# 2022 IEEE International Conference on Assured Autonomy (ICAA 2022)

## Virtual Conference
## 22 – 24 March 2022

**IEEE Catalog Number:** CFP22AH3-POD
**ISBN:** 978-1-6654-8540-1

****** 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: CFP22AH3-POD
ISBN (Print-On-Demand): 978-1-6654-8540-1
ISBN (Online): 978-1-6654-8539-5

**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

# 2022 IEEE International Conference on Assured Autonomy (ICAA)

# ICAA 2022

## Table of Contents

**Preface** ..... **viii**
**Organizing Committee** ..... **ix**
**Program Committee** ..... **xi**
**Keynotes** ..... **xiii**
**Sponsors** ..... **xx**

## AI Safety, Assurance, and Machine Learning

On Using Real-Time Reachability for the Safety Assurance of Machine Learning Controllers ..... 1
*Patrick Musau (Vanderbilt University, USA), Nathaniel Hamilton (Vanderbilt University, USA), Diego Manzanas Lopez (Vanderbilt University, USA), Preston Robinette (Vanderbilt University, USA), and Taylor T. Johnson (Vanderbilt University, USA)*

Zero-Shot Policy Transfer in Autonomous Racing: Reinforcement Learning vs Imitation Learning ..... 11
*Nathaniel Hamilton (Vanderbilt University, USA), Patrick Musau (Vanderbilt University, USA), Diego Manzanas Lopez (Vanderbilt University, USA), and Taylor T. Johnson (Vanderbilt University, USA)*

Robustness Assurance Quotient: Demonstrating Context Matters for AI Performance and ML Security ..... 21
*Samuel Lefcourt (Johns Hopkins University, USA), Nathaniel Gordon (Johns Hopkins University, USA), Hanting Wong (Johns Hopkins University, USA), and Gregory Falco (Johns Hopkins University, USA)*

A Mapping of Assurance Techniques for Learning Enabled Autonomous Systems to The Systems Engineering Lifecycle ..... 28
*Christian Ellis (University of Massachusetts Dartmouth, USA), Maggie Wigness (Army Research Laboratory, United States), and Lance Fiondella (University of Massachusetts Dartmouth, USA)*

Resilient Multi-Agent Reinforcement Learning Using Medoid and Soft-Medoid Based Aggregation ..... 36
*Chandreyee Bhowmick (Vanderbilt University, USA), Mudassir Shabbir (Vanderbilt University, USA), Waseem Abbas (University of Texas at Dallas, USA), and Xenofon Koutsoukos (Vanderbilt University, USA)*

Selective Classification of Sequential Data Using Inductive Conformal Prediction ..... 46
*Dimitrios Boursinos (Vanderbilt University, USA) and Xenofon Koutsoukos (Vanderbilt University, USA)*

Layer-Wise Analysis of Neuron Activation Values for Performance Verification of Artificial Neural Network Classifiers ..... 56
*Darryl Hond (Thales UK Research, Technology and Innovation, UK), Hamid Asgari (Thales UK Research, Technology and Innovation, UK), Leonardo Symonds (Thales UK Research, Technology and Innovation, UK), and Mike Newman (Thales UK Research, Technology and Innovation, UK)*

## Explainable AI, Ethics, and Detection of Disruptive Events

Explainable Forecasts of Disruptive Events using Recurrent Neural Networks ..... 64
*Anna L. Buczak (Johns Hopkins University, Applied Physics Laboratory, USA), Benjamin D. Baugher (Johns Hopkins University, Applied Physics Laboratory, USA), Adam J. Berlier (Johns Hopkins University, Applied Physics Laboratory, USA), Kayla E. Scharfstien (Johns Hopkins University Applied Physics Laboratory and Carnegie Mellon University), and Christine S. Martin (Johns Hopkins University, Applied Physics Laboratory, USA)*

Focusing on the Ethical Challenges of Data Breaches and Applications ..... 74
*Karen Joisten (Technical University of Kaiserslautern, Germany), Nicole Thiemer (Technical University of Kaiserslautern, Germany), Tobias Renner (Technical University of Kaiserslautern, Germany), Anke Janssen (Technical University of Kaiserslautern, Germany), and Alexander Scheffler (Faculty of Computer Science, Ruhr University Bochum, Germany)*

## Adversarial Attack Detection and Defense

Adversarial Email Generation Against Spam Detection Models Through Feature Perturbation ... 83
*Qi Cheng (Johns Hopkins University, Baltimore, MD), Anyi Xu (American University, Washington, D.C.), Xiangyang Li (Johns Hopkins University, Baltimore, MD), and Leah Ding (American University, Washington, D.C.)*

Discovery of AI/ML Supply Chain Vulnerabilities Within Automotive Cyber-Physical Systems ..... 93
*Daniel Williams (Johns Hopkins Applied Physics Lab, Laurel, MD), Chelece Clark (Johns Hopkins Applied Physics Lab, Laurel, MD), Rachel McGahan (John Hopkins Applied Physics Lab, Laurel, MD), Bradley Potteiger (John Hopkins Applied Physics Lab, Laurel, MD), Daniel Cohen (John Hopkins Applied Physics Lab, Laurel, MD), and Patrick Musau (Vanderbilt University, USA)*

Adversarially Robust Edge-Based Object Detection for Assuredly Autonomous Systems ..... 97
*Robert Canady (Vanderbilt University, TN), Xingyu Zhou (Vanderbilt University, TN), Yogesh Barve (Vanderbilt University, TN), Daniel Balasubramanian (Vanderbilt University, TN), and Aniruddha Gokhale (Vanderbilt University, TN)*

Risk-Aware Scene Sampling for Dynamic Assurance of Autonomous Systems ..... 107
*Shreyas Ramakrishna (Vanderbilt University), Baiting Luo (Vanderbilt University), Yogesh Barve (Vanderbilt University), Gabor Karsai (Vanderbilt University), and Abhishek Dubey (Vanderbilt University)*

## AI Bias and Mitigations

Measuring and Mitigating Bias in AI-Chatbots ..... 117
*Hedin Beattie (Johns Hopkins University), Lanier Watkins (Johns Hopkins University), William H. Robinson (Vanderbit University), Aviel Rubin (Johns Hopkins University), and Shari Watkins (American University)*

## Resilience and Verification in Autonomous Space Systems

Reference Architectures for Autonomous on-Orbit Servicing, Assembly and Manufacturing (OSAM) Mission Resilience ..... 124
*Nathaniel G. Gordon (Johns Hopkins University, United States) and Gregory Falco (Johns Hopkins University, United States)*

Hallmarks of an Autonomous Space System's Development and V&V ..... 129
*Martin S. Feather (Jet Propulsion Laboratory, California Institute of Technology, USA)*

**Author Index** ..... **137**