CAREER: Decision Procedures for High-Assurance AI-controlled CPS

Yasser Shoukry

Resilient Cyber-Physical Systems Lab
Electrical Engineering and Computer Science Department
University of California, Irvine
Webpage: https://rcpsl.eng.uci.edu/yshoukry/
Email: yshoukry@uci.edu

Award Number: 1845194

Poster Number: 146, Friday 3:00-4:00 pm

Resilient CPS Lab

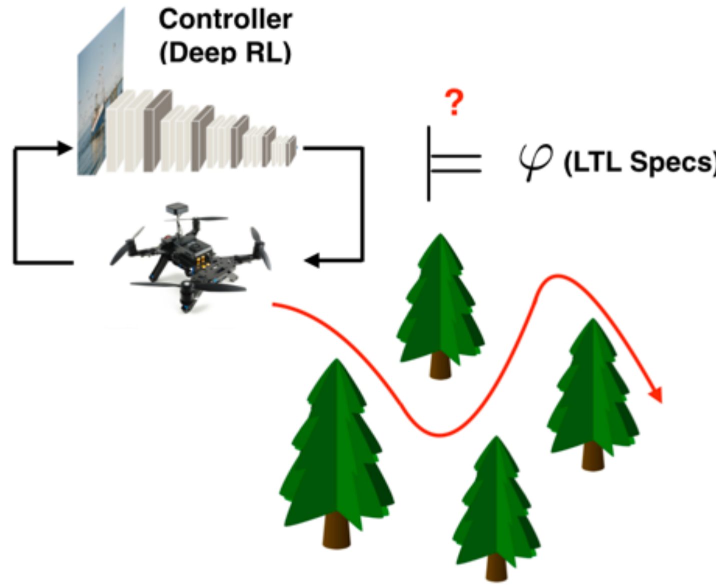
Formally Verified AI-controlled CPS

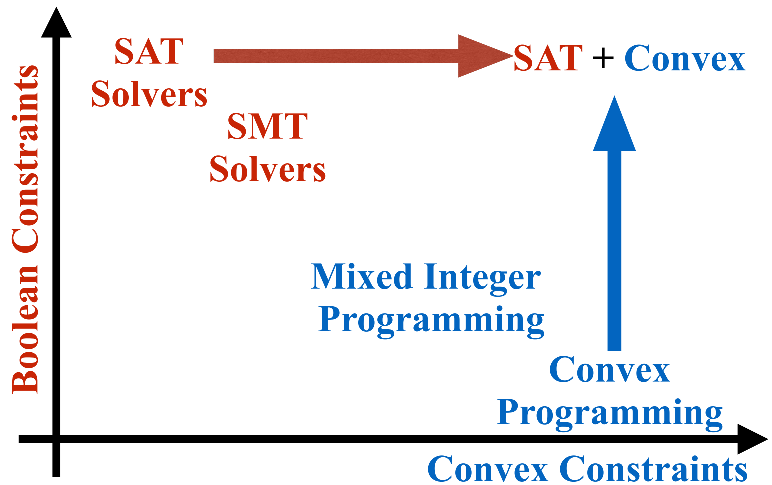
Goal: Develop formal methods to reason about the safety and reliability of AI-controlled CPS providing a scientific basis to understand their fundamental properties and guide their design.

- **Model-based Verification of AI-controlled CPS:** Use model-based techniques to verify data-driven models to provide formal guarantees on their safety and reliability.

- **Blame Analysis in failed, yet formally verified AI-controlled CPS:** A formally verified system may still fail due to the discrepancy between models used for verification and the real system.

- **Scalable decision procedures for AI-controlled CPS:** Combine ideas from SAT/SMT solvers and convex programming towards a scalable framework to reason about AI-controlled CPS.

