Recent cyber-physical attacks have invoked an ominous realization about the vulnerability of critical infrastructure, especially our energy delivery systems. Traditional IT security-biased protection approaches are largely impotent against targeted attacks by advanced cyber adversaries. There is an urgent need to reevaluate the safety and security of critical infrastructure industrial control systems using a systems perspective in the face of such threats.

Our goal is to develop software tools for our Cybersafety method to identify cyber-vulnerabilities & mitigation requirements in energy delivery systems.

Cybersafety is a robust method to identify vulnerabilities and mitigation requirements in complex industrial control systems:

- Based on the STAMP framework (System-Theoretic Accident Model and Processes), it considers the complex system to be a collection of interacting control loops.
- In this view, decision-makers enforce certain safety and security constraints to keep the controlled processes within certain defined limits, by taking relevant control actions.
- Thus, the security problem is transformed into a dynamic control problem where the violation of safety and security constraints results in system-level losses.
- This enables a deeper understanding of structural and process model flaws resulting in cyber-vulnerabilities.
- The goal is to develop an effective control structure that keeps the processes within safe limits.

This control can be implemented via:
- technical means (safety interlocks, fail safe design etc.)
- through changes in process and procedures
- through social controls such as regulatory, cultural, insurance incentives etc.

There is an urgent need to reevaluate the safety and security of critical infrastructure industrial control systems using a systems perspective in the face of such threats.