



CAREER: Synthesis and Control of Cyber-Resilient CPS

Andrew Clark

Dept. of Electrical and Computer Engineering, WPI

aclark@wpi.edu

NSF CPS PI Meeting CAREER Panel

June 2, 2021

Cyber-Physical Resilience

- High-profile attacks against energy, transportation, and IoT CPS have led to economic cost and safety risks
- Adversaries are increasingly sophisticated
- Growing complexity of CPS creates a large attack surface
- Cyber-Physical Resilience: Ensure safety and performance of CPS *even after compromises occur*

NATIONAL SECURITY

What We Know About The Ransomware Attack On A Critical U.S. Pipeline

Updated May 10, 2021 · 8:29 PM ET

SCOTT NEUMAN



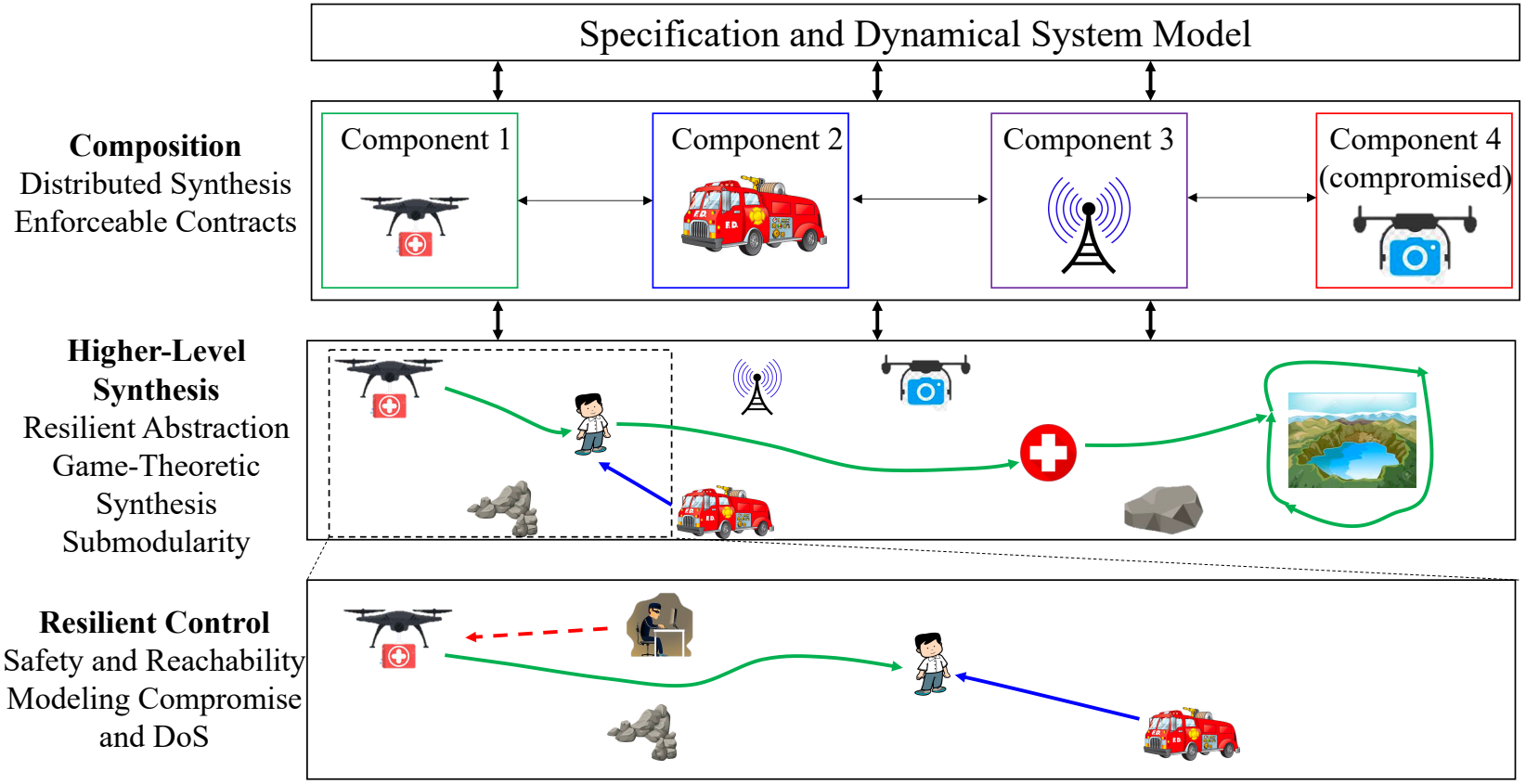
New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction

Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles

Researchers try out methods of jamming and spoofing the car's radar, ultrasonic sensors, and cameras---with disturbing results.