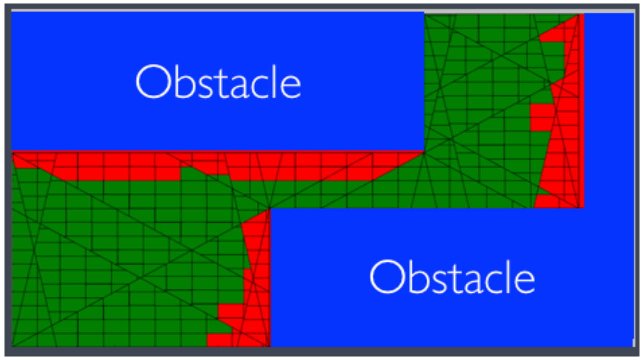


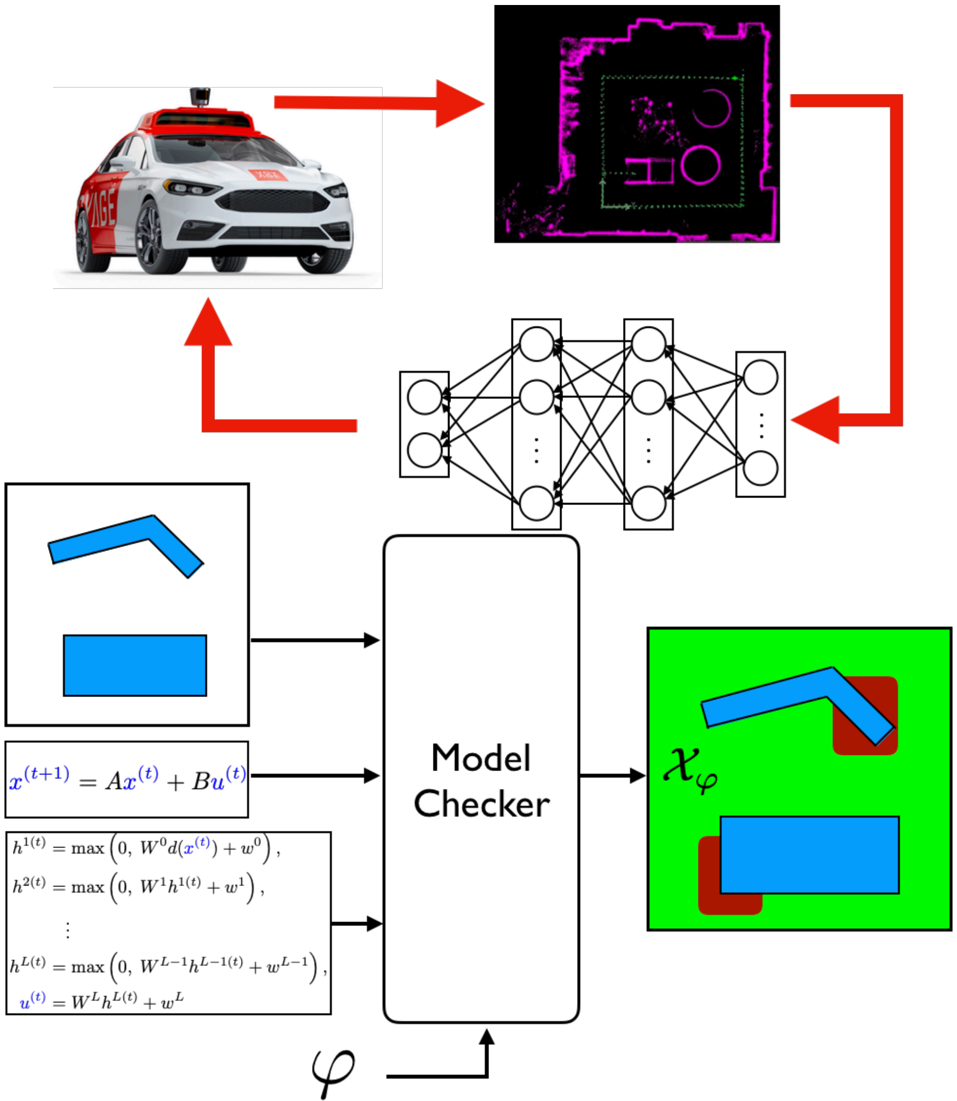


Resilient CPS Lab

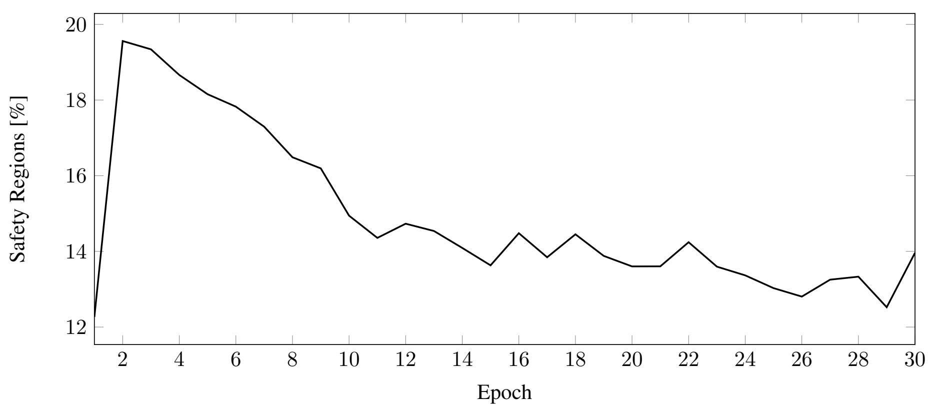
Model Checking for Deep RL

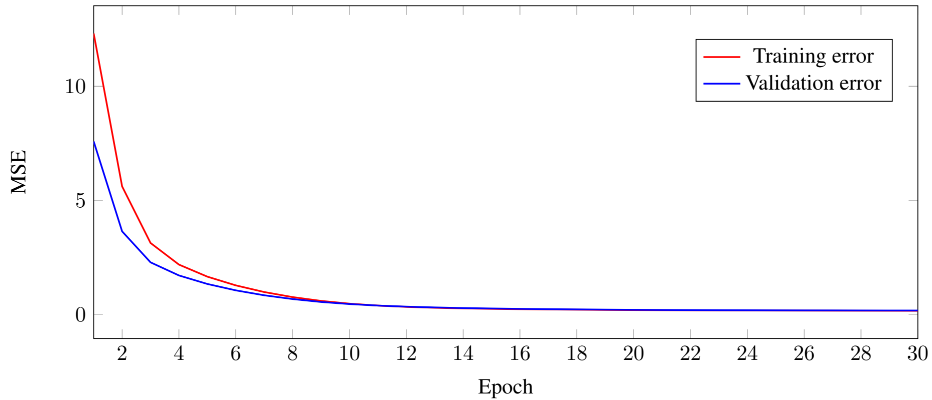
- **Model Checking for Deep RL:** Characterize the