CLOSING THE LOOP: DEVELOPING AND VALIDATING A NEXT-GENERATION CYBER-PHYSICAL ENERGY MANAGEMENT SYSTEM FROM SITUATIONAL AWARENESS TO RISK MITIGATION

Dr. Kate Davis
TEES Young Faculty Fellow
Assistant Professor
katedavis@tamu.edu

PSERC Webinar - Aug. 31, 2022
HOWDY!

My COVID experience: Margaret
March 19, 2020

Resilient or Remedial? (*)

What is Resilience? (*)

“The capacity to recover quickly from difficulties; toughness”
– Oxford English Dictionary

“An ability to recover from or adjust easily to misfortune or change”
– Merriam Webster Dictionary


My recent first hand experience with resilience.
It’s great to be back to normal!
OVERVIEW

• The Cyber-Physical Foundation of Grid Resilience

• Next-Generation Cyber-Physical Energy Management Systems
  – Requirements and Challenges
  – Cyber-Side and Physical-Side
  – Developments

• Opportunities and Discussion

This work is supported by the US Department of Energy under award number DE-OE0000895 and the National Science Foundation under award numbers 1808064 and 1916142.
GRID RESILIENCE IS A CYBER-PHYSICAL PROBLEM!

The system is complicated.

- Considering cyber systems and trustworthiness with physical adds a new layer of complexity
- Cyber-physical interconnections not well known

CRITICAL INFRASTRUCTURE SECTORS

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Financial Services Sector
The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector

Nuclear Reactors, Materials, and Waste

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings.

Defense Industrial Base Sector
The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, production, and support of military systems.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

https://www.dhs.gov/cisa/critical-infrastructure-sectors
Cyber-Physical Systems Perspective

From the National Science Foundation (NSF): “Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components.”

Why it’s important: A better understanding of power systems as cyber-physical systems – informs us how to model, analyze, protect, and defend.
THREAT CATEGORIES

Natural

Accidental

DATA ENTRY

Intentional

EX. HUMANS ON A KEYBOARD

WHICH CATEGORIES ARE CYBER-RELEVANT?
INCREASING NEED FOR DEFENSE

DESIGN REQUIREMENTS & CHALLENGES

• Solutions need to be
  – Scalable
  – Automatic
  – Work for real world systems
  – Promote openness of the algorithms to understand capabilities and limitations

• Resilient Energy Systems Lab (RESLab) Testbed
  – Proving ground for cyber-physical control systems of the future

Texas A&M Electric Grid Control Room
Our Grid Cyber-Physical Security Research

- Deep learning based detection of stealth false data injection attacks
- Harmonized automatic relay mitigations of events
- Validation for models of cyberattacks on the power grid
- CYPRES cyber-physical energy management system
  1. Redesign energy management systems to be intrinsically cyber-physical with analyses that enable the system to prevent, detect, and respond to events through fusion of cyber and physical data
  2. Facilitate online and potentially automated control actions that couple cyber and physical control spaces
  3. Facilitate how to integrate with utility environments

Find more about these and our other projects here: https://katedavis.engr.tamu.edu/
"CLOSING THE LOOP" WITH A UNIFIED MODEL

Cyber-Physical Power System

Data verification layer

Control Center

Power System Topology

Cyber-Physical State Estimation


Cyber-Physical Resilient Energy Systems (CYPRES) https://cypres.engr.tamu.edu/
PART 1: UNDERSTAND YOUR SYSTEM

• To defend a cyber-physical system, you need a map
• Create and leverage new modeling techniques and tools that provide system visibility
• Take a data pipeline integrity approach, prioritized by operational resilience
• Cross organizational silos (data, models, tools, people)

PART 2: FUSE MODELS & DATA TO ASSESS RISK TO RESILIENCE

Cyber-Physical Situational Awareness (CyPSA) Framework

Results identify “high-risk” cyber-attack induced outages

PART 3: RECOMMEND COORDINATED CYBER-PHYSICAL RESPONSE

• State space, actions, reward model, and state transition model are all cyber-physical
• Reward based on cyber recovery of the compromise, considering time, cost, and impact and physical actions to reduce overloads
• Considering Q Learning and Deep Q Networks for dealing with unknown transition probabilities

Cyber-Physical Resilient Energy Systems (CYPRES) [https://cypres.engr.tamu.edu/](https://cypres.engr.tamu.edu/)
CYPRES IN RESLab Testbed

PowerWorld Dynamic Studio for real-time power system simulation acts as a collection of DNP3 outstations.

