Towards Continuous Assurance for Autonomy Software

Sayan Mitra

Reliable Autonomy Research Group

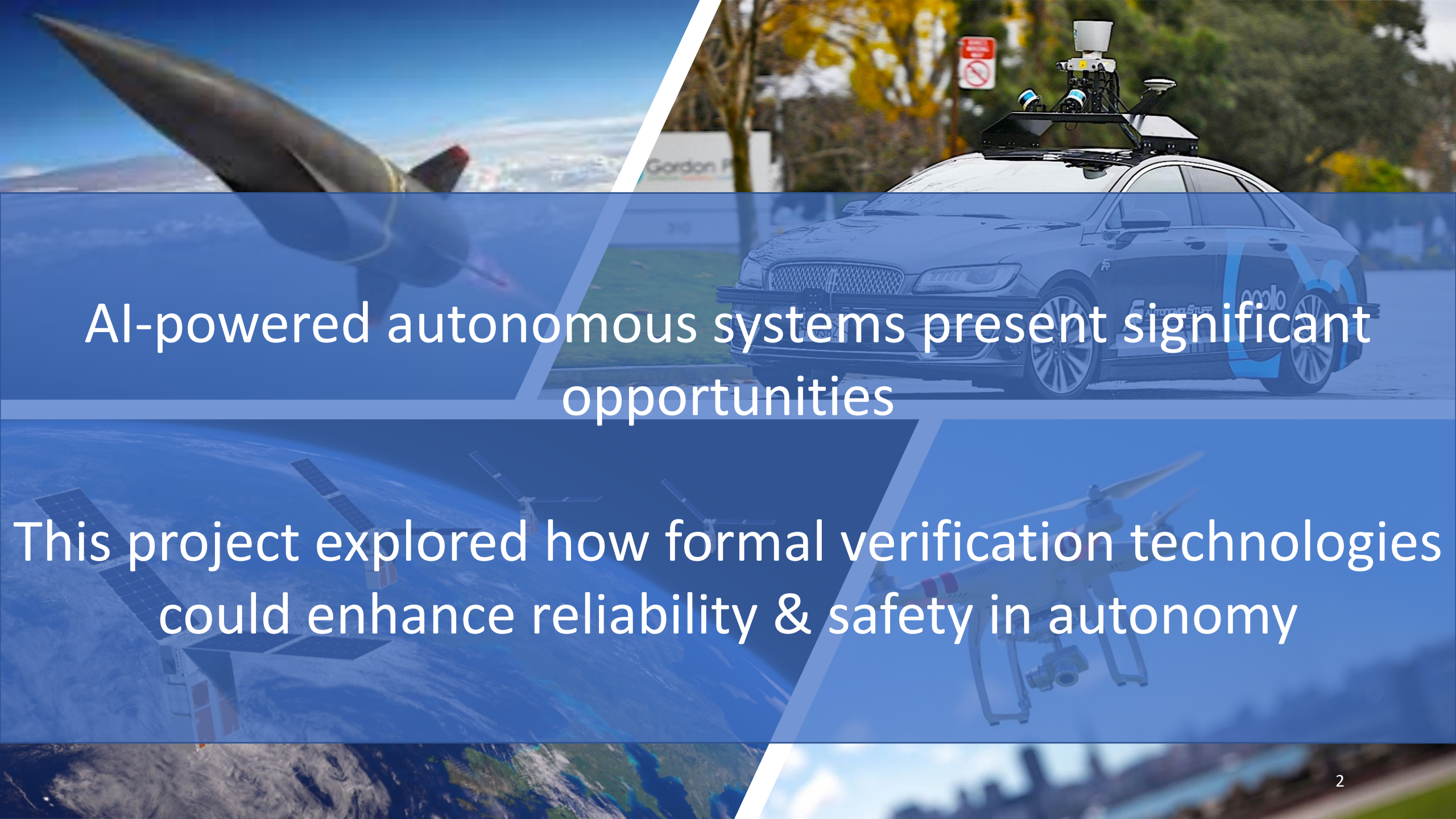
University of Illinois at Urbana-Champaign

Computational Cybersecurity in Compromised Environments (C3E)

