CPS: Medium: Safety Assured, Performance Driven Autonomous Vehicles

Mark Campbell, Edward Suh, Cornell University
CNS-2211599, 7/2022-6/2025

Challenge:

Deployment of autonomous vehicles requires addressing <u>rare events</u> with hardware/software/algorithm solutions:
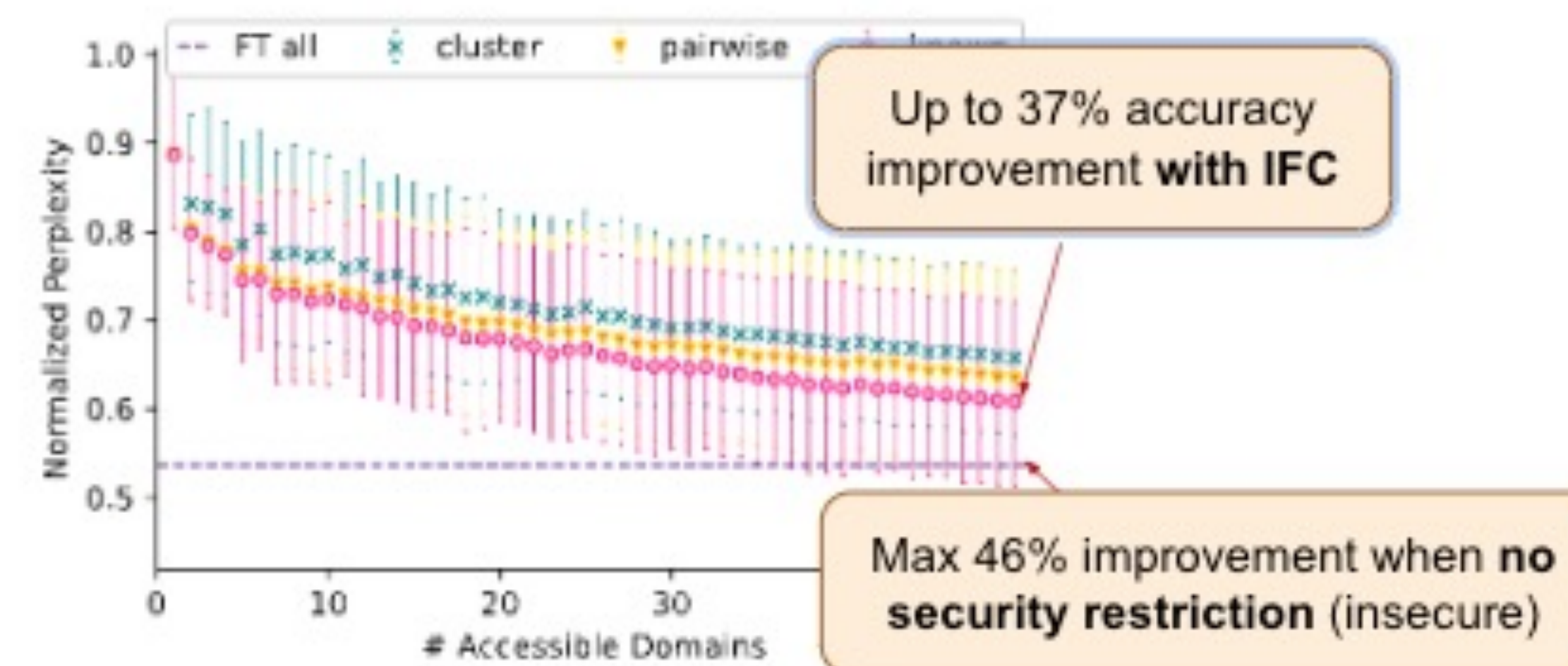- perception errors, environmental anomalies, cyber-attacks

Scientific Impact:

- Directly addresses rare events broadly applicable to CPS
- Solutions inherently coupled in HW+ SW/algorithms
- Balance Safety & Performance

Solution: Safety Assured (with guarantees), Performance Driven (adapt), Self-Improving (learn over time) architectures
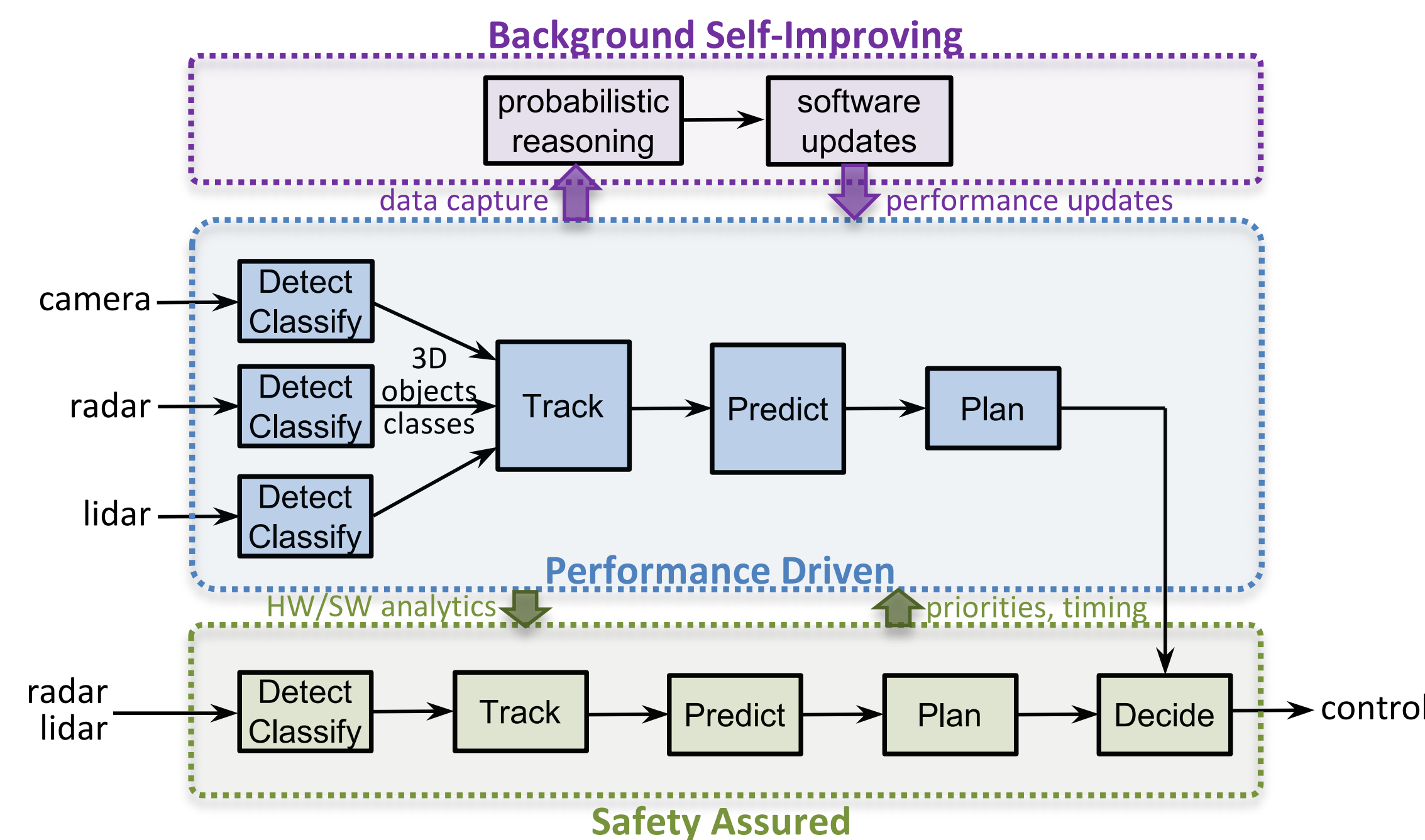

Information Flow Control (IFC) for ML:

- Remove (unlearn) bad data without full re-training via transformers

Up to 37% accuracy improvement **with IFC**

Max 46% improvement when **no security restriction** (insecure)

Physics + deep learning predictions:

