Apostol Vassilev
NIST ITL

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Lessons Learned from the NIST Automated Vehicle Program

and How They May Apply to Uncrewed Aircraft Systems

Apostol Vassilev

February 1, 2024

Overview

❖ Automated Vehicles Program*

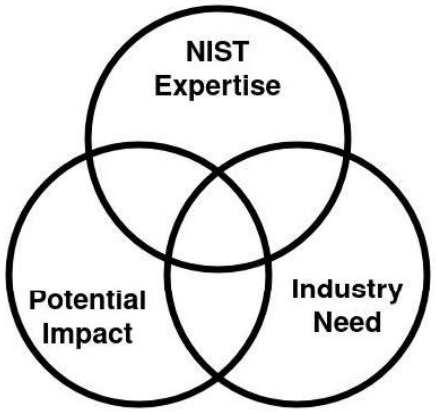
- ❖ SERI (Strategic and Emerging Research Initiatives)
- ❖ Focus:
  - ❖ Address system technology performance and measurement methods
    - ❖ System technologies: Perception sensors, AI, Cybersecurity, and Communications (onboard and offboard)
  - ❖ Design and establish a systems interaction testbed
- ❖ Goals:
  - ❖ Provide the metrology and standards to increase the safety and security of automated vehicles (Avs)
  - ❖ Allow industry to better understand and characterize their AVs' performance
  - ❖ Provide Government agencies the knowledge to create regulations

---

* https://www.nist.gov/programs-projects/nist-automated-vehicles-program

Industry voices

Within NIST scope and expertise/infrastructure is available	Within NIST scope and expertise/infrastructure is lacking (NIST can support agencies)	Not within NIST scope
Develop novel individual and fused sensor measurement science solutions for vehicles	Define the data that should be measured before, during, and after operation of automated vehicles	Create and enforce a baseline for AV safety systems testing
Help define testing guidance for stakeholders to meet regulatory agency requirements	Provide reference materials for what infrastructure investment state and local governments should invest in	Enforce sensor specs that should be used in AVs
Develop mitigation standards for adversarial AI	Collect standardized data from the DoT from accidents to develop representative testing environments	Create regulation on periodic testing and updating
Develop AV simulation-based measurement science	Provide classification and levels for AV components	
Advance standards with SAE, 3GPP, and Teleoperation Consortium		
Develop measurement science for traffic infrastructure that can support AVs		
Develop metrics to identify what aspects of AVs should be measured to ensure safety		
Create test models and measurement science for AV communications		
Foster a community of stakeholders to agree on common taxonomies and standards		
Be a one-stop-shop for pointers to relevant autonomous vehicle standards		
Measure how different parts of an AV work together		
"Do you know that NIST cybersecurity framework? Just do that for autonomous vehicles."		



Outcomes

2023 Standards and Performance Metrics for On-Road AVs Workshop

September 5-8, 2023 (virtual)[Y]

- 619 attendees
- Overall keynote speaker:

Ann Carlson (NHTSA)

- Keynote speakers:

Anuja Sonalkar (STEER)
Cybersecurity

Rajeev Thakur (Ouster)
Perception

David Agnew (Dataspeed Inc)
Systems Interaction

Jim Misener (Qualcomm)
Communication

Aleksander Madry (MIT)
Artificial Intelligence

Ed Straub (SAE)
Infrastructure

[Y] https://www.nist.gov/news-events/events/2023/09/standards-and-performance-metrics-road-automated-vehicles-workshop

Artificial Intelligence

NIST

❖ Artificial Intelligence

Develop mitigation standards for adversarial AI

❖ Contacts:

- ❖ Apostol Vassilev (apostol.vassilev@nist.gov)
- ❖ Send feedback to ai-100-2@nist.gov