CYPRES DNP3 Master

CYPRES EMS Application

Balancing Authority

SEL-RTAC DNP3 Master

Utility Control Center

Hardware Devices

Substations

DNP3 Data Flow

Cyber Alert Data

Industry Roles

* synthetic model shown


“CLOSING THE LOOP” WITH A UNIFIED MODEL

1. Model
   – Represent, manage, and visualize the cyber physical model

2. Monitor and Verify
   – Fuse streaming inputs to the model
   – Estimate cyber-physical state

3. Analysis
   – Early attack detection
   – Cyber-physical risk analysis
   – Cyber-physical detection and situational awareness use cases

4. Verify and Control
   – Recommend cyber-physical actions
   – Mitigations, countermeasures

Cyber-Physical Resilient Energy Systems (CYPRES) [https://cypres.engr.tamu.edu/](https://cypres.engr.tamu.edu/)
THE OLD WAY VS. THE NEW WAY

WHAT I TELL MY STUDENTS!
CYPRES EMS RESEARCH & DEVELOPMENT

CYPRES EMS Application

- Cyber-Physical Resilient Energy Systems (CYPRES) is a centralized cyber-physical energy management application under development

- The objective is a prototype next-generation energy management system for cyber and physical

Cyber-Physical Resilient Energy Systems (CYPRES) [https://cypres.engr.tamu.edu/](https://cypres.engr.tamu.edu/)

* synthetic model shown
CYPRES MODELING AND WORKFLOW

Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/
RISK ASSESSMENT: NERC & THE DRIVERS

• Ensure the computer system networks vital to the operation of the Bulk Electric System (BES) have a sufficient level of protection
• Protections should be related to their importance to a functioning society
• Addressed by NERC CIP, also TPL & PRC

(TPL) Transmission Planning
(PR) Protection and Control
(CIP) Critical Infrastructure Protection
RISK ASSESSMENT

Risk = Likelihood x Impact
Likelihood = Threat x Vulnerability
Threat = Capability x Intent

Assessing Assets: What’s Really Out There?

Risk = Likelihood x Impact
Likelihood = Threat x Vulnerability
Threat = Capability x Intent

Assessing Assets: What’s Really Out There?
A POWER SYSTEM AS A CYBER-PHYSICAL SYSTEM

Synthetic 2000-bus test case


Cyber-Physical Classes & Data Flows

EXPANDING CPS RISK FRAMEWORK

Cyber-Physical Situational Awareness (CyPSA) and its model comparisons

Results identify “high-risk” cyber-attack induced outages

EXPANDING CPS RISK FRAMEWORK

• New scalable approach for finding multiple-element critical contingencies
• Verified by brute force search to find exact critical lines for the N-1 and N-2 contingency analysis
• Execution time increases linearly by x, which makes it tractable for N-x contingency analysis in large systems
• We’ve shown its usefulness for cyber-physical risk considering the integrated CPS as well


Studying how failures propagate in time and space, in cyber and physical layers, is crucial.

Even slight errors in DC power flows can turn out to be important at cascade stages.

Best paper award at SGRE
FAILURE PROPAGATION ANALYSIS

Cyber-Physical Resilient Energy Systems (CYPRES)

https://cypres.engr.tamu.edu/
The intruder can
1. Sniff traffic
2. Modify measurement
3. Modify commands
4. Cause network congestion

Contact us for a live demo (virtual) in our testbed.
INFERENCE USING ONLINE DATA

• Objective is to merge cyber & physical data to detect intrusions and reduce false positives, e.g., using
  – Real-time and offline features from cyber protocol layers such as Ethernet, IP and TCP
  – Features from DNP3 protocol layer that carries physical side control commands and measurements

• The inferencing goal is to estimate **cyber-physical state**, e.g., what is compromised and actual adversary paths toward a target, and use that to enhance system operator’s knowledge
  – Building upon offline CPS risk
  – The idea is making sense of what we would expect to see vs. what we actually do see

