PreventOTPhysDamage: Anticipating and Preventing Catastrophic OT Physical Damage Through System Thinking Analysis

Shaharyar Khan, Stuart Madnick

MOTIVATION

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.*

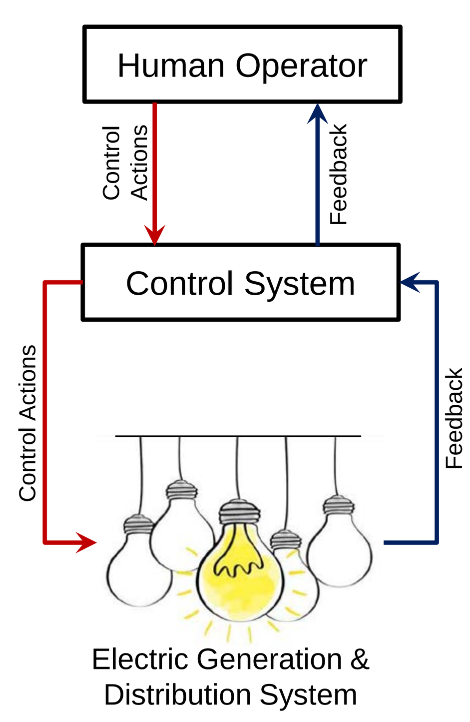
RESEARCH VISION

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

WHAT IS CYBERSAFETY?

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

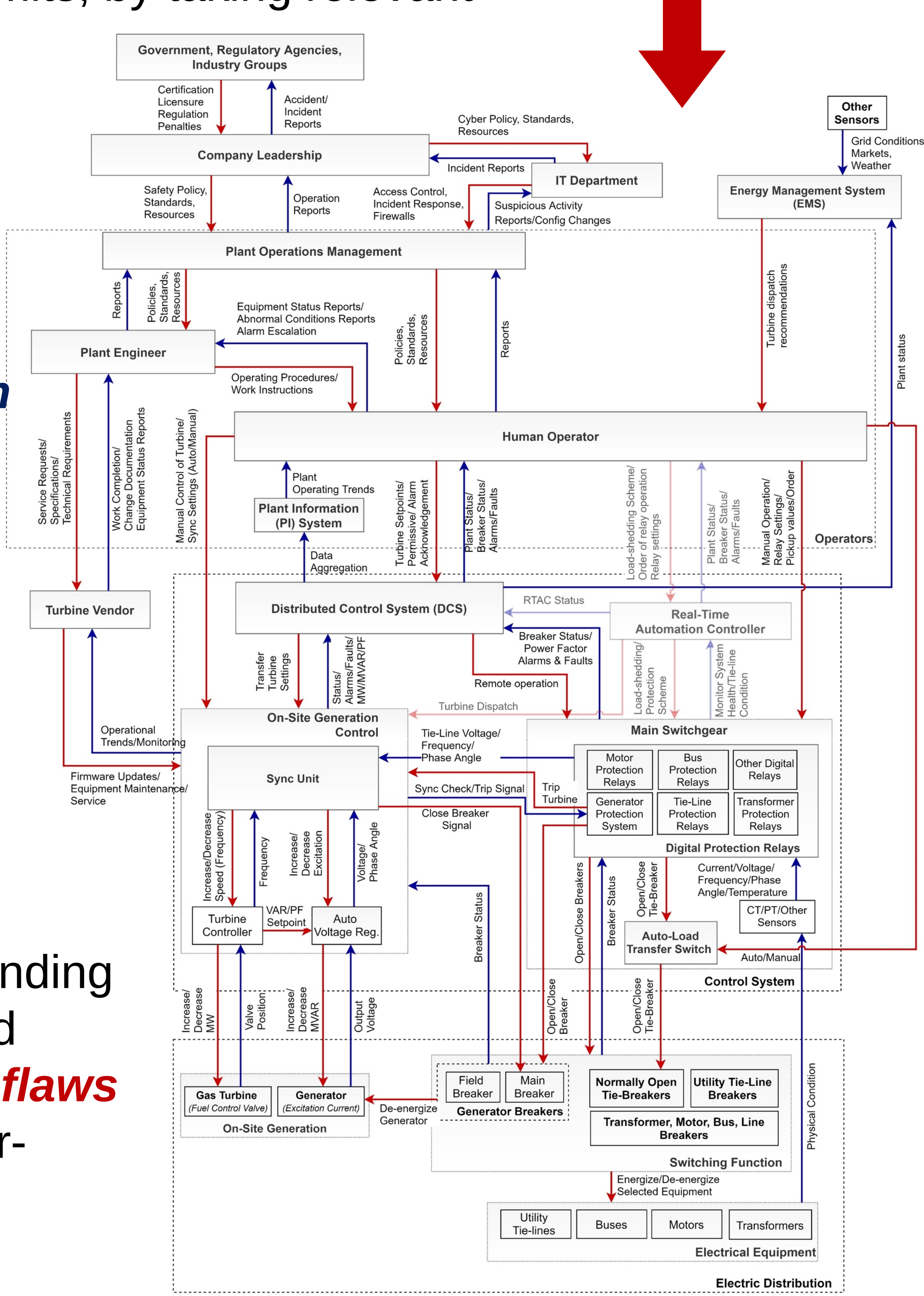
- Based on the ***STAMP*** framework (System-Theoretic Accident Model and Processes), it considers the complex system to be a collection of ***interacting control loops***