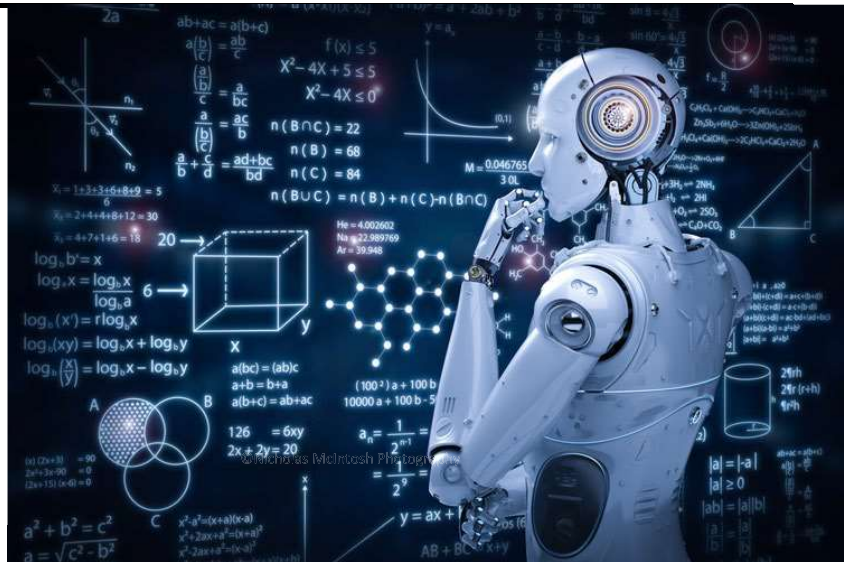
Artificial Intelligence

NIST

- Adversarial Machine Learning (AML)

Work on establishing a methodology for assessing risks and mitigations of attacks on AI models

- **NIST AI 100-2**[†] defines a taxonomy of attacks and mitigations in AML.
- Can be used in conjunction with the **NIST AI RMF**[‡] to identify and manage risks.



[†] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

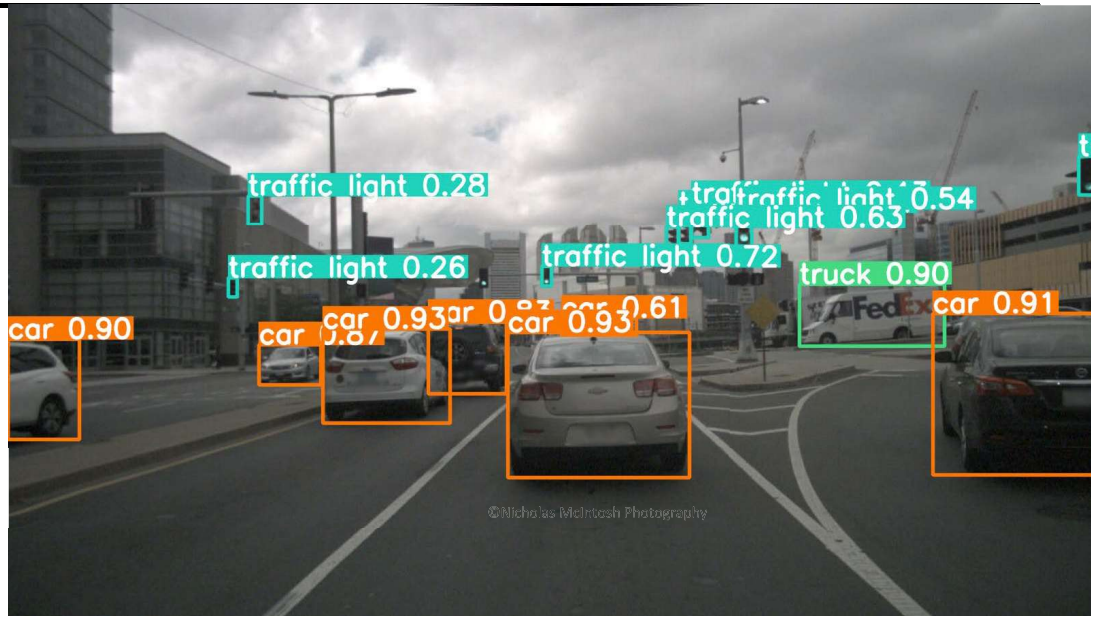
[‡] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Artificial Intelligence

❖ Uncertainty Estimation for AI in AVs

Work on establishing a methodology for assessing robust measurement of uncertainties in AI models used in the perception and other systems of the vehicle

- ❖ Predictive Uncertainty Estimation helps to reduce the cascading propagation of risk in the systems of the car
- ❖ This effort will allow quantification of risk in AI for AVs and UAS



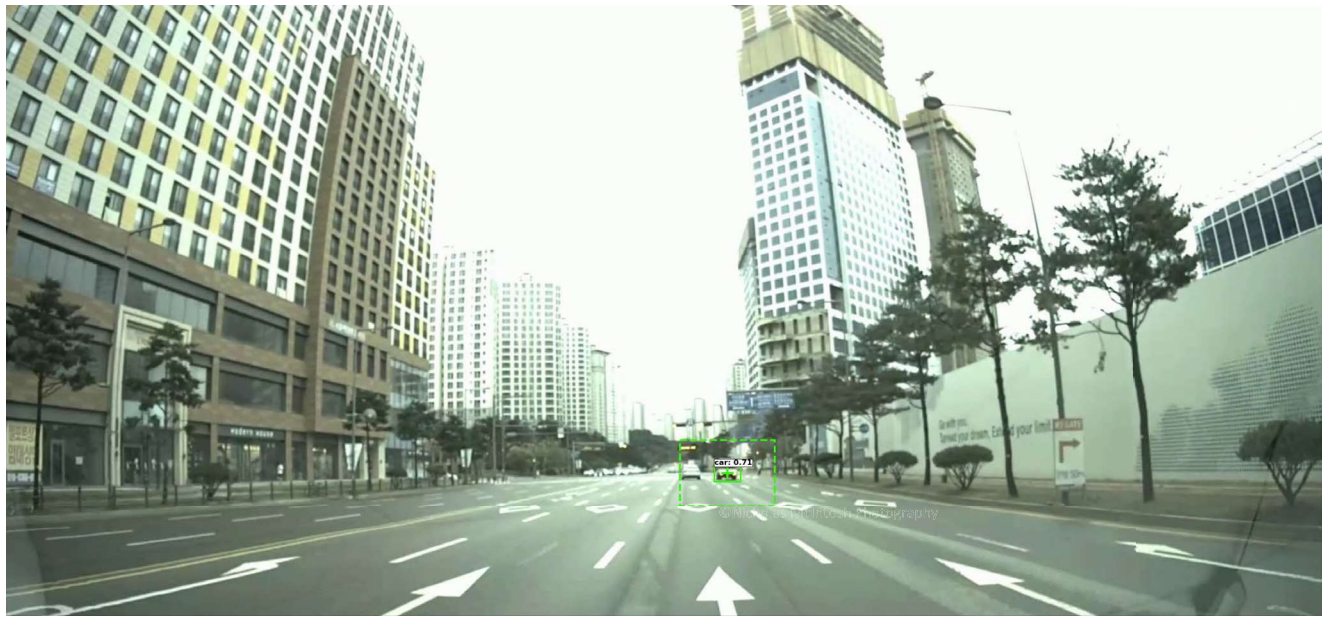
Artificial Intelligence

❖ Next Steps

Investigate the dependency of uncertainty on vehicle speed and distance to object

- ❖ View from a far, high speed, time T_0
- ❖ Dashed line box indicates the positional uncertainty around an object
- ❖ The model does not distinguish yet the car and the truck in front

