An adversarial model for attack vector vulnerability analysis on power and gas delivery operations.

Ignacio Losada Carreno, Anna Scaglione, Anatoly Zlotnik, Kaarthik Sundar, Deepjyoti Deka

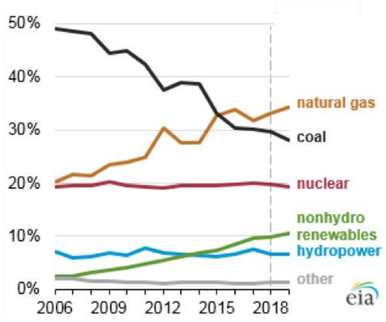
GRID RESILIENCE DEPENDS ON GAS PIPELINES

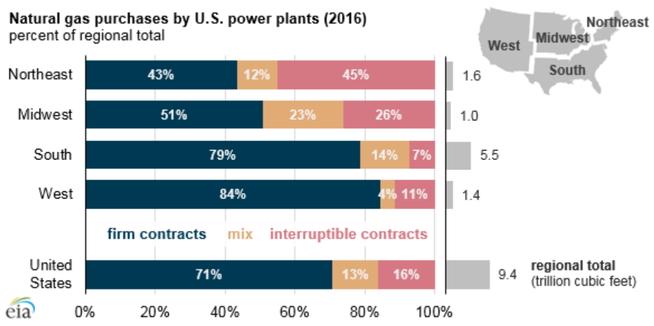
OT

- Reliance on natural gas for electricity generation has increased in US
- Alters traditional status-quo
- No formal coordination for reliability purposes

IT

- Cyber regulation not homogeneous across sectors
- High risk of cyber attack (poor TSA guidelines and implementation of NIST voluntary)
- Concerns raised by DNI and GAO

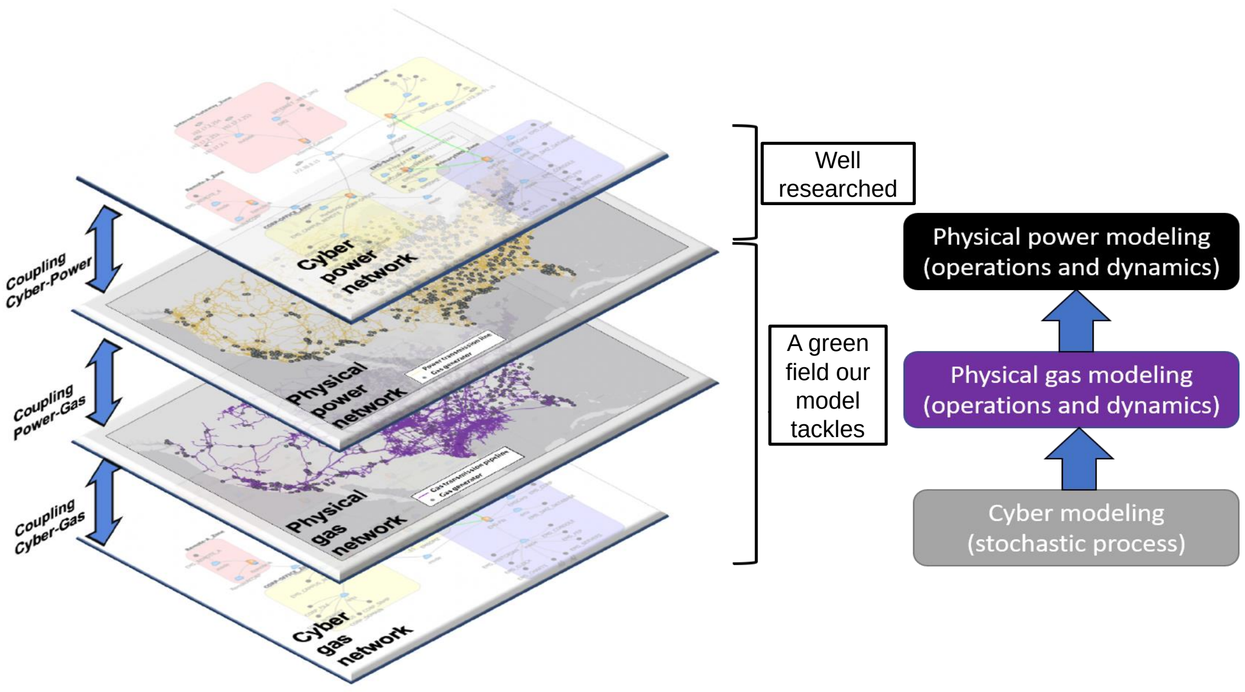




Problem: The inability of power system operators to asses the inherent cyber risks of being coupled to other infrastructures