environments for which a neural-network controlled autonomous robot will violate safety specifications.





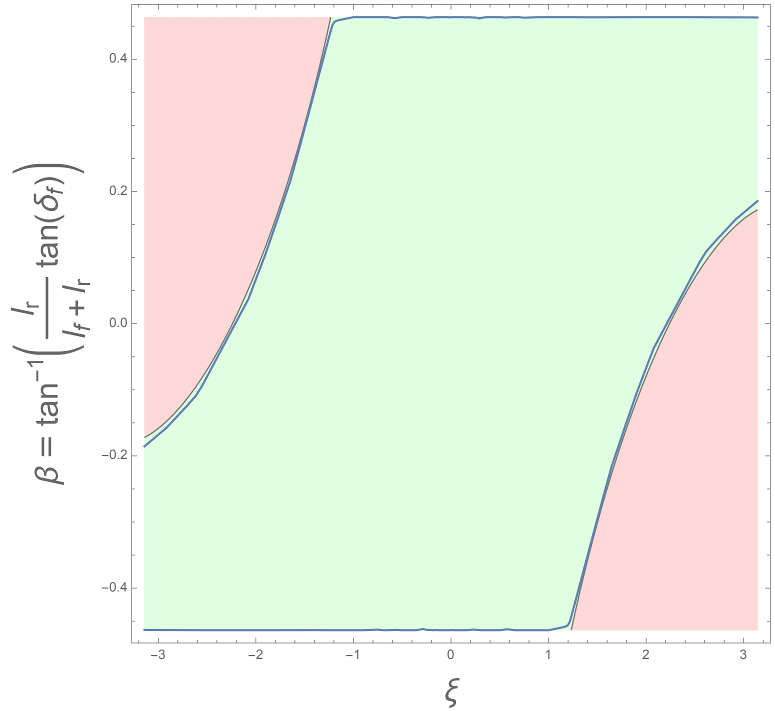
- **Safety vs Learning:** Empirically understand how safety evolves during the training phase of neural networks.