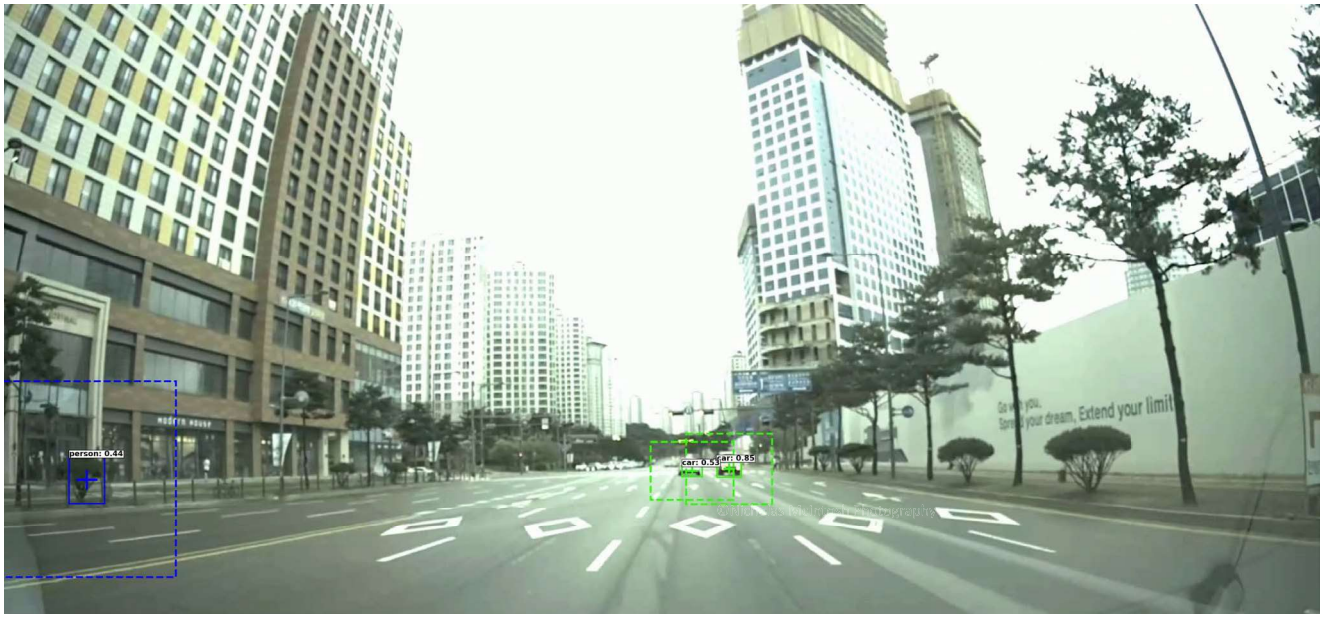
Example w/ Gaussian YOLO v3



❖ Next Steps

Investigate the dependency of uncertainty on vehicle speed and distance to object

- ❖ Getting closer, high speed, time T_1
- ❖ The model is now able to detect the two objects but the truck in front is misclassified as a car, a bush misclassified as a person
- ❖ Large uncertainty boxes

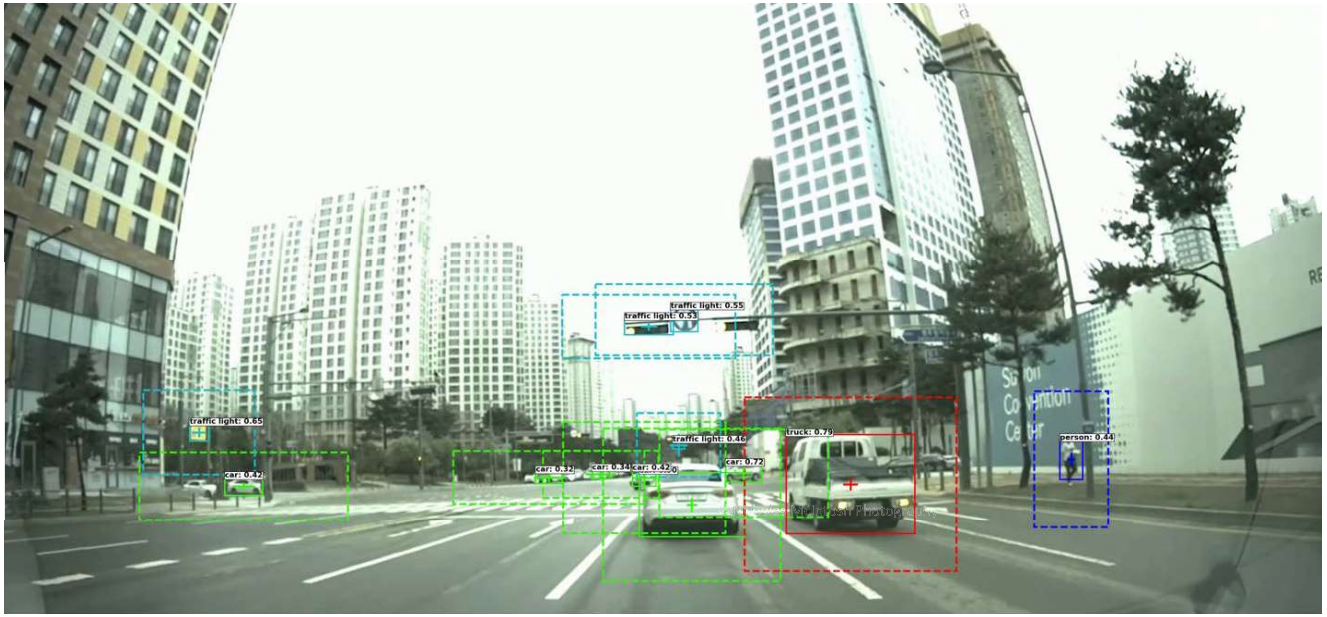


Artificial Intelligence

❖ Next Steps

Investigate the dependency of uncertainty on vehicle/system speed and distance to object

- Getting close, low speed, time T_2
- The model's object detection improves and picks up multiple objects: pedestrian (in blue), cars (in green), a truck (in red), etc.
- Smaller uncertainty boxes around the closest objects
- Larger uncertainty boxes around far objects



Artificial Intelligence

NIST

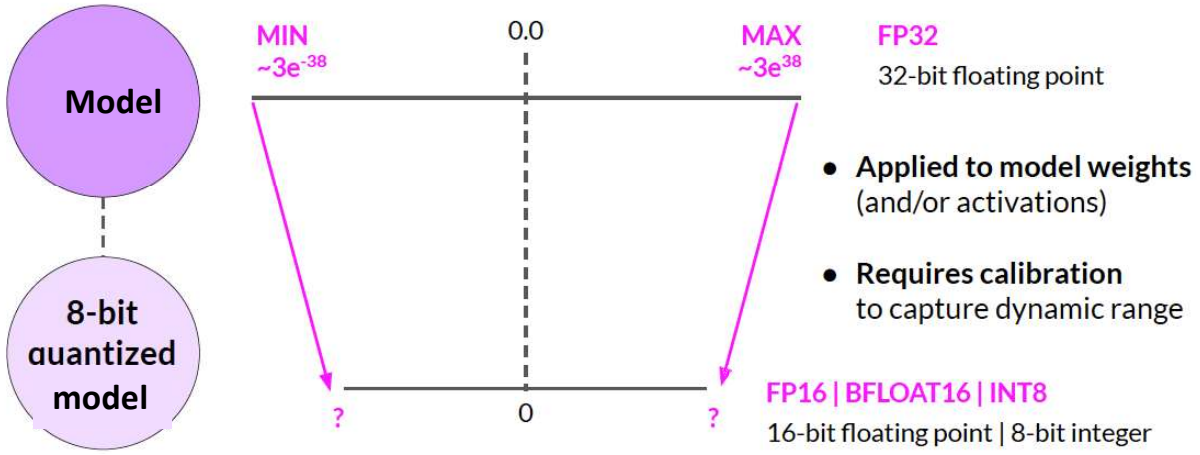
❖ Quantization

*Investigate the effects of **quantization** on the robustness and security of AI models used in UAS*

- **Quantization** helps to fit AI models into the constrained computational resources of the UAS
- However, **quantized models** DO inherit the vulnerabilities of the original models and bring in additional weaknesses
- Quantized models are **vulnerable** to adversarial attacks.

Post-Training Quantization (PTQ)

Reduce precision of model weights



Thank you !

- Questions and comments

  Send to: apostol.vassilev@nist.gov

Artificial Intelligence Disclaimer

NIST

- Disclaimer

Certain commercial hardware, open source software, and tools are identified in this presentation in order to explain our research. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the software tools identified are necessarily the best available for the purpose.