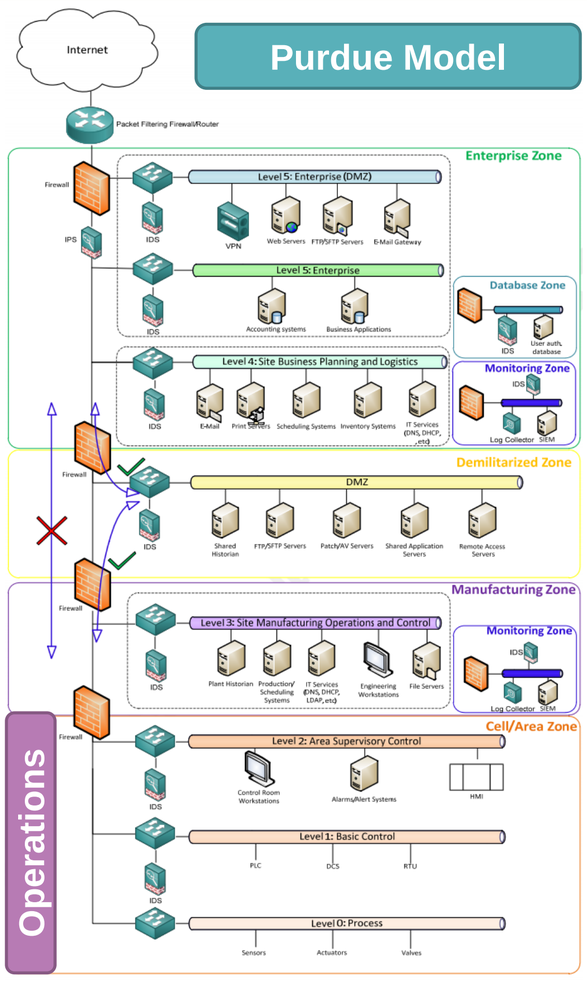
RESEARCH VISION

Objective: To provide a tool that improves the cyber-physical resilience of gas pipelines and the electric power industry

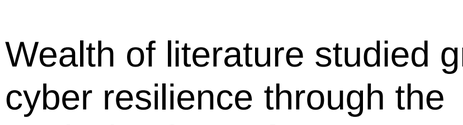


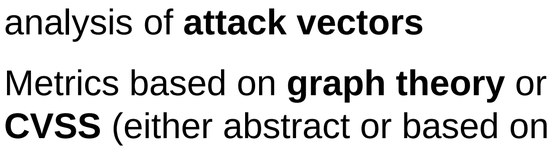
BACKGROUND ON MODELING ATTACKS

- Wealth of literature studied grid cyber resilience through the analysis of **attack vectors**
- Metrics based on **graph theory** or **CVSS** (either abstract or based on expert knowledge)
- No **physical** models
- Attackers could compound **physical weaknesses** hidden to the operator
- Cybersecurity best understood with **physical models**