DATA FUSION GAPS & MOTIVATION

• Few valuable data sources for studying the impact of cyber intrusions in energy sector
  – Hard to get data sources that are truly cyber-physical
  – Need datasets that are combination of BOTH
• Lack of CPS testbed capability that provides this platform for multi-source data aggregation
  – Our RESLab testbed fills this need
• Challenges with inter-domain fusion: time, location, domain knowledge
  – Cyber-side features can be huge! Need to focus on most important
  – Fusion of data from both sides is needed to make inferences to protect the grid

DATA SOURCES

PacketBeat: captures flow-based traffic and store in the Elasticsearch database

Use of Pyshark

Snort: alerts and logs from IDS

Wireshark: Raw Packet capture at Outstation

Wireshark: Raw Packet capture at Substation Router

DNP3 Master A python client program using OpenDNP3

Utility Control Center

**Data Fusion Engine & Inference**

Correlating cyber alerts with physical sensors makes detection more efficient.

- **Collection**
  - Raw pcaps from 3 nodes
  - Extraction of DNP3 features
  - Pyshark to collect RTT and retransmission
  - Elasticsearch to get packetbeat features
  - Get Snort unified2 formatted alerts

- **Merge**
  - Fusion of cyber, physical and security features
  - Time based merge
  - Location based merge

- **Processing**
  - Imputation of missing values
  - Encoding of categorical features
  - Visualization of merged features
  - Feature reduction with PCA

- **Detection**
  - Supervised Learning:
    - SVM, Naïve Bayes, RF, DT and MLP
  - Semi-Supervised Learning:
    - Co-Training

- **Fusion by Location**
  - Dempster Shafer Rules of Combination
  - Disjunctive
  - Conjunctive

---


Dataset: [https://ieeeportal.org/documents/cyber-physical-dataset-mitm-attacks-power-systems](https://ieeeportal.org/documents/cyber-physical-dataset-mitm-attacks-power-systems)
ESTIMATING CYBER PHYSICAL STATE - DATA FUSION

LAB (TRY ON YOUR OWN!)

• Tutorials page on the CYPRES website to download the hands-on training materials:
  • https://cypres.engr.tamu.edu/tutorials/
  • cypres2021
• In the GridSecCon2021 folder:
  • Tutorial2_Cyber_Physical_Data_Fusion
• How to cite:
  
DEALING WITH ADVERSARY DYNAMICS

• An adversary’s behavior is uncertain
• Techniques like Bayesian Networks (BNs) are beneficial for modeling attack graphs
• Perform causal reasoning between each step in of adversary’s trajectory toward compromise of final target
• Determine structure from raw data, e.g., network logs or Intrusion Detection Systems (IDS)
• Bridge data fusion back to the models

CYPRES MODELING AND WORKFLOW

Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/
INTERACTIVE GRID DEFENSE

- Web-based
- Multi-player
- Real-time
- Interactive dynamic simulation

Cyber Attack Risk Identification, Analysis, and Response

Visualization & Response

W4IPS by Zeyu Mao

RECONFIGURATION-BASED DEFENSE

• Detection Mechanism:
  1. SNORT: Use of Intrusion Detection Systems
  2. Use of Tcp Dump
  3. Detection based on Firewall rule hits
  4. Use of Network Monitoring tools like Zabbix, Packetbeat or other SIEMS such as Splunk

• Response:
  1. Blocking intruder Node using firewalls
  2. Rerouting traffic from its intended path under compromise

See demo on our website or contact us for live demo with updated threat use cases and validation approach
See demo on our website or contact us for live demo with updated threat use cases and validation approach.
RESILIENCE-ORIENTED OPTIMAL OPERATION & DESIGN AS A SOLUTION