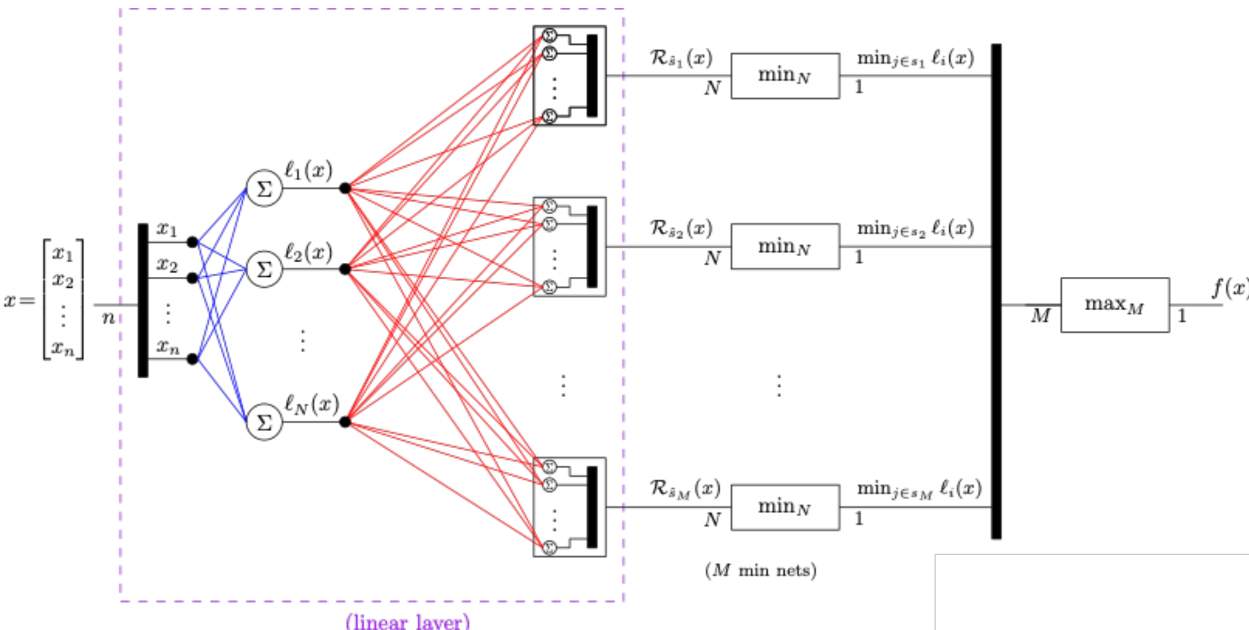




Certifiable DNN Architectures

- **Certifiable DNN Architectures:** Compute a neural network architecture (number of layers and number of neurons/layer), such that the NN is guaranteed to be equivalent to a Model Predictive Controller.
- **Synthesis of DNN-based Barrier Functions :** Construct a DNN-based control barrier function to ensure the safety of autonomous robots during the training phase of the neural network.





- **Education:** new undergrad and grad classes on safe autonomy.
- **Outreach:** STEM Scouts (K-5) – AI4ALL (9-12) – Tech + Research: Welcoming Women to Computing Research (undergraduate).

Poster # 146, Friday 3:00-4:00 pm

Resilient CPS Lab