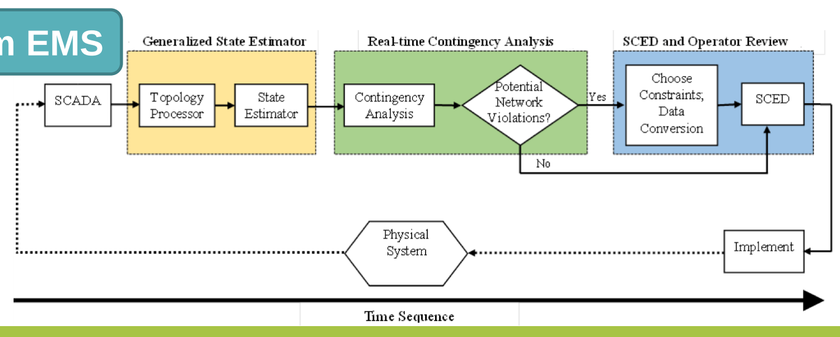
CVSS scoring system



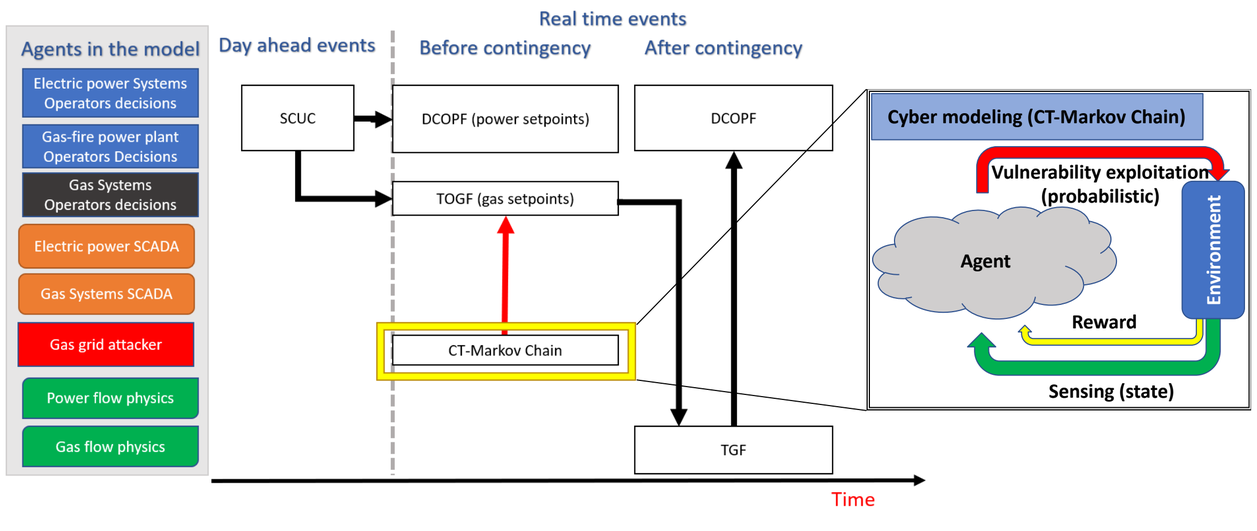


Product: An EMS tool that models the true risk of a cyber attack to the operational state of the system

