2024 International Conference on Assured Autonomy (ICAA 2024)

Nashville, Tennessee, USA
10-11 October 2024

IEEE Catalog Number: CFP24AH3-POD
ISBN: 979-8-3315-2102-8

Copyright © 2024 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:	CFP24AH3-POD
ISBN (Print-On-Demand):	979-8-3315-2102-8
ISBN (Online):	979-8-3315-2101-1

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

2024 International Conference on Assured Autonomy (ICAA)

ICAA 2024

Table of Contents

Message from General Chairs ix
Organizing Committee x
Steering Committee xi
Technical Program Committee/Reviewers xii
Keynotes xiii
Sponsors xv

Design for Assured and Safe Autonomy

Designing Robust Cyber-Defense Agents with Evolving Behavior Trees 1
Nicholas Potteiger (Vanderbilt University, USA), Ankita Samaddar (Vanderbilt University, USA), Hunter Bergstrom (Vanderbilt University, USA), and Xenofon Koutsoukos (Vanderbilt University, USA)

Who is Responsible? Explaining Safety Violations in Multi-Agent Cyber-Physical Systems 11
Luyao Niu (University of Washington, USA), Hongchao Zhang (Washington University in St. Louis, USA), Dinuka Sahabandu (University of Washington, USA), Bhaskar Ramasubramanian (Western Washington University, USA), Andrew Clark (Washington University in St. Louis, USA), and Radha Poovendran (University of Washington, USA)

Domain Knowledge Elicitation for Data Curation to Promote Trustworthiness in Artificial Intelligence 21
Mary Versa Clemens-Sewall (The Johns Hopkins University Applied Physics Laboratory, USA), Emma Rafkin (The Johns Hopkins University Applied Physics Laboratory, USA), and Christopher Cervantes (The Johns Hopkins University Applied Physics Laboratory, USA)

Methods for Testing and Assuring AI and Autonomy

Graph-Based Grounding in a Conversational Clinical Decision Support System 31
Samuel Barham (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Michael Kelbaugh (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Arun Reddy (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Devin Ramsden (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Chase Chandler (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Adam Tobin-Williams (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Ben Shalom Elhadad (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), Georgia R. Cooper (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA), and Kari Alexander (Johns Hopkins University Applied Physics Laboratory (JHU/APL), USA)

Estimating Data Requirements for Learning-Enabled Systems using Metadata 38
Chi Phuong Ngoc Huynh (Vanderbilt University, USA) and James Weimer (Vanderbilt University, USA)

Shrinking POMCP: A Framework for Real-Time UAV Search and Rescue 48
Yunuo Zhang (Vanderbilt University, USA), Baiting Luo (Vanderbilt University, USA), Ayan Mukhopadhyay (Vanderbilt University, USA), Daniel Stojcsics (Vanderbilt University, USA), Daniel Elenius (SRI), Anirban Roy (SRI), Susmit Jha (SRI), Miklos Maroti (University of Szeged, Hungary), Xenofon Koutsoukos (Vanderbilt University, USA), Gabor Karsai (Vanderbilt University, USA), and Abhishek Dubey (Vanderbilt University, USA)

Security and Robustness of AI and Autonomous Systems

Dynamic View Translation for Robust Multi-Agent Autonomy 58
Grayson Byrd (Johns Hopkins University; The Johns Hopkins University Applied Physics Laboratory, USA), Dan Zhang (Clemson University, USA), Feng Luo (Clemson University, USA), Venkat Krovi (Clemson University, USA), David Gorsich (US Army DEVCOM, USA), Jonathon Smereka (US Army DEVCOM, USA), and Mark Brudnak (US Army DEVCOM, USA)