- 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.

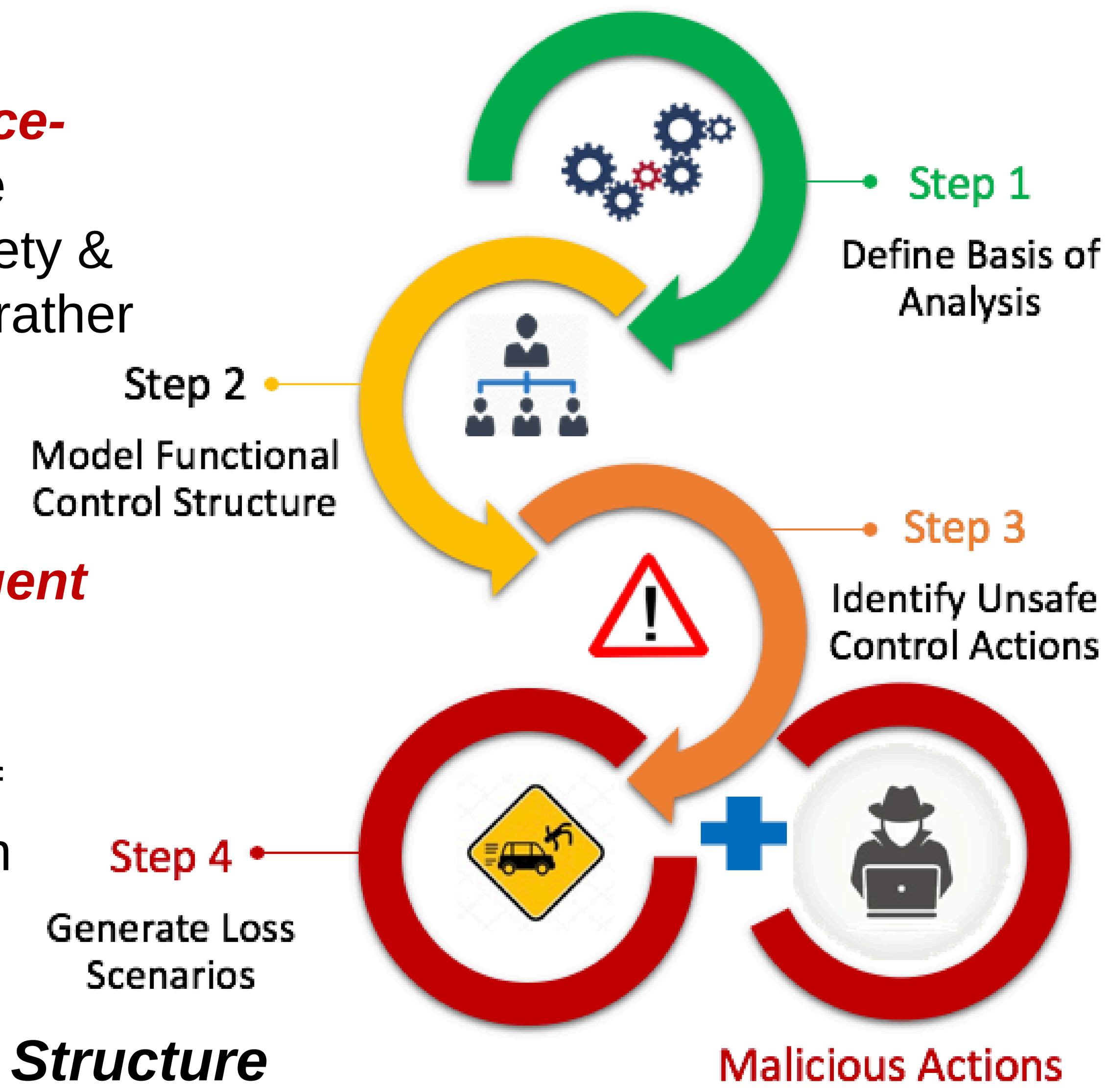


- **The goal is to develop an effective control structure that keeps the processes within safe limits.**

  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.

KEY PRINCIPLES OF CYBERSAFETY

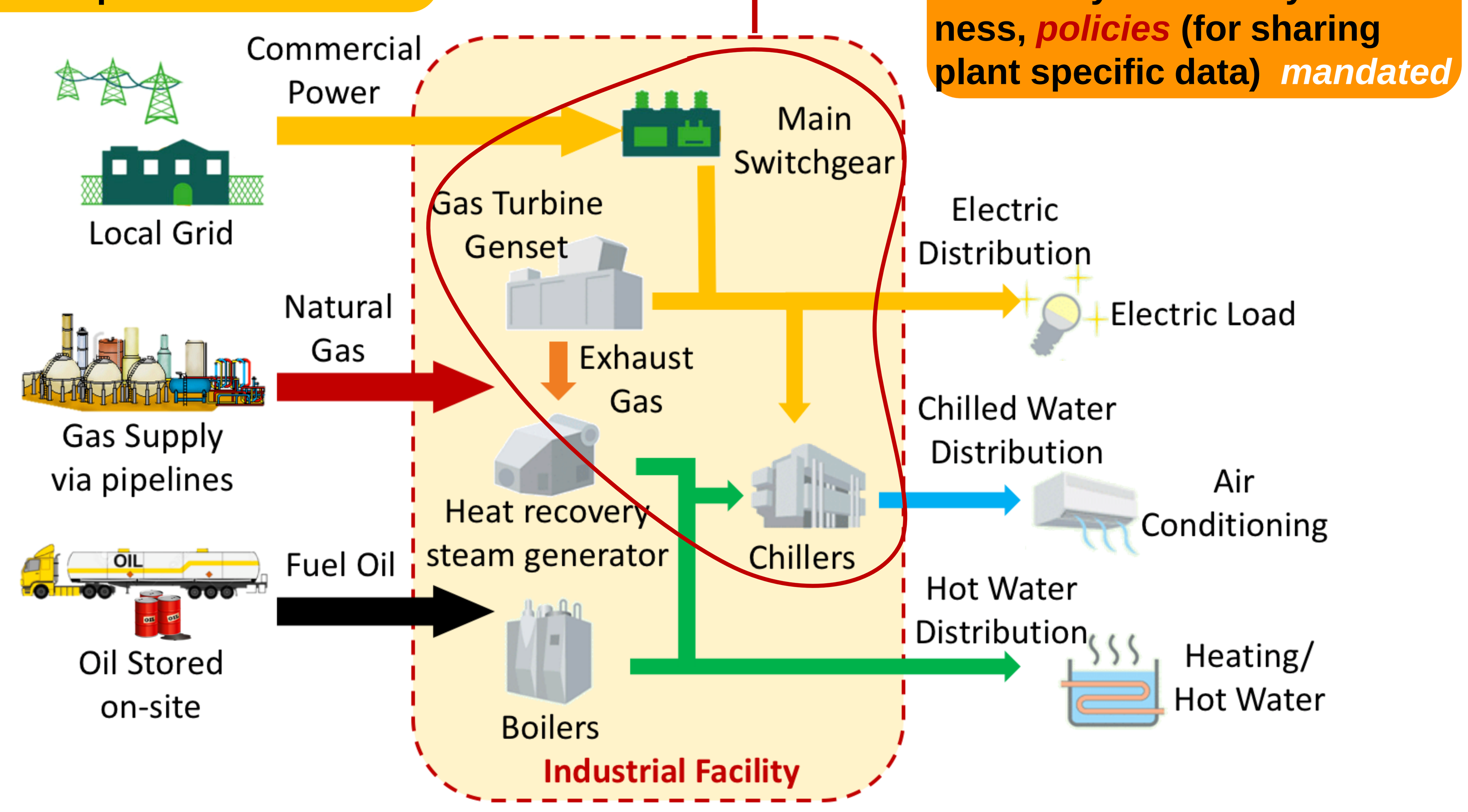
- ***Top-down***
  - This is a ***consequence-driven*** method where ***outcomes*** derive safety & security ***constraints*** rather than external threats
- ***Emergence***
  - ***Security*** is an ***emergent*** property of a system
  - Unanticipated results ***emerge*** as a result of ***interactions*** between components



