI International), Oleg Sokolsky (University of Pennsylvania), and Insup Lee (University of Pennsylvania)</i>	

Session 2: Autonomous Systems

Driver Alerting in ADAS-Equipped Cars: A Field Study	29
<i>Mary Cummings (George Mason University) and Ben Bauchwitz (Duke University)</i>	
Leveraging Compositional Methods for Modeling and Verification of an Autonomous Taxi System	34
<i>Alessandro Pinto (NASA Jet Propulsion Laboratory, California Institute of Technology), Anthony Corso (Stanford University), and Edward Schmerling (Stanford University)</i>	
Safe Explainable Agents for Autonomous Navigation using Evolving Behavior Trees	44
<i>Nicholas Potteiger (Vanderbilt University, USA) and Xenofon Koutsoukos (Vanderbilt University, USA)</i>	

Live Virtual Constructive Environment for Assuring the Safety and Security of Complex Autonomous Vehicles	53
<i>Bradley Potteiger (Johns Hopkins Applied Physics Lab), Thomas Dignan (Johns Hopkins Applied Physics Lab), Amber Mills (Johns Hopkins Applied Physics Lab), Ed Pavelka (Johns Hopkins Applied Physics Lab), Caleb Frey (Johns Hopkins Applied Physics Lab), Ben Nathan (Johns Hopkins Applied Physics Lab), Milki Dagne (Johns Hopkins Applied Physics Lab), Violet Garibaldi (Johns Hopkins Applied Physics Lab), and Ben Otter (Johns Hopkins Applied Physics Lab)</i>	
Probabilistic Dynamic Modeling and Control for Skid-Steered Mobile Robots in Off-Road Environments	57
<i>Ananya Trivedi (Northeastern University, USA), Salah Bazzi (Northeastern University, USA), Mark Zolotas (Northeastern University, USA), and Taskin Padir (Northeastern University, USA)</i>	

Session 3: Verification

Proposed V-Model for Verification, Validation, and Safety Activities for Artificial Intelligence	61
<i>Benjamin Schumeg (Quality Engineering & System Assurance, Combat Capabilities Development Command Armaments Center, USA), Franklin Marotta (Aberdeen Test Center, Army Test and Evaluation Command, USA), and Benjamin Werner (Quality Engineering & System Assurance, Combat Capabilities Development Command Armaments Center, USA)</i>	
Example Applications of Formal Methods to Aerospace and Autonomous Systems	67
<i>Laura Humphrey (Air Force Research Laboratory)</i>	
Detecting Trojaned DNNs Using Counterfactual Attributions	76
<i>Karan Sikka (SRI), Indranil Sur (SRI), Anirban Roy (SRI), Ajay Divakaran (SRI), and Susmit Jha (SRI)</i>	

Session 4 Assuring Systems

Watchdog for Assuring COLREG Compliance of Autonomous Unmanned Surface Vessels that Include Artificial Intelligence	86
<i>Joshua Prucnal (Weather Gage Technologies, LLC, USA) and David Scheidt (Weather Gage Technologies, LLC, USA)</i>	
Architecting Systems for Assured Autonomy	91
<i>Richard Avila (Northrop Grumman) and Jason Clark (Northrop Grumman)</i>	
Assurance for Autonomy – JPL’s Past Research, Lessons Learned, and Future Directions	97
<i>Martin Feather (Jet Propulsion Laboratory, California Institute of Technology) and Alessandro Pinto (Jet Propulsion Laboratory, California Institute of Technology)</i>	

Session 5: Cyber Deterrence

AI Forensics	106
<i>Samuel Lefcourt (Johns Hopkins University, USA) and Gregory Falco (Johns Hopkins University, USA)</i>	

Space Booby Traps: Hacking Back and Assured Cyber Deterrence in Space	115
<i>Jocelyn Hsu (Johns Hopkins University) and Gregory Falco (Johns Hopkins University)</i>	
Assured Point Cloud Perception	119
<i>Christopher Serrano (HRL Laboratories, LLC), Aleksey Nogin (Red Balloon Security), and Michael Warren (HRL Laboratories, LLC)</i>	
A Safety Fallback Controller for Improved Collision Avoidance	129
<i>Daniel Genin (Johns Hopkins University Applied Physics Laboratory), Elizabeth Dietrich (Johns Hopkins University Applied Physics Laboratory), Yanni Kouskoulas (Johns Hopkins University Applied Physics Laboratory), Aurora Schmidt (Johns Hopkins University Applied Physics Laboratory), Marin Kobilarov (Johns Hopkins University), Kapil Katyal (Johns Hopkins University Applied Physics Laboratory), Shahriar Sefati (Johns Hopkins University), Subhransu Mishra (Johns Hopkins University), and Ivan Papusha (Johns Hopkins University Applied Physics Laboratory)</i>	

Session 6: Machine Learning and AI Design

Explanation Through Reward Model Reconciliation Using POMDP Tree Search	137
<i>Benjamin D. Kraske (University of Colorado Boulder, USA), Anshu Saksena (Johns Hopkins University Applied Physics Laboratory, USA), Anna L. Buczak (Johns Hopkins University Applied Physics Laboratory, USA), and Zachary N. Sunberg (University of Colorado Boulder, USA)</i>	
Cascading Negative Transfer in Networks of Machine Learning Systems	141
<i>Tyler Cody (Virginia Tech, USA) and Peter Beling (Virginia Tech, USA)</i>	
Dehallucinating Large Language Models Using Formal Methods Guided Iterative Prompting ..	149
<i>Susmit Jha (SRI International, USA), Sumit Kumar Jha (University of Texas at San Antonio, USA), Patrick Lincoln (SRI International, USA), Nathaniel D. Bastian (United States Military Academy, USA), Alvaro Velasquez (University of Colorado Boulder, USA), and Sandeep Neema (Vanderbilt University, USA)</i>	
Privacy-Aware Blockchain-Based AV Parking System Registration Scheme	153
<i>Alexander Haastrup (University of Southern Mississippi, USA), Muhammad Hataba (University of Southern Mississippi, USA), Ahmed Sherif (University of Southern Mississippi, USA), and Mohamed Elserly (Higher Colleges of Technology, UAE)</i>	
Author Index	161