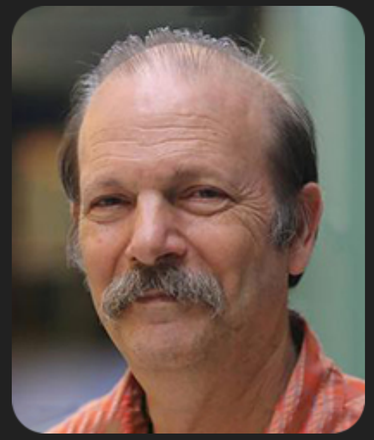
Panel Discussion: Assured Autonomy

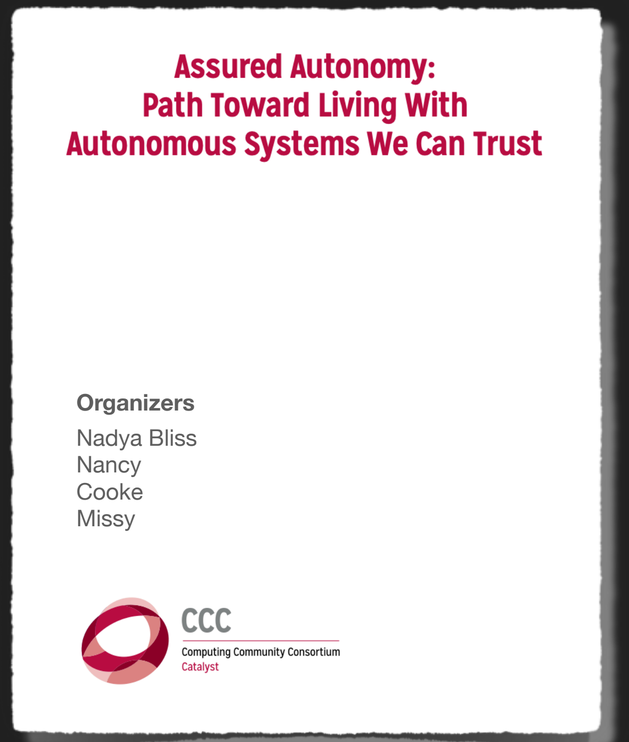
Heather Roff
JHU Applied Physics Laboratory



Moshe Vardi
Rice University

Kymie Tan
Jet Propulsion Laboratory

Missy Cummings
Duke University



Moderator: Ufuk Topcu

Kymie Tan
Jet Propulsion Laboratory

Path Toward Living With Autonomous Systems We Can Trust

Moshe Y. Vardi

Rice University

Houston, TX, USA

vardi@cs.rice.edu

Laudable Goal --Assurance

I completely agree that proper assurances that autonomous systems are safe, secure, dependable, privacy-preserving, fair, equitable, accountable, and ethical are key for positive impact at scale.

Trusting Autonomous Vehicles

- **Question 1**: Do I trust an AV to drive safely?
  - Do I trust tech companies? Cf. Tesla and Uber

- **Question 2**: Do I trust that the AV will not get hacked.
  - Physics World, Aug. 2020: "Any car built with devices that connect to the Internet is vulnerable to a hack, but the threat to autonomous cars is particularly high because computers control so many functions."

Have we earned the public trust?

- Here we are, 75 years into the computer age and we still do not seem to be able to build secure information systems.
- The risk is no longer merely about compromised privacy. We must worry now about the integrity of vital infrastructure components.

Do we deserve the public trust?

- The computing community marches forward with no special sense of urgency.
  - What the report fails to do, IMHO, is to acknowledge the current "**crisis of cybersecurity**".
- The failure is one of attitude, not of aptitude!
  - Unless we change our attitude and adopt the Hippocratic Oath -- "**First, Do No Harm**", the glorious future of autonomous system is bound to fail.

Heather Roff

JHU Applied Physics Laboratory

Missy Cummings

Duke University

Academia vs. industry & government

HAL

	Industry	Government	Academia
Safety	1	4	9
Cybersecurity	2	5	6
System integration	3	8	3
Certification	3	1	15
Software engineering	5	7	6
Testing	6	1	11
Legal and regulatory frameworks	6	15	16
Human-autonomous system interaction	6	1	2
Machine/deep learning	7	11	1
Motion planning	8	9	3
Computer Vision	8	8	3
Perception	12	6	6

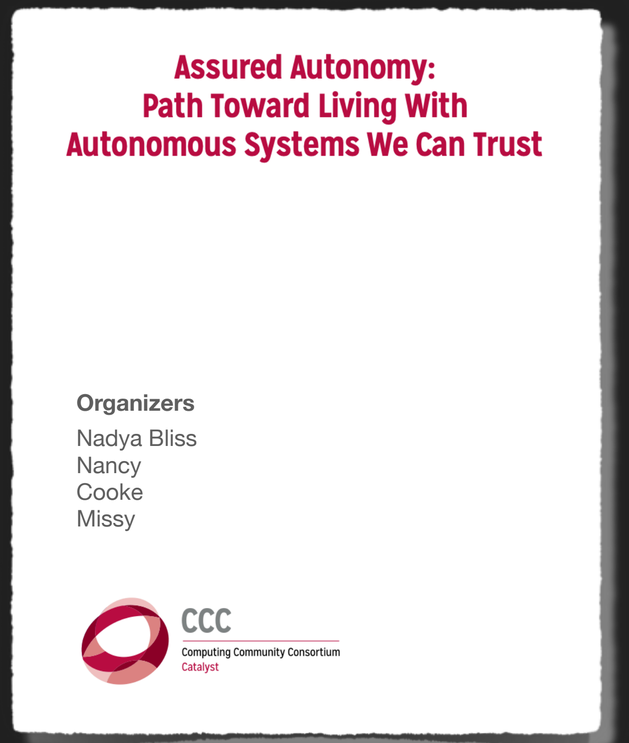
Panel Discussion: Assured Autonomy

Heather Roff
JHU Applied Physics Laboratory

Moshe Vardi
Rice University

Kymie Tan
Jet Propulsion Laboratory

Missy Cummings
Duke University



Scan me!

Moderator: Ufuk Topcu