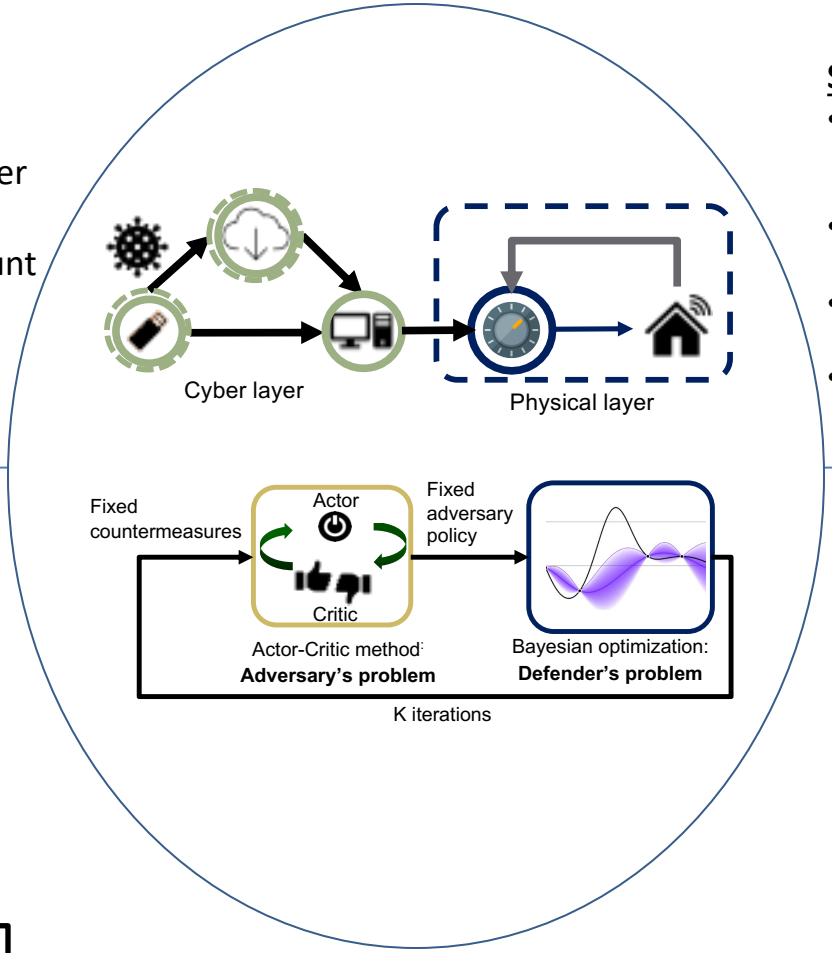
SaTC: CORE: SMALL: Data-driven Attack and Defense Modeling for Cyber-physical Systems (CPS)

MICHIGAN STATE UNIVERSITY

Challenge:

- Coupled security requirements between cyber and physical layers of a CPS
- Continuous search to account for newer vulnerabilities

Goal: Develop a **data-driven** framework for CPS security



Solution:

- Automated strategies to characterize attacker intent using **reinforcement learning**
- Integrated defense to guide countermeasures using **game-theoretic methods**
- Realistic validations in **intelligent buildings** applications

Project info (#2134076, Michigan State University, PI: Shaunak D. Bopardikar, shaunak@egr.msu.edu)

Scientific Impact:

- Systematic deployment of countermeasures for resource constrained CPS
- Quantifying fundamental limits on performance loss
- Security principles for Learning-enabled CPS
- Increased readiness to zero-day attacks

Broader Impact and Broader Participation:

- Societal: Security of power grids and vaccine distribution
- Collaboration with Pacific Northwest National Lab
- Interactive attacker-defender games for STEM aspirants
- Include at least one underrepresented student in project demos. Serve as mentor to at least one schoolteacher under NSF RET