October 2021

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

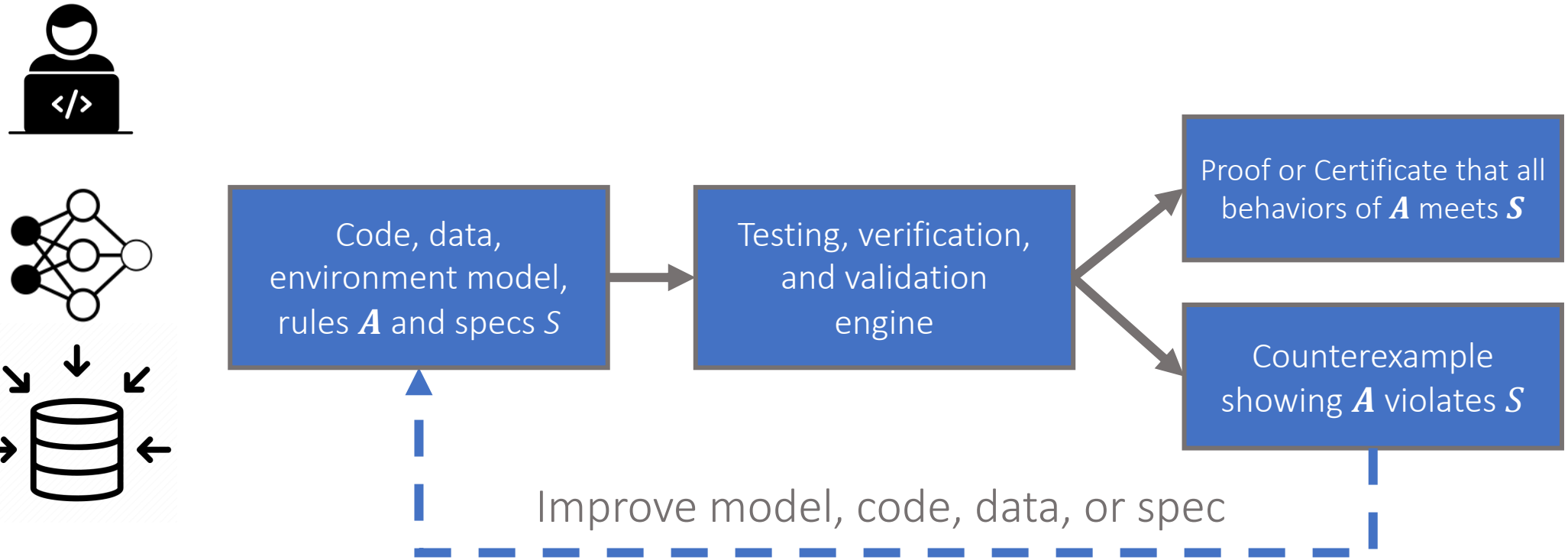
@Mitrasayn



AI-powered autonomous systems present significant opportunities

This project explored how formal verification technologies could enhance reliability & safety in autonomy

Development & maintenance workflow for autonomous systems



How fast can this loop close with changes in {data, env specs, code} ?

Continuous Integration and Testing

Static analysis part of developer workflow at Google

Infer prover running on iOS, android WhatsApp code

Specs and proofs for hypervisors, boot loaders, IoT OS being written by AWS developers

Verification must communicate with developers using artifacts/APIs that are already part of workflow

New languages/formalisms are non-starters

150 million tests/day on a compute farm; 1000s bug reported & fixed

100s bug reports and fixed every month [3]; runs on a "diff" in about **10-15 minutes**

[2] 4 yr experience: loss of expressive power (not using TL) more than made up by benefits of using same language for code & spec

[1] Sadowski, et al. Lessons from Building Static Analysis Tools at Google. CACM, 2018.

[2] Chong, et al. Code-level model checking in the software development workflow. ICSE, 20.

[3] O'Hearn. Continuous reasoning: Scaling the impact of formal methods. LICS '18.

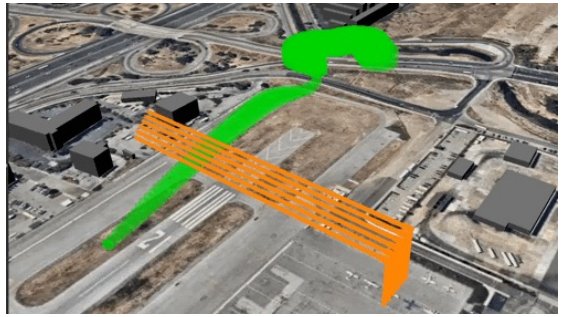
Data-driven verification successes

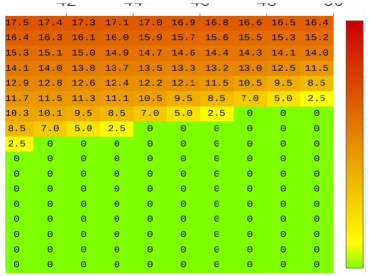
Safety analysis of UTM protocols with fixed-wing and quadrotor models [IEEE ITSC 2021]

