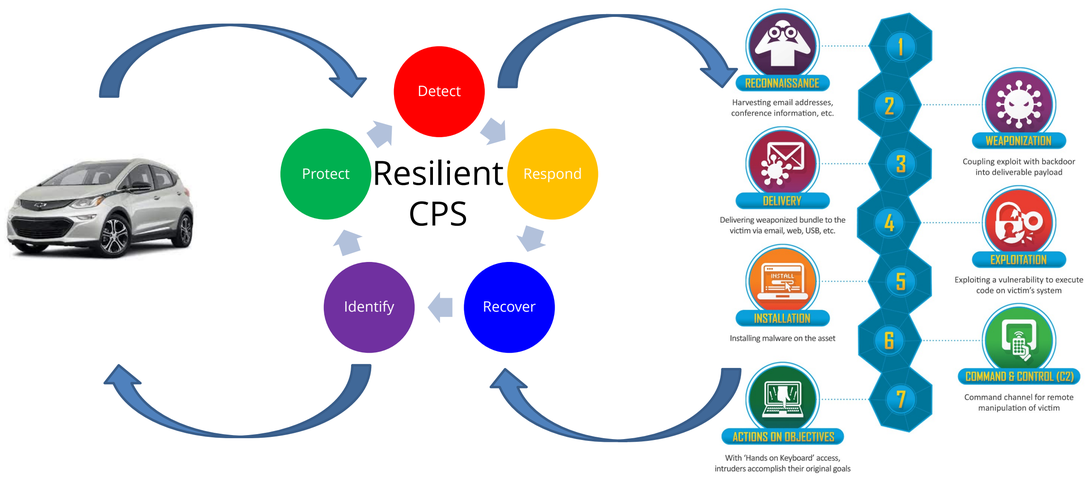
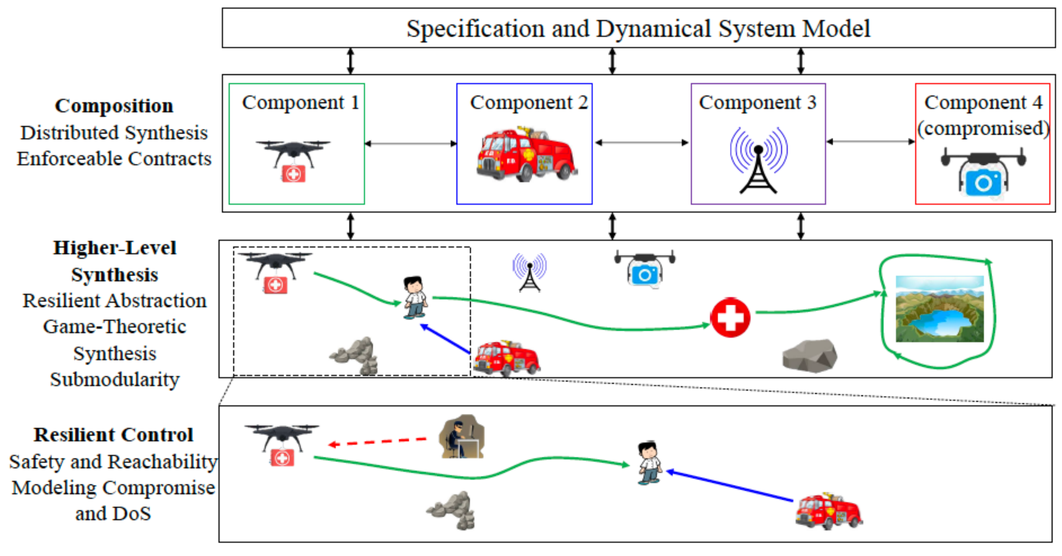
CAREER: Synthesis and Control of Cyber-Resilient CPS