- ***Hierarchical Control Structure***
  - Models the system as processes ***controlled*** by controllers which are in turn controlled by ***higher-level*** controllers, etc.
  - Enables identification of missing feedbacks and ***key leverage points*** within the broader ***socio-organizational*** system

USE-CASE – 20MW INDUSTRIAL FACILITY

Technical	Procedural	Policy
No *overflux* protection in the electric distribution system ***Turbine Overspeed* protection implemented in software only** **The type of VFDs used allow *remote* connection and *reverse* operation**	**Lack of *out-of-band* control/feedback loops** **Operator does not have *quality controlled copy* of procedure in control room** **Transfer of real-time data *off-site* via internet**	**Regulations do not mandate overflux relay protection for plants < *100MW*** **No policy to screen purchased equipment for cyber vulnerabilities – *hidden functionality*** **Lack of cybersecurity awareness, *policies* (for sharing plant specific data) *mandated***



Results of applying the *Cybersafety* Method

Uncovered cyber-vulnerabilities in energy delivery systems (especially in ***operational procedures*** and ***management policies***) not previously realized

IMPACT ON YOUR CYBER-PHYSICAL SYSTEM

- Using the top-down ***systems-thinking*** approach, you can deal with the complexity of your cyber-physical system in a strategic, structured manner that focuses on the most critical cyber-vulnerabilities and mitigation requirements in your organization.
- By analyzing the ***functional control structure***, new insights naturally emerge about the system which you can then leverage to develop a deeper understanding of the system and uncover ways to make it more resilient.

COLLABORATION OPPORTUNITIES

Cooperation, support and guidance from industry in the following areas would benefit this research activity:

- **Review and validation of our functional control models and assumptions against real-world use-cases**
- **Discussions about and testing of our software tools to facilitate the use of the *Cybersafety* Method by OT personnel**

- Contact: shkhan@mit.edu, smadnick@mit.edu

- Activity Webpage: https://cred-c.org/researchactivity/PreventOTPD

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY