CAREER: Towards Non-Conservative Learning-Aided Robustness for Cyber-Physical Safety and Security

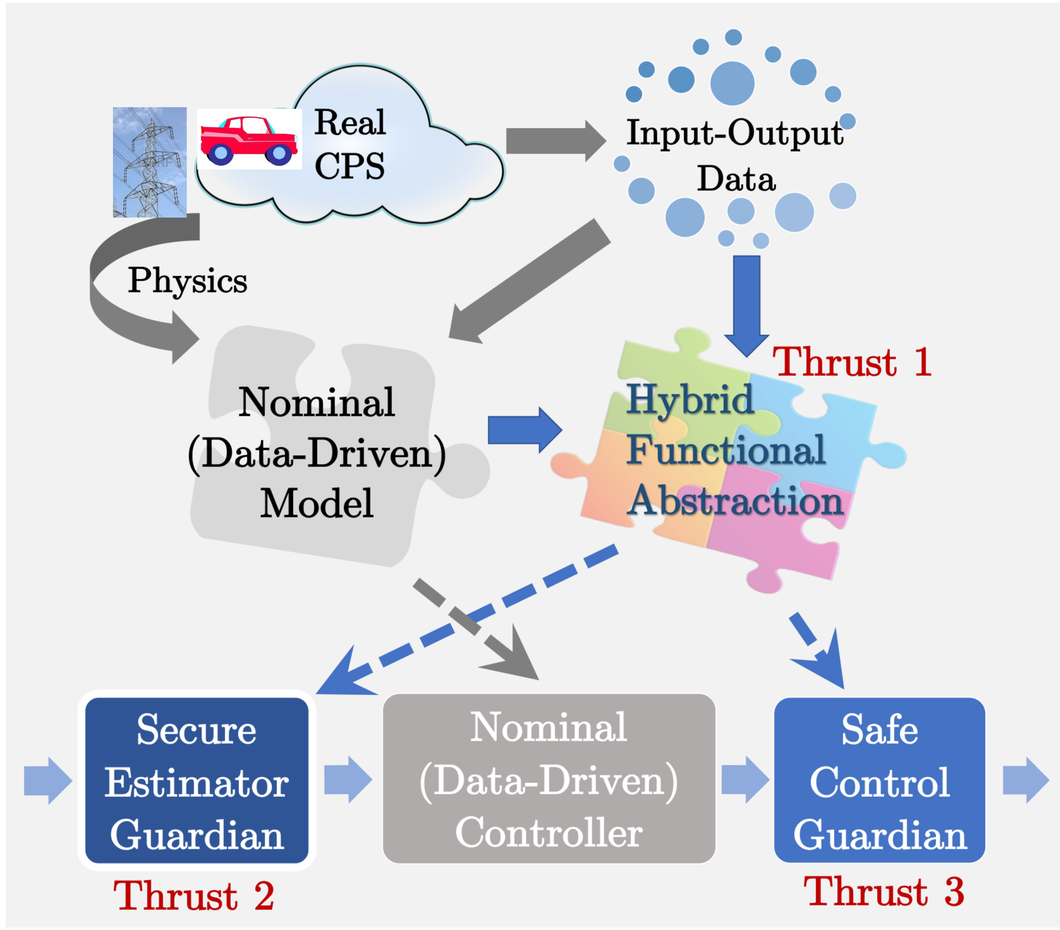
Sze Zheng Yong, Northeastern University/Arizona State University

Challenge:

- Model mismatch and uncertainties jeopardize safety and security guarantees
- How to quantify and learn uncertainty model?
- How to keep a system secure and safe while learning?

Solution:

- Characterize uncertainty using set-inclusion models
- Enable secure state estimators with run-time learning of attack models/strategies
- Develop safe-by-design control algorithms with attack-resilient output feedback designs with learning from run-time data



Scientific Impact:

- Theory and algorithms directly applicable/ generalizable to a broad class of CPS, e.g., power systems, medical devices, that must operate under various sources of uncertainties

Broader Impact:

- Improving security and safety can save lives and ensure integrity of critical infrastructures
- Involve undergraduate and graduate students, especially first-generation students, and engage with industry partners

Award ID#: 1943545