The Second IEEE International Workshop on Workshop on Assured Autonomy, AI and Machine Learning (WAAM 2023)

November 2, 2023

Part of The Fifth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications

http://www.sis.pitt.edu/lersais/conference/tps/2023/

November 2, 2023. Atlanta, GA, USA

Description

Artificial intelligence (AI) and Machine Learning (ML) systems are increasingly seen in many domains such as self-driving land vehicles, autonomous aircraft, and medical systems. AI systems should equal or surpass human performance, but given the consequences of failure in these systems, how do we determine that the data gathered to train an AI system is suitably representative of the real world? How do we assure the public that these systems work as intended and will not cause harm? These questions have given rise to a new term: "assured autonomy." In this workshop, issues in assured autonomy such as explain ability, bias, verification, validation, privacy, trust and more for AI and ML systems will be explored. Research, experiences and best practices will be presented to illustrate the challenges and possible approaches to assured autonomy. Finally, the road ahead will be explored.

This workshop will bring together researchers from government, industry and academia to discuss these challenging issues. The workshop will be in the form of panel discussions and invited presentations. While the panelist and presenters are invited only, any conference attendee is welcome to attend the workshop.

Time	Event/Panel
08:00am-08:30am	**Breakfast**
08:30am-09:15am	**Panel 1: Identifying and Measuring Properties of Autonomous/AI/ML Systems** • **Junhua Ding, University of North Texas** • **Erin Lanus, Virginia Tech** • **Adam Porter, University of Maryland** • **Sandeep Neema, Vanderbilt University** • **David Stracuzzi, Sandia National Laboratories**
09:15am-10:45am	**Panel 2: Identifying Risk and Mitigation Strategies for Autonomous/AI/ML Systems** • **Darren Cofer, Collins Aerospace** • **Cody Fleming, Iowa State** • **Junhua Ding, University of North Texas** • **Ering Lanus, Virginia Tech** • **Carl Elks, Virginia Commonwealth University**

10:45am-11:00am	**Break**
11:00am-12:00pm	**Panel 3: Designing Autonomous/AI/ML Systems for Assurance** • **Cody Fleming, Iowa State** • **Stephen Magill, Sonatype** • **Alessandro Pinto, NASA JPL** • **Jaganmohan Chadrasekaran, Virginia Tech** • **Sandeep Neema, Vanderbilt University**
12:00pm-01:30pm	**Lunch (provided)**
01:30pm-02:30pm	**Panel 4: The impact of AI/ML in Application Security** • **Alwyn Goodloe, NASA Langley** **Junhua Ding, University of North Texas** • **Stephen Magill, Sonatype** • **Joanna DeFranco, Penn State**
02:30pm-03:45pm	**Panel 5: Societal Implications: Awareness, Education, Training and Certification** • **Darren Cofer, Collins Aerospace** • **Alwyn Goodloe, NASA Langley** • **Cate Richards, Sonatype** • **Phil Laplante, US National Institute of Standards and Technologies**
03:45pm-04:00pm	**Break**
04:00pm-06:00pm	**Panel 6: Industry-Government perspective (joint with TSP Conference)** **TBA**
06:00pm-8:00pm	**Dinner**

A summary of the findings of the Workshop will appear in IEEE *Computer* magazine and IEEE *Reliability* magazine.

Workshop Organizers

Phil Laplante, NIST phillip.laplante@nist.gov
Rick Kuhn, NIST rkuhn@nist.gov
This workshop is sponsored by the IEEE Reliability Society

The findings of the workshop will appear later in one or more papers published outside of the conference proceedings (in IEEE Computer and Reliability magazines).

Conference Hotel

Atlanta Marriott Buckhead Hotel & Conference Center, Atlanta

3405 Lenox Road NE
Atlanta, Georgia 30326 USA
Phone +1 404-261-9250

Conference Rate
Hotel Booking link for conference attendees: **Click here to reserve at conference rate**.