Goals of This Project

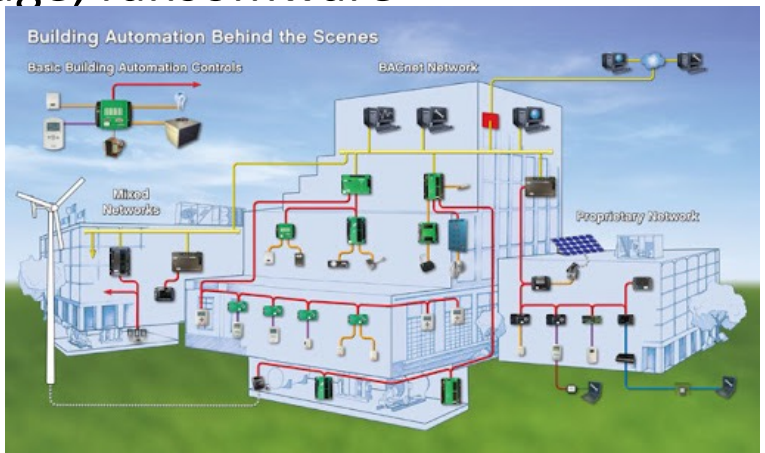
Develop models and algorithms to ensure CPS security and performance even when a subset of system components is compromised



Application Domains

- Autonomous vehicles
  - Must satisfy safety (collision avoidance, lane-keeping) and performance (fuel efficiency, reaching desired destination) requirements
  - System compromises: denial-of-service of V2V communication; false data injection into onboard sensors; software and protocol vulnerabilities of ECUs
- Industrial control systems (e.g., building automation)
  - Safety requirements of humans in the loop
  - Software vulnerabilities lead to equipment damage, ransomware



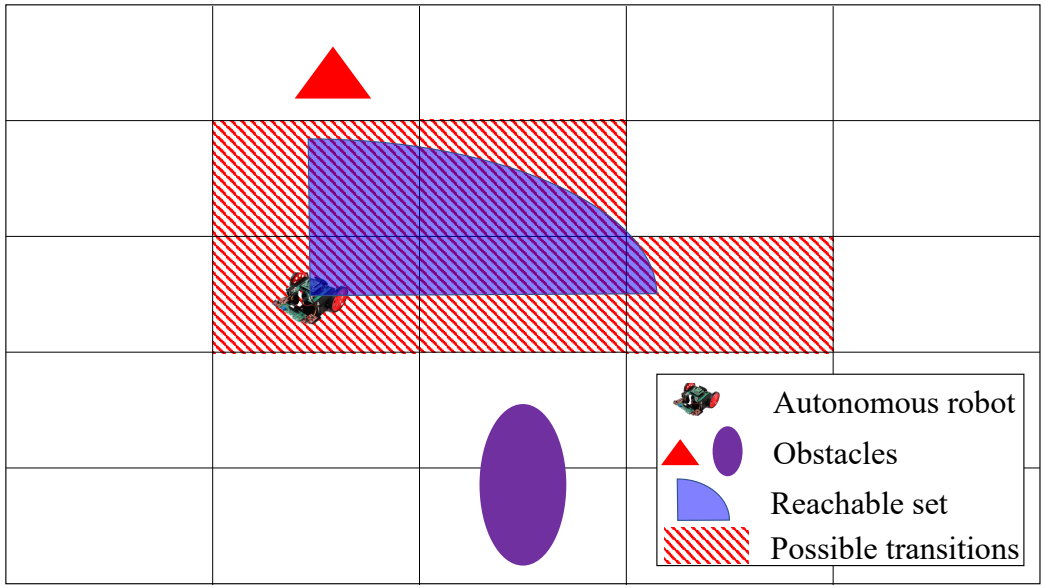


Thrust One: Resilient Nonlinear Control

- Real-time feedback controllers that satisfy *safety* and *reachability* requirements under *sensor compromise, actuator compromise,* and *denial-of-service attacks*
- Approach: New class of *attack-resilient* and *fault-tolerant* Control Barrier and Control Lyapunov Functions (CBFs/CLFs)
- Improve scalability via *abstraction-free synthesis* to satisfy high-level requirements