ACTIVSg500 System

\(R_{ECO}\) OPF has better cost-effectiveness compared to SCOPF. \(R_{ECO}\) reduced 10% violations, 100% unsolved contingencies, and 31% violated contingencies.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Power Flow Model</th>
<th>Cost/($/hr)</th>
<th>Total Violations</th>
<th>Total Unsolved</th>
<th>Violated Contingencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>(R_{ECO}) OPF</td>
<td>DC</td>
<td>89,447.79</td>
<td>207</td>
<td>0</td>
<td>34</td>
</tr>
<tr>
<td>(R_{ECO}) OPF</td>
<td>QCLS</td>
<td>77,159.61</td>
<td>243</td>
<td>0</td>
<td>37</td>
</tr>
<tr>
<td>(R_{ECO}) OPF</td>
<td>AC</td>
<td>77,482.57</td>
<td>219</td>
<td>0</td>
<td>39</td>
</tr>
<tr>
<td>OPF</td>
<td>AC</td>
<td>66,287.91</td>
<td>252</td>
<td>10</td>
<td>55</td>
</tr>
<tr>
<td>SCOPF N-1</td>
<td>DC</td>
<td>80,025.06</td>
<td>238</td>
<td>8</td>
<td>48</td>
</tr>
<tr>
<td>SCOPF N-x</td>
<td>DC</td>
<td>94,438.72</td>
<td>221</td>
<td>8</td>
<td>49</td>
</tr>
</tbody>
</table>
RESILIENCE-ORIENTED OPTIMAL OPERATION & DESIGN AS A SOLUTION

Objective

Max($R_{ECO} = g([T])$)

$[T] = f(P_{ij}, P_{geni}, P_{loadi}, P_{lossi}, a_{ij})$

Formulation

$R_{ECO} = \frac{ASC}{DC}ln\left(\frac{ASC}{DC}\right)$

$ASC = -TSTp \sum_{i=1}^{N+3N+3} T_{ij} \sum_{j=1}^{N+3N+3} \log_2\left(\frac{T_{ij}}{T_{ii}}\right)$

$DC = -TSTp \sum_{i=1}^{N+3N+3} T_{ij} \sum_{j=1}^{N+3N+3} \log_2\left(\frac{T_{ij}}{T_{ii}}\right)$

$TSTp = \sum_{i=1}^{N+3N+3} T_{ij}$

$P_{ij} = V_i^2[-G_{ij}] + V_j V_i[G_i \cos(\theta_{ij}) + B_i \sin(\theta_{ij})](\forall (i,j) \in B)$

$Q_{ij} = V_i^2[B_j] + V_j V_i[G_j \sin(\theta_{ij}) - B_j \cos(\theta_{ij})](\forall (i,j) \in B)$

$P_i = P_{loadi} - P_{geni} = \sum_{j} P_{ij}(\forall j \in M')$

$Q_i = Q_{loadi} - Q_{geni} = \sum_{j} Q_{ij}(\forall j \in M')$

$P_{lossi} = \frac{1}{Z} \sum_{j} (P_{ij}^2 + Q_{ij}^2)/(B_i V_i^2)(\forall j \in M')$

$M'$: Set of buses; $B$: Set of branches; $N'B$: Set of candidate branches; $G$: Set of generators

Power System Operational Limits

$\psi_i \leq V_i \leq \psi_i^u (\forall i \in M)$

$\theta_i \leq \theta_i \leq \theta_i^u (\forall i \in M')$

$s_{ij}^l \leq s_{ij} \leq s_{ij}^u (\forall (i,j) \in B)$

$s_{geni}^l \leq s_{geni} \leq s_{geni}^u (\forall i \in G)$

CPMA Team at Hao Huang’s PhD defense on Aug. 22

CYPRES MODELING & WORKFLOW

Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/
CYPRES MODELING & WORKFLOW

Cyber-Physical Resilient Energy Systems (CYPRES)

https://cypres.engr.tamu.edu/
CYPRES MODELING & WORKFLOW

Cyber-Physical Resilient Energy Systems (CYPRES)

https://cypres.engr.tamu.edu/
Mapping Real System Architectures and Technologies to the Emulated Environment

OpenConduit: NPView to CORE Data Pipeline
Collaboration for Sector Defense

- Targeted end users are asset owners and regional reliability organizations with a focus on transmission and generation
- Security-oriented cyber-physical energy management system application
- Goal is to be easily deployable in utilities as a plugin, achieved by testing as a proof-of-concept in emulated utility in RESLab as a safe proving ground, with sharable test cases and engaging industry throughout project
- Past and upcoming workshops and live/recorded demos to increase engagement with us
CYPRES AND RESLab: LOOKING AHEAD

We gratefully acknowledge the US Department of Energy under award number DE-OE0000895 and the National Science Foundation under award numbers 1808064 and 1916142.