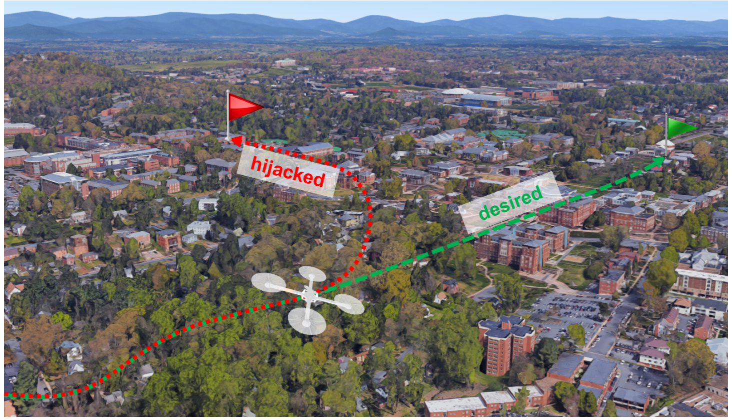
Online Malicious Intent Inference for Safe CPS Operations under Cyber-attacks

UVA ENGINEERING
LINK LAB

Challenges:

- Identify/predict the *intent* of an attack on an autonomous CPS
- Defend, control, and reconfigure the compromised CPS to guarantee safety



Scientific Impact:

The proposed framework will:

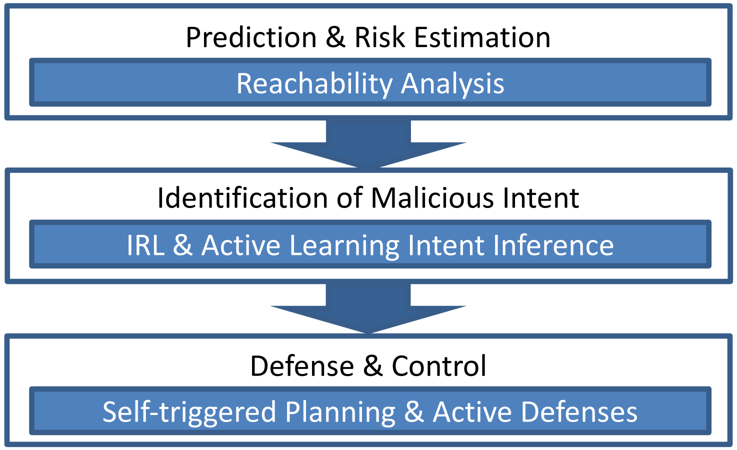
- increase resiliency against cyber-attacks on autonomous systems
- improve system's safety and trust

Solution:

- Behavior prediction via reachability analysis
- Intent inference via inverse reinforcement learning and active learning
- Self-triggered replanning

Award #1816591
University of Virginia
PI: Nicola Bezzo nbezzo@virginia.edu
https://www.bezzorobotics.com

Proposed Framework



Prediction & Risk Estimation

Reachability Analysis

Identification of Malicious Intent

IRL & Active Learning Intent Inference

Defense & Control

Self-triggered Planning & Active Defenses

Broader Impact:

- The proposed framework will contribute to the development of safe autonomous systems and CPS broadly.
- The intent inference solution is applicable beyond cyber-security problems.
- Planned education activities include the development of CPS security courses and outreach activities