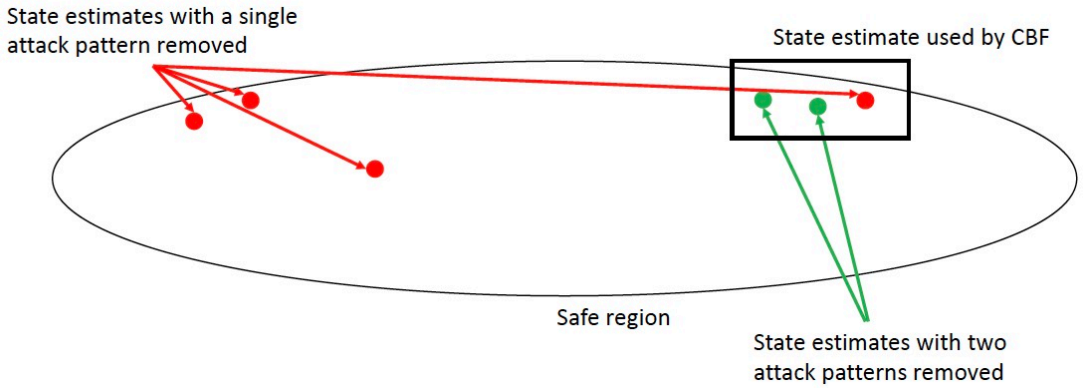
Thrust Two: Resilient High-Level Task Performance

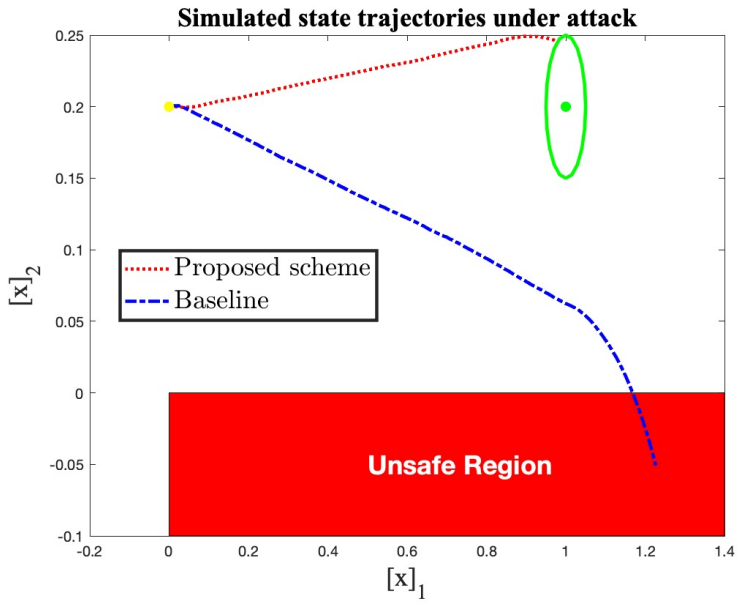
- Satisfy high-level requirements (temporal logic specifications) under malicious attacks
- Formulate stochastic games that jointly capture system dynamics, adversary strategy, and logical requirements
- Develop resilient abstractions that capture the impact of adversaries
- Compose secure systems via *enforceable contracts*



Preliminary Results: Resilient CBFs Under Sensor Attacks

- Sensor attacks bias the state estimate, leading to safety violations
- Control Barrier Functions ensure safety via linear constraints on control signal
- Our approach: introduce multiple CBFs, one for each attack pattern
- Key challenge: Identify and remove conflicts between estimates to ensure constraints are feasible





Education and Outreach Activities

- Undergraduate capstone projects as part of WPI's IQP/MQP program
- K12 and public outreach: Talks at local high schools, TouchTomorrow event at WPI
- Serious games for education and outreach
- Modules for undergraduate and graduate control courses