GPU Partitioning & Neural Architecture Sizing for Safety-Driven Sensing in Autonomous Systems 67
Shengjie Xu (The University of North Carolina at Chapel Hill, USA), Clara Hobbs (The University of North Carolina at Chapel Hill, USA), Yukai Song (University of Pittsburgh, USA), Bineet Ghosh (The University of Alabama, USA), Tingan Zhu (The University of North Carolina at Chapel Hill, USA), Sharmin Aktar (The University of North Carolina at Chapel Hill, USA), Lei Yang (George Mason University, USA), Yi Sheng (George Mason University, USA), Weiwen Jiang (George Mason University, USA), Jingtong Hu (University of Pittsburgh, USA), Parasara Sridhar Duggirala (The University of North Carolina at Chapel Hill, USA), and Samarjit Chakraborty (The University of North Carolina at Chapel Hill, USA)

Pinpointing Actuator Attacks: A Novel Diagnostic Framework for Cyber-Physical Systems 77
Zifan Wang (Syracuse University, USA), Qinru Qiu (Syracuse University, USA), and Fanxin Kong (University of Notre Dame, USA)

Work-In-Progress Poster Session

Reliability Evaluation of CNN-enabled Systems in Adversarial Scenarios 87
Karen da Mata (University of Massachusetts Dartmouth, USA), Zakaria Faddi (University of Massachusetts Dartmouth, USA), Priscila Silva (University of Massachusetts Dartmouth, USA), Vidhyashree Nagaraju (Stonehill College, USA), Susmita Ghosh (Jadavpur University, IN), Gokhan Kul (University of Massachusetts Dartmouth, USA), and Lance Fiondella (University of Massachusetts Dartmouth, USA)

New Framework for Defining Command and Control Structure of Complex Aviation Systems 91
Walter Bender (Johns Hopkins University, USA) and Michael Castle (Johns Hopkins University, USA)

Mixed-Reality Testbed for Autonomous Fixed-Wing UAVs Human-Autonomy Teaming 94
Worawis Sribunma (Purdue University, USA), Li-Yu Lin (Purdue University, USA), Kartik A. Pant (Purdue University, USA), Chuhao Deng (Purdue University, USA), James M. Goppert (Purdue University, USA), Sabine Brunswicker (Purdue University, USA), and Joe Roberts (Windracers Limited, United Kingdom)

Towards Verification-Driven Control Learning 98
Stefan Mitsch (DePaul University, USA)

Leveraging RAG-LLM to Translate C++ to Rust 102
Ahmet Okutan (Leidos, USA), Samuel Merten (Leidos, USA), Christoph C. Michael (Leidos, USA), and Ben Ryjikov (Leidos, USA)

Towards Trustworthy Distributed AI Demand Response 106
Raphael Norman-Tenazas (JHU Applied Physics Laboratory, USA), Cameron Hickert (JHU Applied Physics Laboratory, USA), Tamim Sookoor (JHU Applied Physics Laboratory, USA), Aurora Schmidt (JHU Applied Physics Laboratory, USA), Edward Staley (JHU Applied Physics Laboratory, USA), Joseph Maurio (JHU Applied Physics Laboratory, USA), Jesse Silverberg (JHU Applied Physics Laboratory, USA), Paul Wood (JHU Applied Physics Laboratory, USA), and Yair Amir (JHU Whiting School of Engineering, USA)

Analyzing Neural Network Robustness Using Graph Curvature 110
Shuhang Tan (Rensselaer Polytechnic Institute, USA), Jayson Sia (University of Southern California, USA), Paul Bogdan (University of Southern California, USA), and Radoslav Ivanov (Rensselaer Polytechnic Institute, USA)

Neuro-Symbolic Program Synthesis for Multi-Hop Natural Language Navigation 114
William English (University of Florida, USA), Dominic Simon (University of Florida, USA), Rubel Ahmed (University of Central Florida, USA), Sumit Jha (Florida International University, USA), and Rickard Ewetz (University of Florida, USA)

Solving Mystery Planning Problems Using Category Theory, Functors, and Large Language Models 118
Sumit Kumar Jha (Florida International University, USA), Susmit Jha (SRI International, USA), Rickard Ewetz (University of Florida, USA), and Alvaro Velasquez (University of Colorado Boulder, USA)

Author Index **123**