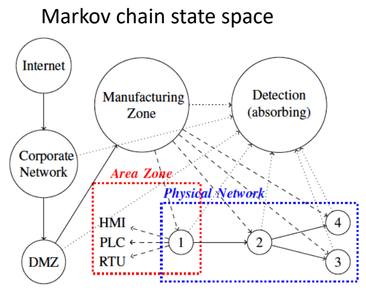
Power system EMS



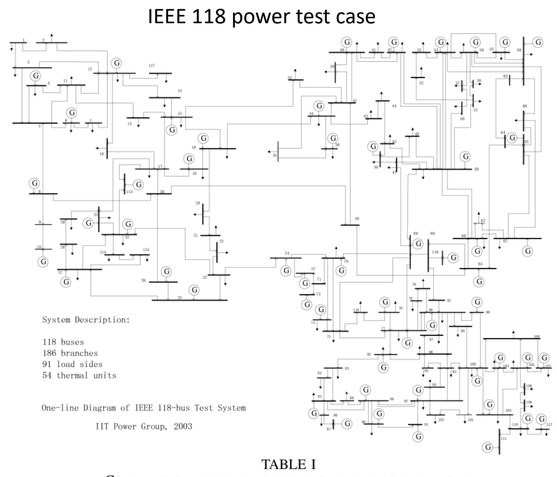
CYBER-PHYSICAL MODELING



Markov chain state space



IEEE 118 power test case



25-node natural gas test case

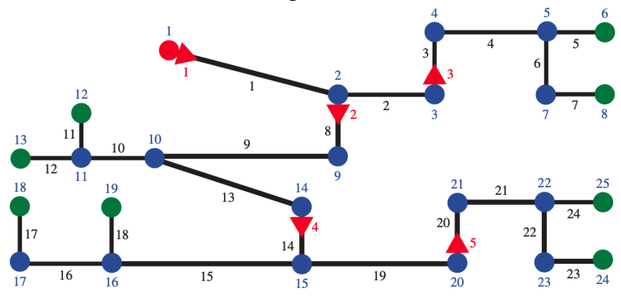
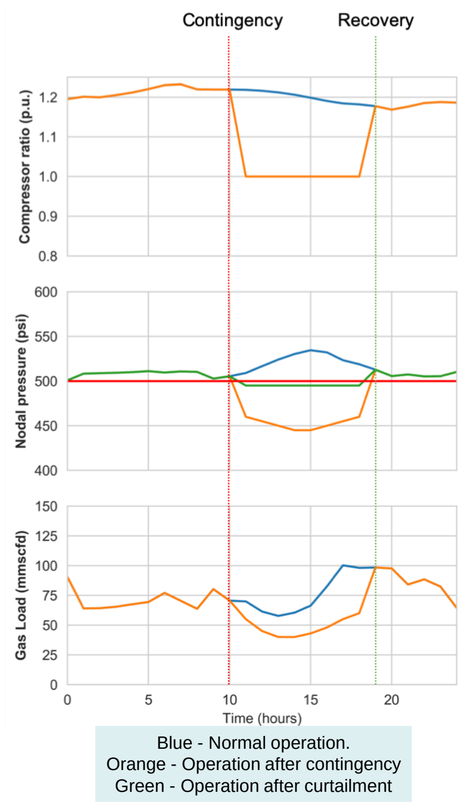
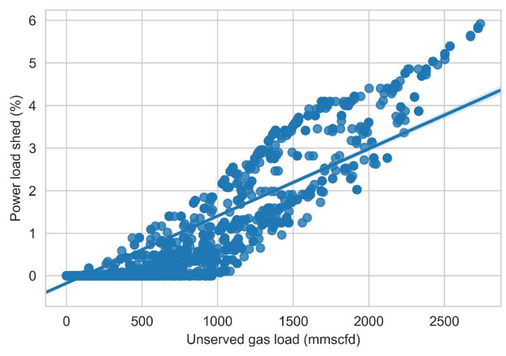


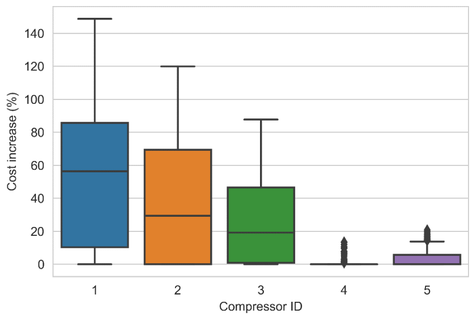
TABLE I
COUPLING OF PIPELINE NODES TO GAS-FIRED GENERATORS.

Gas Node	Generator ID	Total Capacity (MW)
6	4,20,21	255
8	5,22,23	255
12	11,24,25	255
13	12,26,27	255
18	13,28,29	255
19	15,31	231
24	36,37,38	228
25	39,40	152

IMPACT ON GRID SECURITY







Blue - Normal operation.
Orange - Operation after contingency
Green - Operation after curtailment

Impacts on your system

Protected system through an algorithm implemented in the EMS. Your system would be able to:

- Assess the operational impacts of a potential/imminent attack
- Account for security breaches in interconnected infrastructures

Business benefit

- Reduced power load curtailment to customers
- Significant savings in operational cost
- Increased cyber resilience
- Better understanding of exposure based on ICS/SCADA configuration

Market: - OT software companies (DNV GL, ABB, Emerson)
- IT software (NPview, Applied Risk, Dragos)
- Operators (ISOs, Kinder Morgan)
- Federal agencies (FERC, TSA, DHS, DoD)

COLLABORATION OPPORTUNITIES

This research would benefit from collaboration with industry partners:

- Insights on cyber modeling, attacker representation
- Industry level implementation for ISOs to commercialize our solution
- Contact: Anna.Scaglione@asu.edu, ilosadac@asu.edu
- Activity webpage: https://cred-c.org/researchactivity/security-gaps-due-coupling-energy-delivery-sub-systems

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