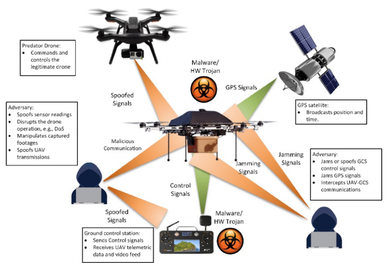
PI: Andrew Clark, Dept. of Electrical and Systems Engineering, Washington University in St. Louis. Email: andrewclark@wustl.edu





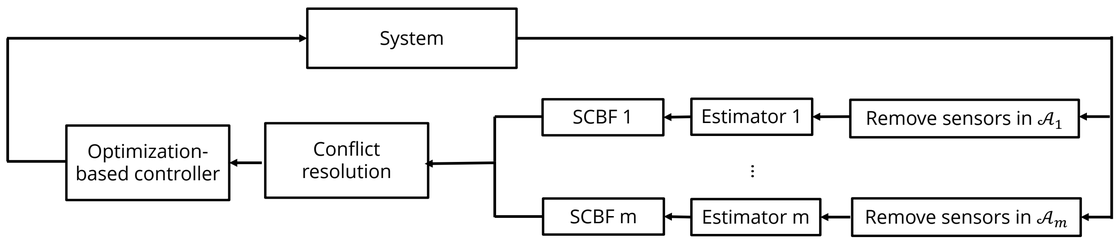
Challenges

- CPS targeted by malicious attacks
- Large attack surface
- Must satisfy safety and performance requirements during and after attacks



Scientific Impact

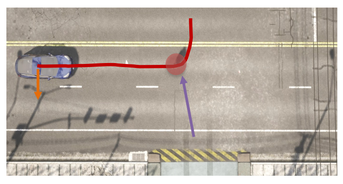
- Algorithms for safety and performance under malicious attacks
- Scalable verification of safety and resilience
- Modeling impact of cyber attacks on complex specifications (liveness, task



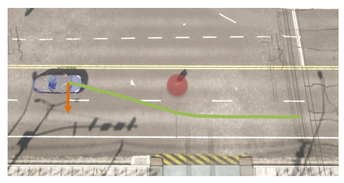
Solutions

- Resilient Control Barrier and Lyapunov Functions for safety and stability
- Algebraic-geometric framework for safety verification
- Verifiable safety under Lidar spoofing

- Discretization-free synthesis to satisfy task specifications
- Safe and resilient learning algorithms



Sensor attack



Proposed safe control

Impact on application domains:

- Autonomous vehicles: Safety under sensor attacks
- Industrial control systems: Resilience to system compromise and malware

Education and Outreach:

- Undergraduate summer research mentoring
- Public outreach

References:

[1] Z. Li, L. Niu, and A. Clark, "LQG Reference Tracking with Safety and Reachability Guarantees under Unknown False Data Injection Attacks." To appear in IEEE Transactions on Automatic Control (TAC), February 2023.

[2] A. Clark, "Control Barrier Functions for Stochastic Systems." Automatica, vol. 130, 2022.

[3] H. Zhang, J. Wu, Y. Vorobeychik, and A. Clark, "Exact Verification of ReLU Neural Control Barrier Functions." Advances in Neural Information Processing Systems (NeurIPS), 2023.

[4] L. Niu, Z. Li, and A. Clark, "Abstraction-Free Control Synthesis to Satisfy Temporal Logic Constraints under Sensor Faults and Attacks." IEEE Conference on Decision and Control (CDC), 2022.

[5] H. Zhang, Z. Li, S. Cheng, and A. Clark, "Cooperative Perception for Safe Control of Autonomous Vehicles under LiDAR Spoofing Attacks." In Symposium on Vehicle Security and Privacy (VehicleSec), 2023. **General Motors Autodriving Security Award.**

[6] L. Niu, D. Sahabandu, A. Clark, and R. Poovendran, "Verifiable Safety for Resilient Cyber-Physical Systems via Reactive Software Restart." IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS), 2022.

[7] A. Clark, "Verification and Synthesis of Control Barrier Functions." IEEE Conference on Decision and Control (CDC), 2021.

Washington University in St. Louis
James McKelvey School of Engineering

Award ID#: CNS-1941670