- Closed loop, physics driven forecasting for collision evaluation

high probability collision

uncertainty ellipses

initial time
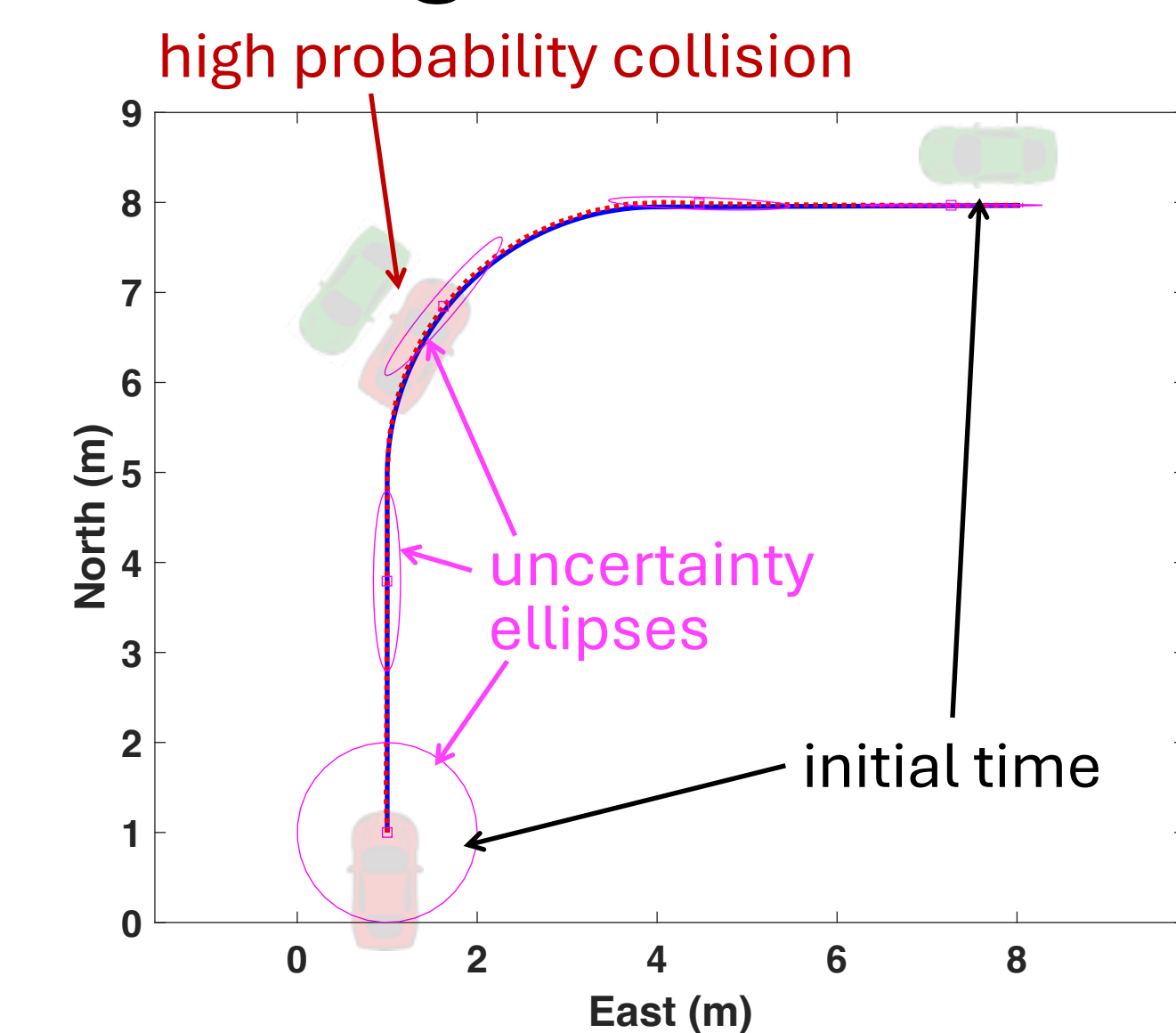
Broader Impact (society):

- CPS with safety/performance reqmts: self-driving cars, delivery robots, etc.
- Enable longer operations with robust solutions to rare events

Broader Impact (outreach):

- Improve Female/URM transitions: HS-UG-grad-faculty
- Programs: LSAMP, CURIE, CATALYST, 4-H, research groups

Broader Impact (metrics):

- Probabilistic guarantees of safety
- Convergence speed/accuracy of collision probability, contingency plans
- % rare events impacting safety