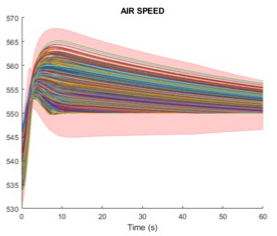
Automatic Emergency Braking (AEB) risk analysis for ISO26262 [IEEE DT 2018]

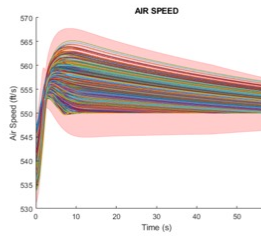
Quadrotor with NN controller exploiting symmetries [CAV 2020]

Safety of Auto Ground Collision Avoidance System (GCAS) for F16 [Ongoing]



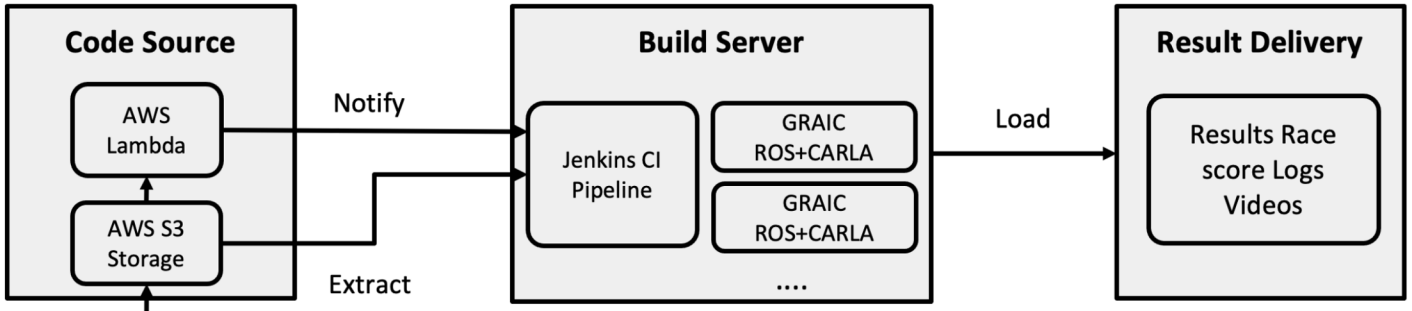




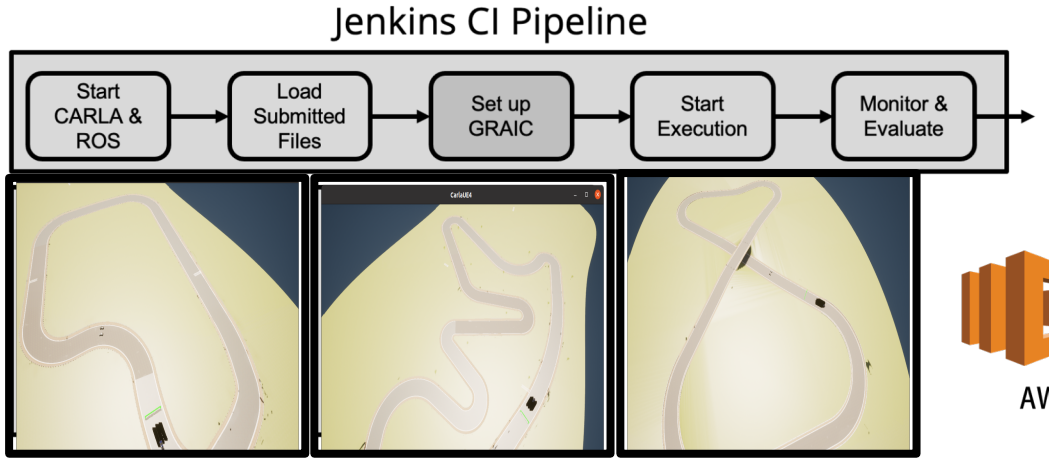


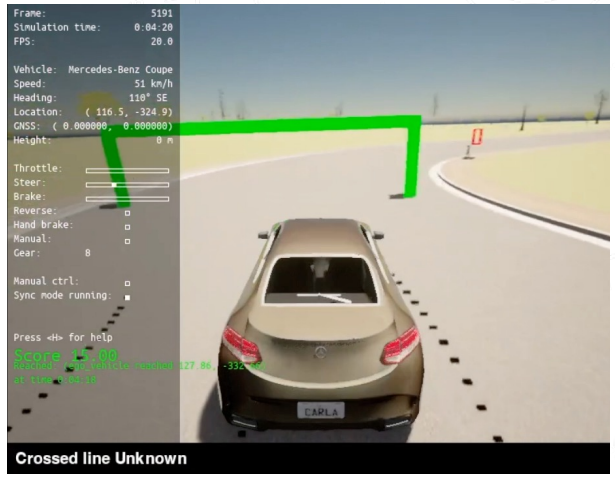
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Continuous Testing for Autonomy:
straightforward setup for addressing hard challenges



Controller code
Race submission





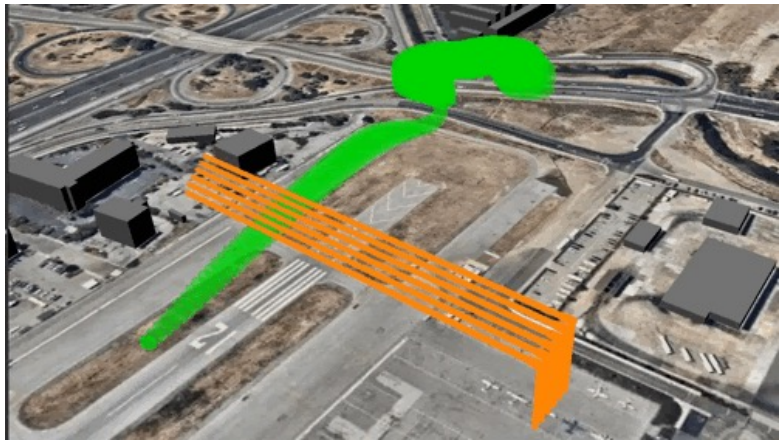
AWS Lambda docker Jenkins

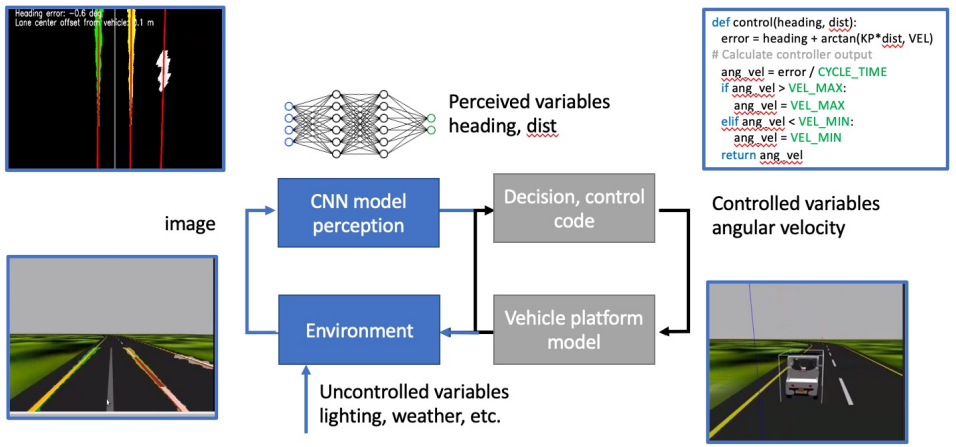
GRAIC Testing V&V pipeline

Continuous integration and testing for autonomous racing software: An experience report from GRAIC. Jiang, Miller, Sun, Liu, Jia, Datta, Ozay, and Mitra. ICRA 2021 Workshop on Opportunities and Challenges in Autonomous Racing.

Challenges and future directions

- Nondeterminism:
  - Communication delays
  - Sensor and perception system
- Perception systems
  - Analysis of autonomy pipeline with AI-powered perception modules
- Ongoing approaches:
  - Exploiting symmetries for Testing ACAS SxU with autonomous air vehicles [Sibai et al. 2021]
  - Intelligible abstractions for safety analysis of vision-based lane following control [Hsieh et al 22]





UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN