Modeling, Emulation, and Testing for Power Grid Cyber-Physical Security Studies

Dr. Kate Davis
Associate Professor
Electrical and Computer Engineering
Texas A&M University
katedavis@tamu.edu

PSERC Webinar - April 16, 2025

PSERC

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Cyber-Physical Response for Keeping the Lights On:

Scalable Cyber-Physical Optimal Response Engine (SCORE) Project

SCORE Academic/Industrial Team

Texas A&M Engineering Experiment Station

Kate Davis
Ana Goulart

Georgia Institute of Technology

Saman Zonouz

Oregon State University

Rakesh Bobba

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Sibin Mohan

network perception

Robin Berthier

tdi technologies

Pam Johnson
Bill Johnson
Tim Simmons

Texas A&M Engineering TEEX Extension Service Cyber Readiness Center

Lisa Mutchler
Bart Taylor
Dayo Olasosebikan

EPE

Hala Ballouz
Bill Yancy
Hugo Mena
Meisam Ansari

PSC

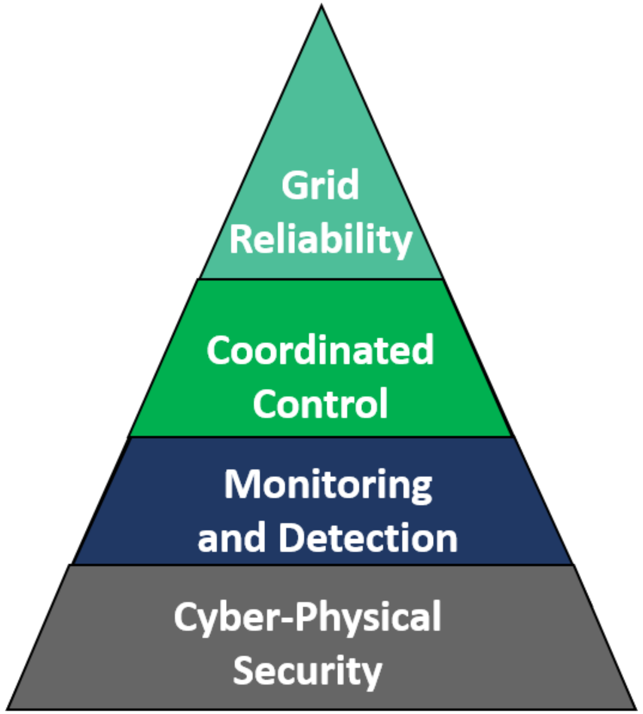
John Camilleri
Rick Hudella
Jeffery Mayger
Mark Prentice

U.S. DEPARTMENT OF ENERGY

Robert Hayes
Prima Asante

Overview

- The Cyber-Physical Foundation of Grid Resilience
- Next-Generation Cyber-Physical Energy Management Systems
  - Requirements and Challenges
  - Cyber-Side and Physical-Side
  - Development and Testbeds
- Opportunities and Discussion



This work is supported by the US Department of Energy under award numbers DE-OE0000895 and DE-CR0000018, the National Science Foundation under award numbers 1808064 and 2220347, and ERDC under W9132T239C007.

The Cyber-Physical Foundation of Grid Resilience

Considering cyber systems and trustworthiness with physical adds a new level of complexity

- What is meant by "resilience"?

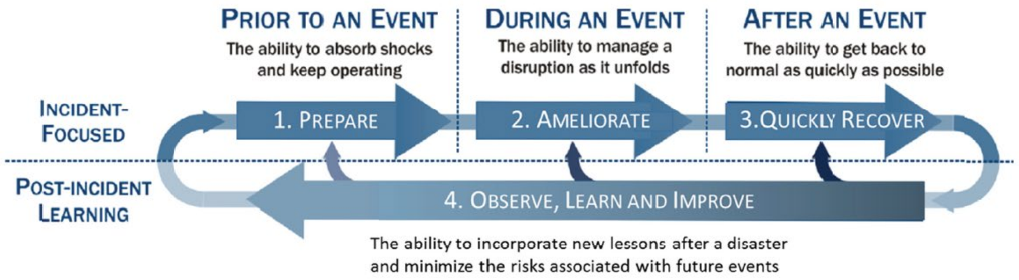
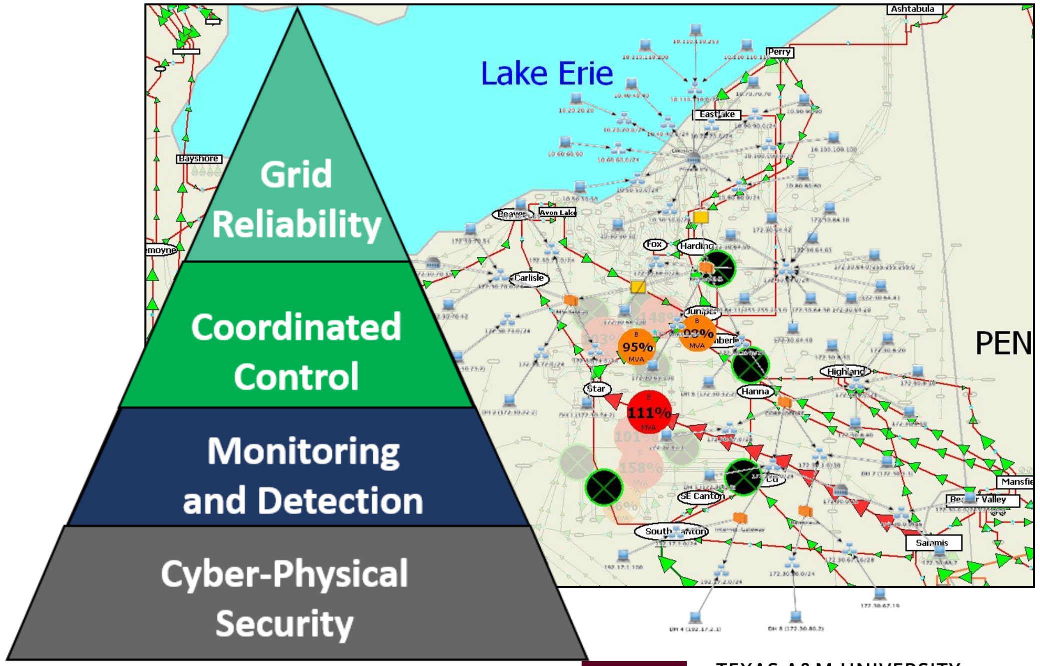


Fig. 1.2 (A), p. 36

- Need to consider resilience across entire event lifecycle



The National Academies "Enhancing the Resilience of the Nation's Electricity System," July 2017.

SCORE: Resilience Enhancement

Restoration

Remedial actions

Cyber attack mitigation

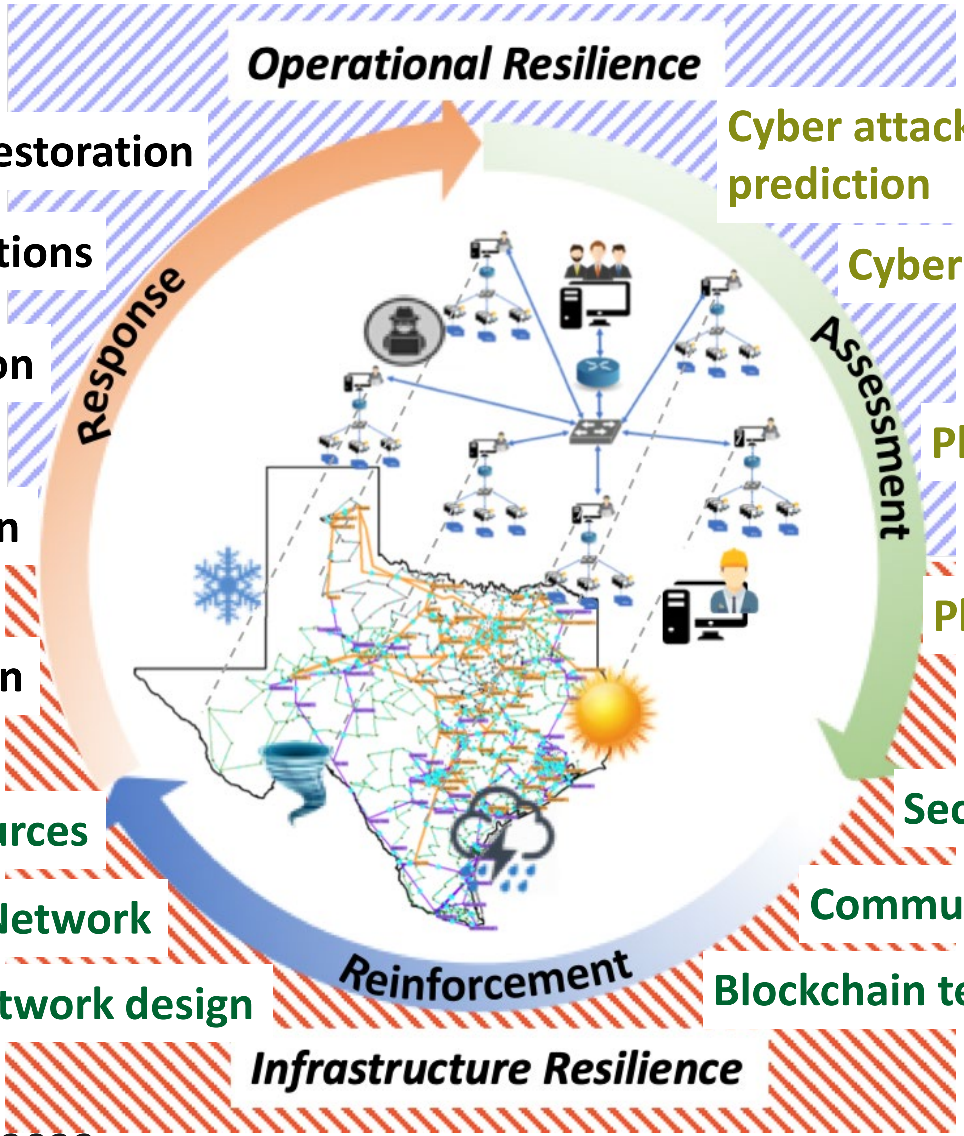
Preventative operation

Ahead-of-Time Preparation

Distributed Energy Resources

Software Defined Network

Transmission network design



Cyber attack prediction

Cyber attack assessment

Physical Hazards prediction

Physical Hazards Assessment

Security Constrained Optimal Power Flow

Communication protocol

Blockchain technology

CPMA Team at Hao Huang's PhD defense in Aug. 22

(*) Hao Huang PhD thesis, 2022

Critical Infrastructure Sectors

PPD-21 identifies 16 critical infrastructure sectors:

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.

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.

Chemical Sector

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

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.

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 co-Sector-Specific Agencies for the Food and Agriculture Sector.

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.

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.

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.

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

Water and Wastewater Systems Sector

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

Information Technology Sector

Nuclear Reactors, Materials, and Waste

https://www.dhs.gov/cisa/critical-infrastructure-sectors

WHAT IS A CYBER-PHYSICAL SYSTEM?

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

TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

THREAT CATEGORIES

Natural

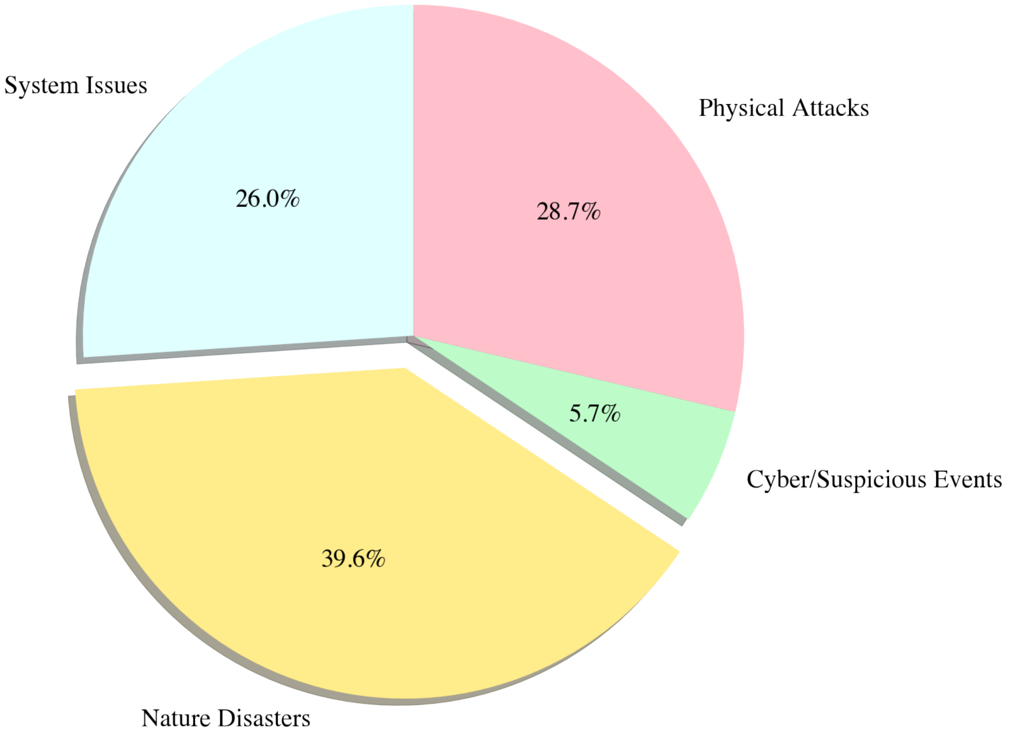
Accidental

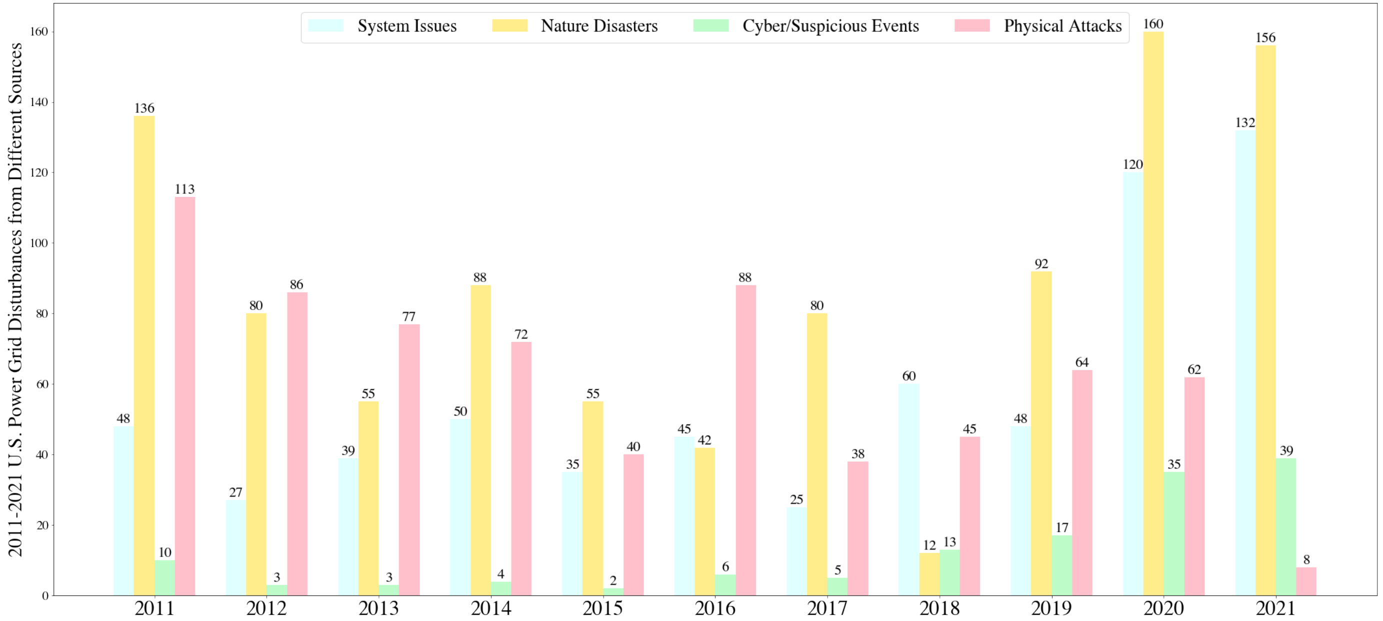
Intentional

WHICH CATEGORIES ARE CYBER-RELEVANT?

EX. HUMANS ON A KEYBOARD

INCREASING NEED FOR DEFENSE





U.S. power disturbances from 2011-2021, visualized by Hao Huang, data from https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

Design Requirements & Challenges

- Solutions need to be
  - Scalable
  - Automatic
  - Work for real world systems
  - Promote openess 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

Texas A&M's DOE CyberForce 2019 Competition team

Texas A&M Researchers showing RESLab to Students


Abhijeet Sahu

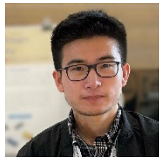
Hao Huang

Zeyu Mao

Amara Umunnakwe

Andy Mael

Leen Al Hamoud

Mohamed Massaoudi

Xiang Huo

Shining Sun

Akram Haque

Samantha Israel

Rhett Gutherie

Texas A&M Cyber-Physical Student Team and Research Staff

- **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; prevent, detect, respond
  2. Facilitate online and potentially automated control actions that couple cyber and physical control spaces
  3. Facilitate how to integrate with utility environments
- **Scalable cyber-physical optimal response engine**
- **Microgrid reliability and resiliency research**

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories

NSF

ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

Find more about these and our other projects here: https://katedavis.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

"Closing the Loop" with a Unified Model

U.S. DEPARTMENT OF ENERGY

Measurements

Cyber-physical data

Model

Cyber-physical model

Analyses

Cyber-physical situational awareness

Cyber-physical state estimation

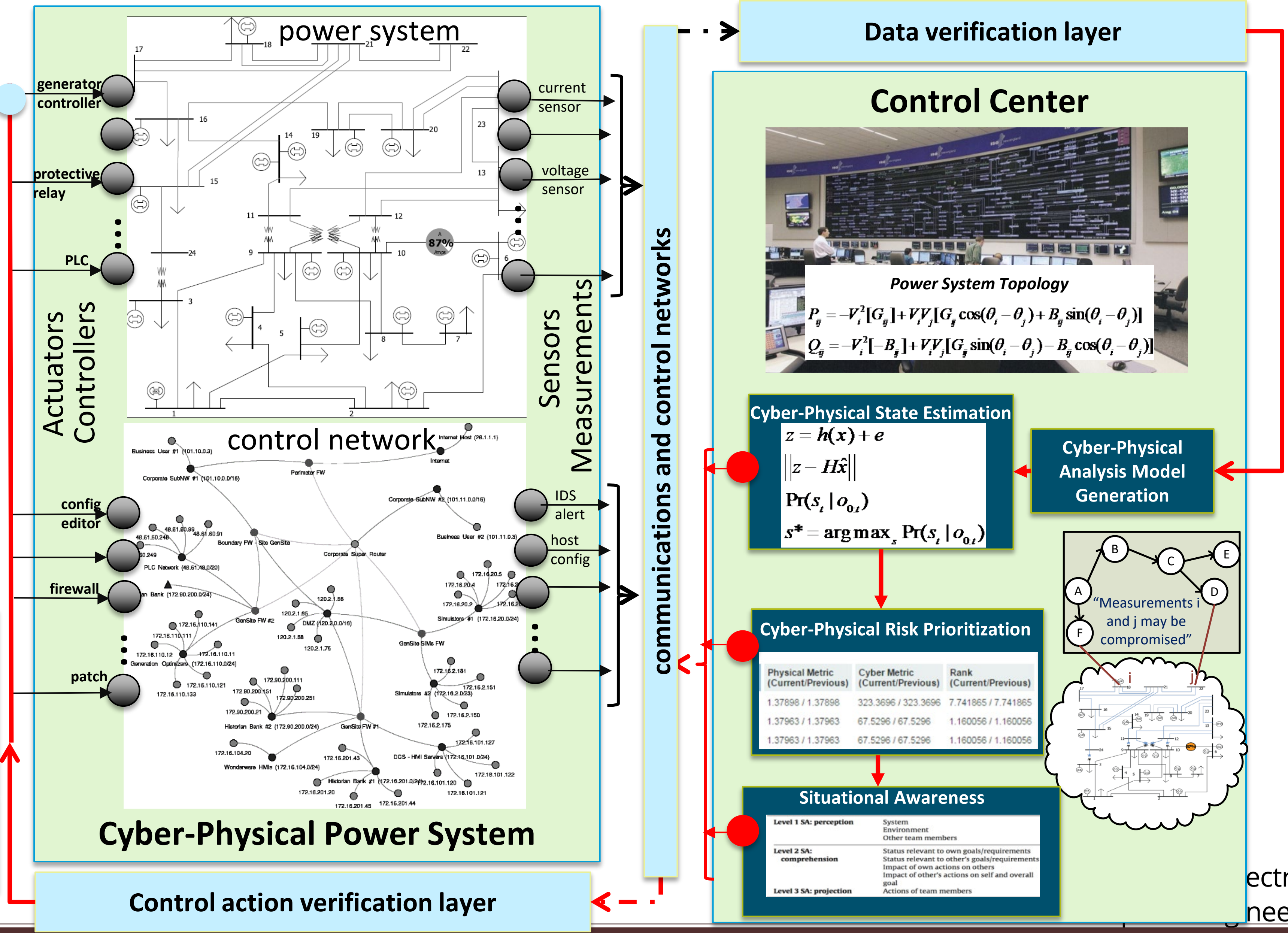
Dependencies among assets

Cyber-physical contingency analysis

Response

Reconfigura-tions

Cyber-physical controls



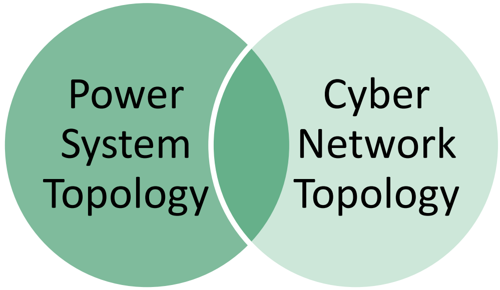
Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management

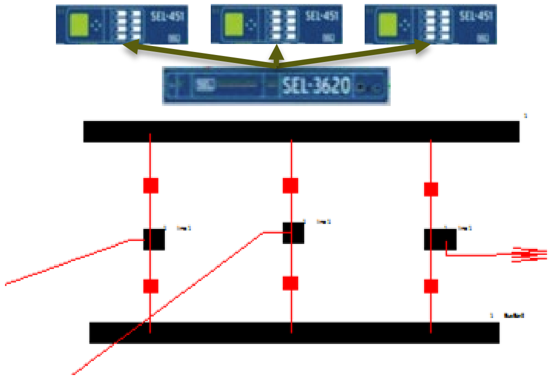
Cyber-Physical Resilient Energy Systems (CYPRES) https://cypres.engr.tamu.edu/

ectrical
neering

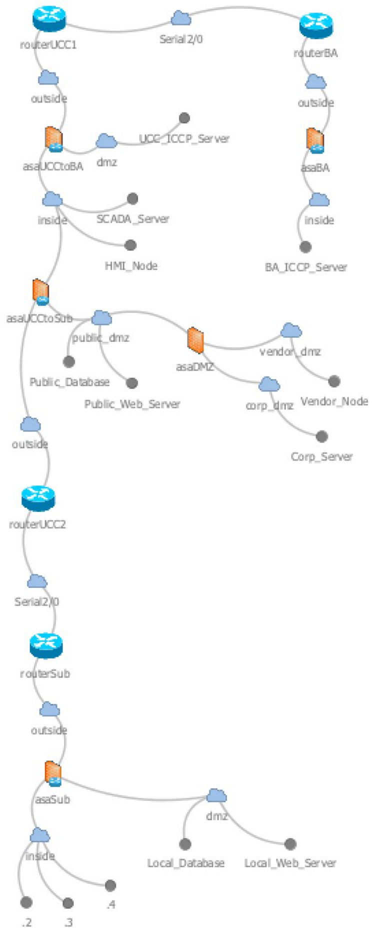
PART 1: UNDERSTAND YOUR SYSTEM

- 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)





Cyber-Physical View: Substation

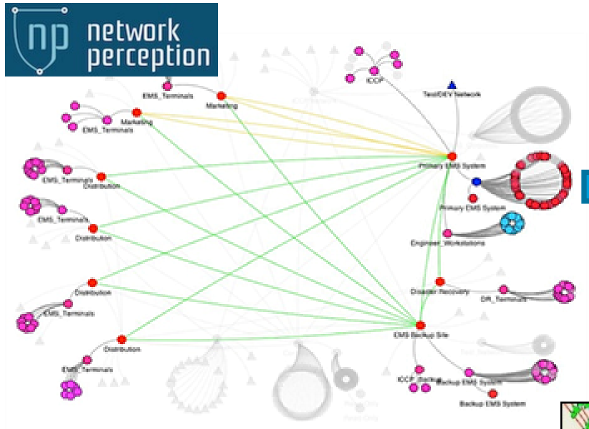


P. Wlazlo, et al, "A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid," *IPTComm* 2019.

N. Gaudet, et al, "Firewall Configuration and Path Analysis for Smart Grid Networks," *IEEE CQR* 2020.

M. R. Narimani, et al, "Generalized Contingency Analysis Based on Graph Theory and Line Outage Distribution Factor," *IEEE Systems Journal*, 2021.

Part 2: Fuse Models & Data to Assess Risk to Resilience

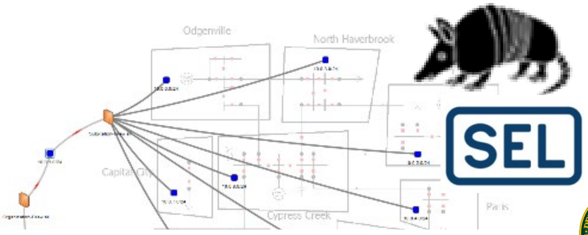


CyPSA

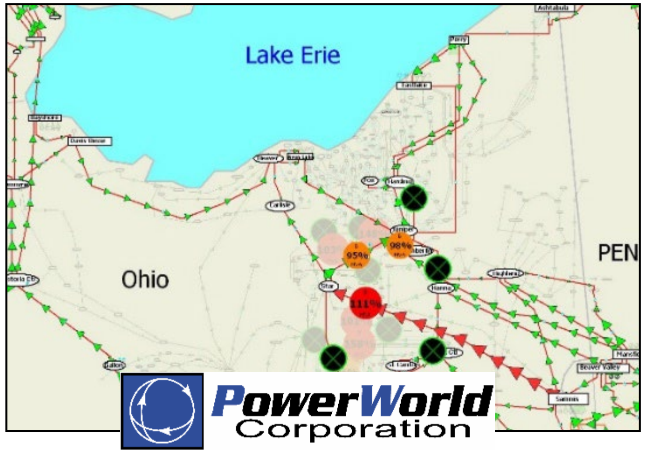
1

2

3



ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776
5	10.31.1.101	10.31.1.101	3.622776



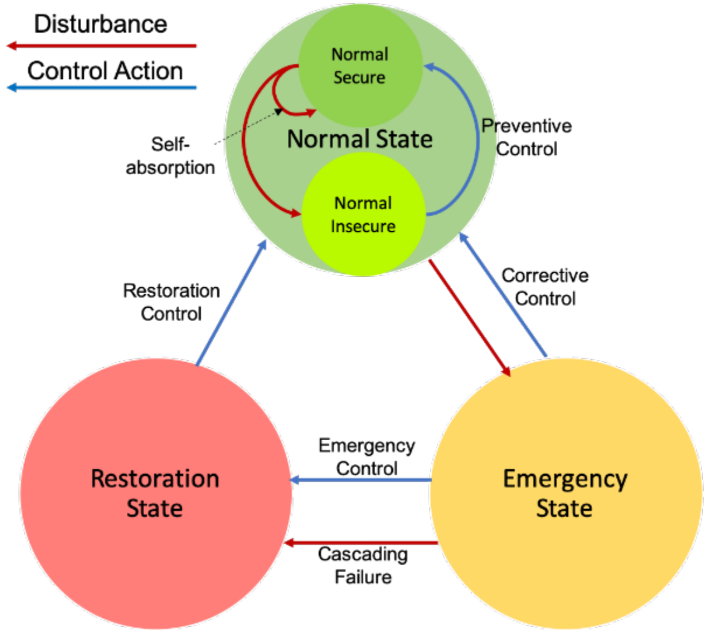
Cyber-Physical Situational Awareness (CyPSA) Framework

Results identify "high-risk" cyber-attack induced outages

K. R. Davis, et. al, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid*, 2015.
K. R. Davis, et. al., "Cyber-Physical Security Assessment for Electric Power Systems," *IEEE-HKN: The Bridge*, 2016.
A. Sahu, et al. "A Framework for Cyber-Physical Model Creation and Evaluation," *ISAP*, 2019.
A. Umunnakwe, et al, "Cyber-physical Component Ranking for Risk Sensitivity Analysis using Betweenness Centrality," *IET Cyber-Physical Systems*, 2021.
S. Sun, et. al., "A Graph Embedding-Based Approach for Automatic Cyber-Physical Power System Risk Assessment to Prevent and Mitigate Threats at Scale," *IET Cyber-Physical Systems: Theory and Applications*, 2024.

Part 3: Recommend Coordinated Cyber-Physical Response

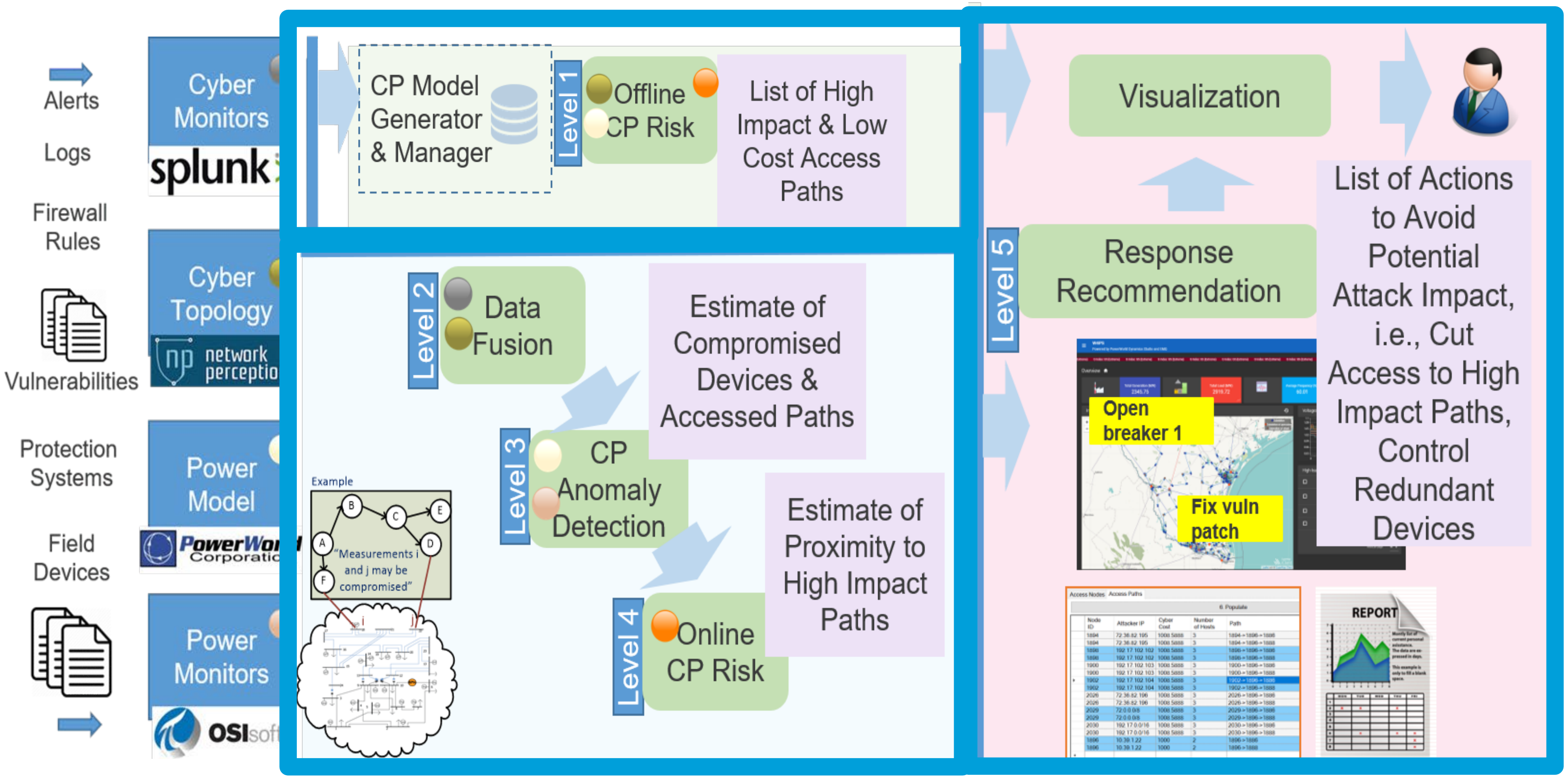
- State space, actions, reward model, and state transition model are all cyber-physical
- Reward based on cyber recovery of the compromise, considering time, cost, and impact and physical actions to reduce overloads
- Considering Q Learning and Deep Q Networks for dealing with unknown transition probabilities



S. Sun, et.al, “An AI-based Approach for Scalable Cyber-physical Optimal Response in Power Systems,” *TPEC*, 2024.
H. Huang, et.al., “Toward Resilient Modern Power Systems: From Single Domain to Cross-Domain Resilience Enhancement,” *Proceedings of IEEE*, 2024.

Resiliency process. Adapted from North American Transmission Forum (2022). T. Overbye, K. Davis, A. Birchfield, “The Electric Grid and Severe Resiliency Events,” *BRIDGE*, 2023.

CYPRES EMS MODELING & WORKFLOW

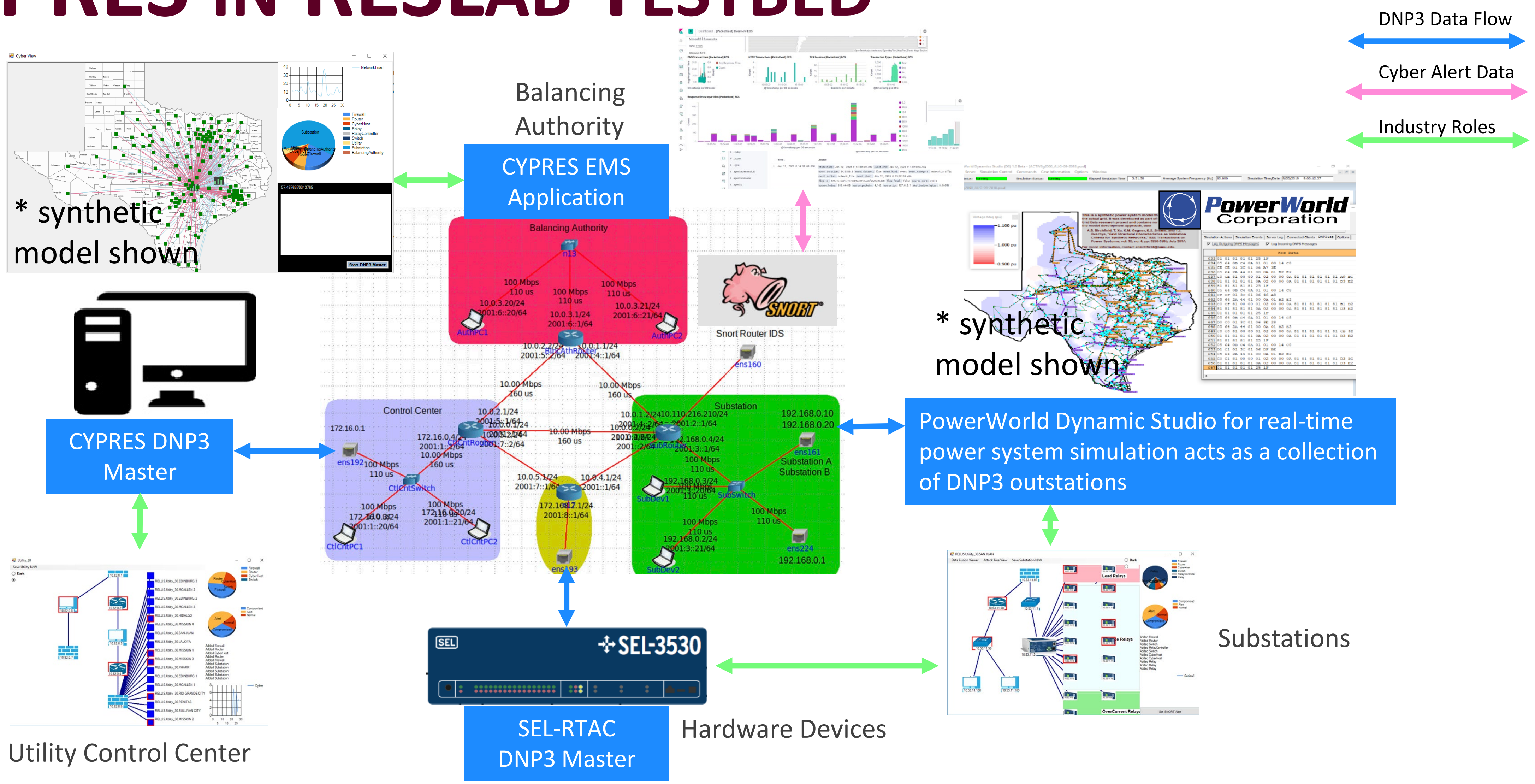


U.S. DEPARTMENT OF ENERGY

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

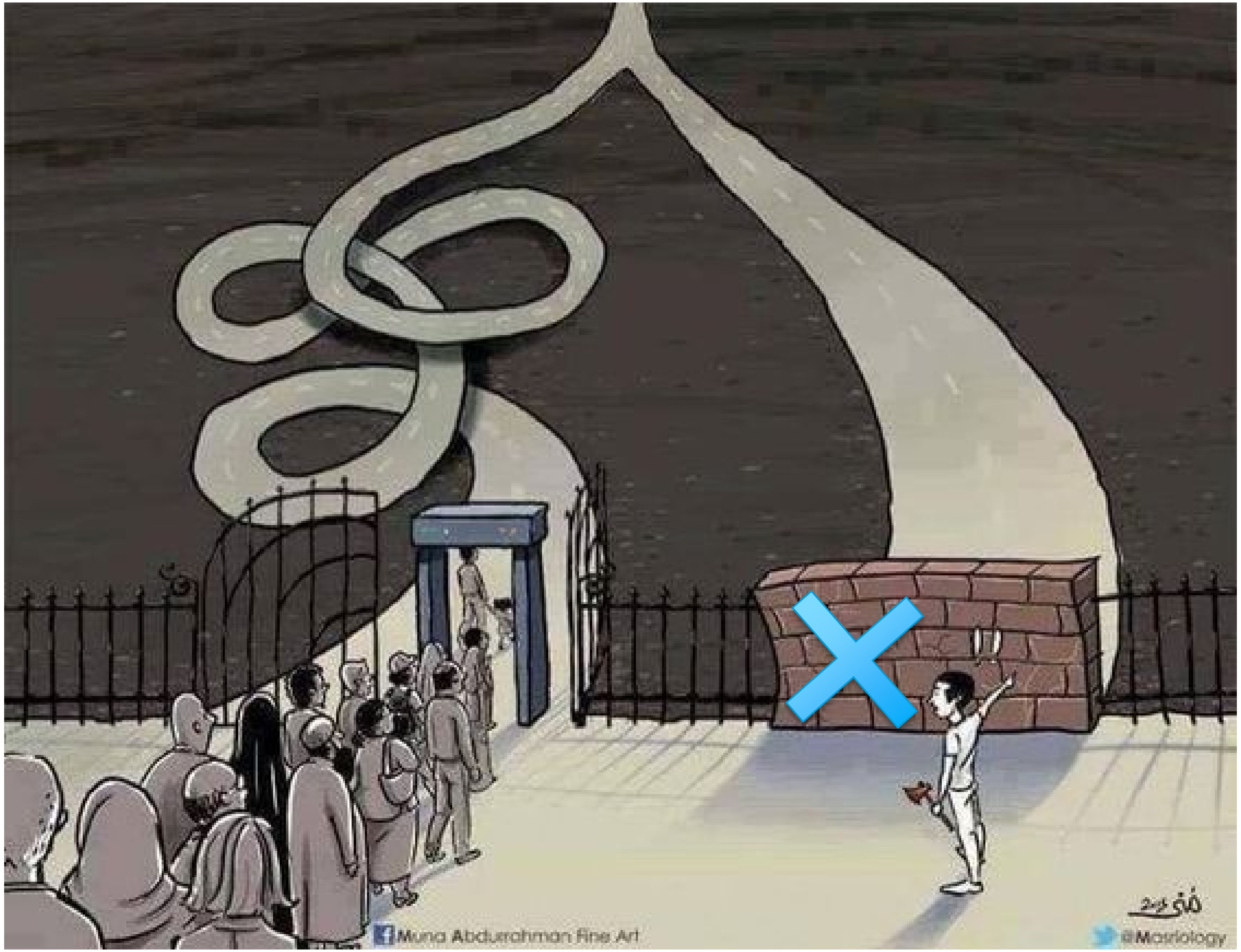
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

CYPRES in RESLab Testbed



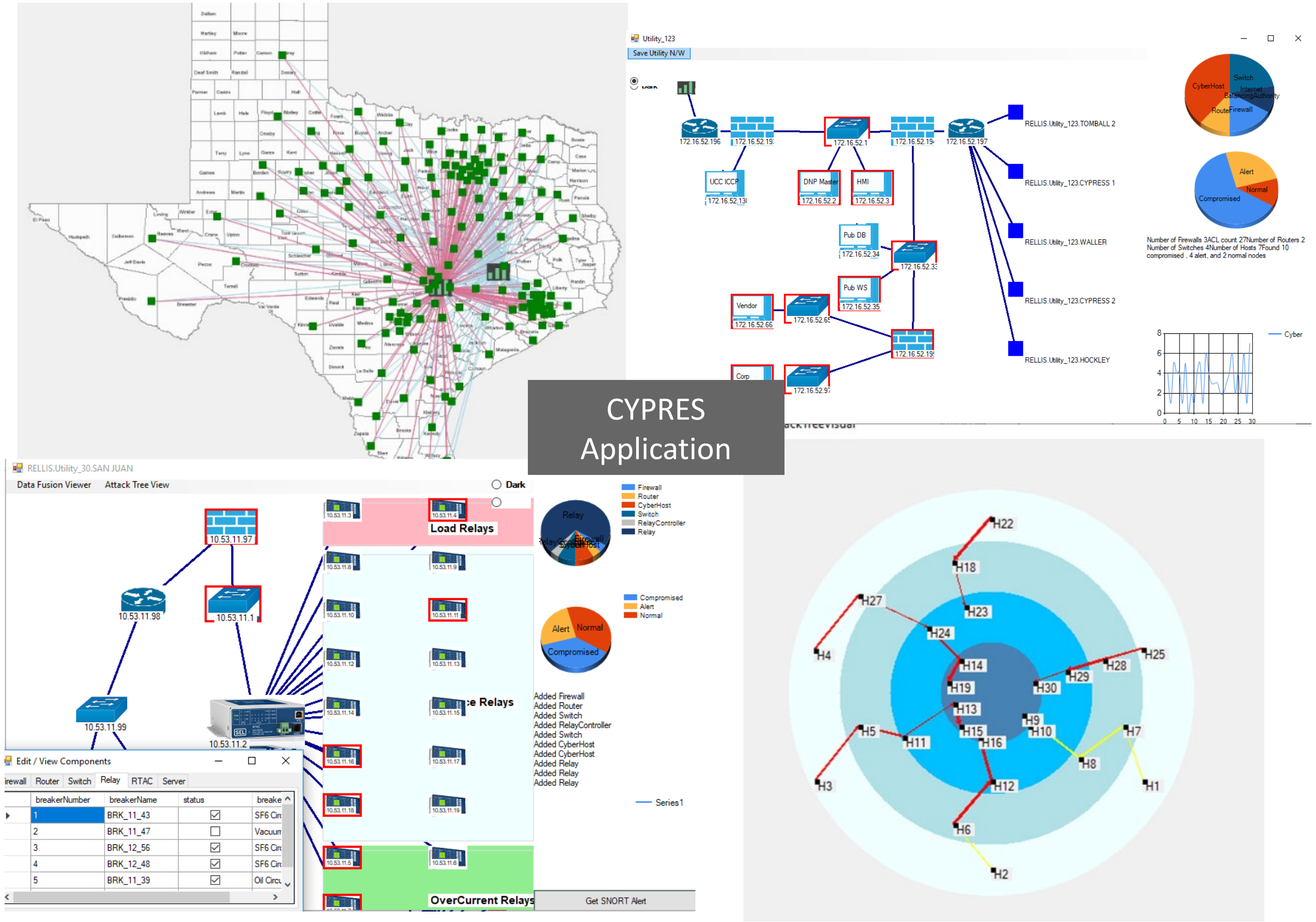
A. Sahu, et al. "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Physical Systems: Theory & Applications*, 2021.
P. Wlazlo, et al. "Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed," *IET Cyber-Physical Systems: Theory and Applications*, 2021.

The Old Way vs. The New Way



What I Tell My Students!

The New Way



Cyber-Physical Energy Management

(*) A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, A. Goulart, "Design of Next-Generation Cyber-Physical Energy Management Systems: Monitoring to Mitigation," *IEEE Open Access Journal of Power and Energy*, 2023.

From CYPRES EMS to Testbeds and V&V

Develop Defense Mechanisms

Verify and Validate

Deliver Models, Methods, Designs

TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

Cyber-Physical Resilient Energy Systems

1. Model

- Represent, manage, and visualize the cyber physical model

2. Monitor and Verify

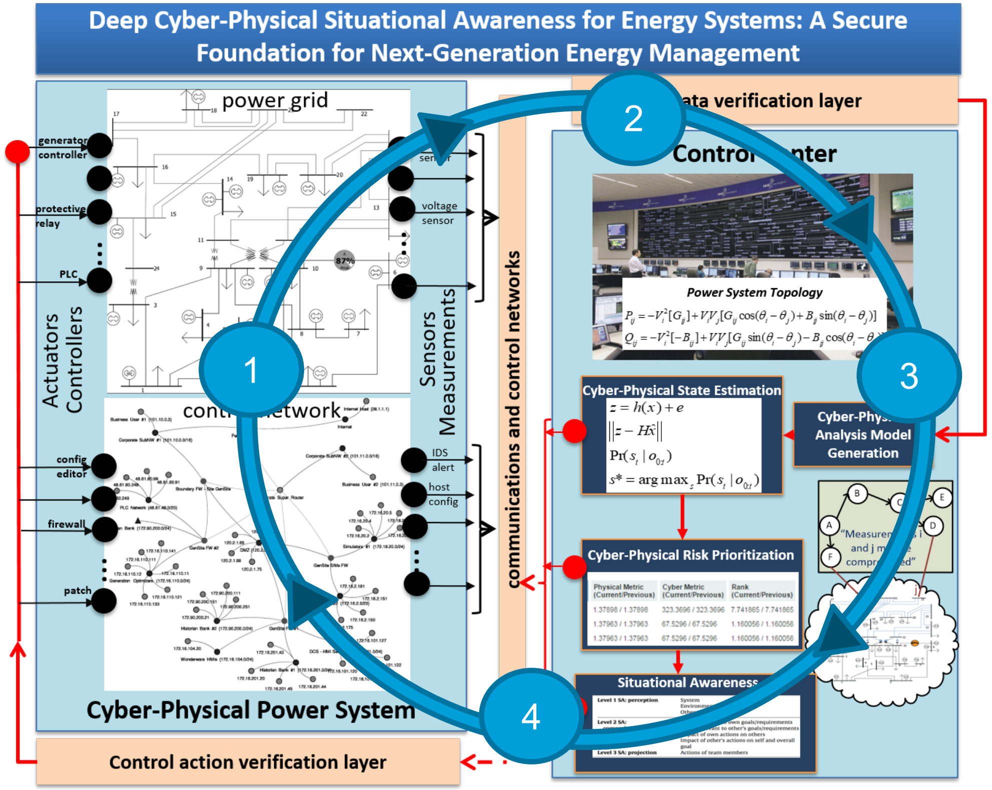
- Fuse streaming inputs to the model
- Estimate cyber-physical state

3. Analysis

- Early attack detection
- Cyber-physical risk analysis
- Cyber-physical detection and situational awareness use cases

4. Verify and Control

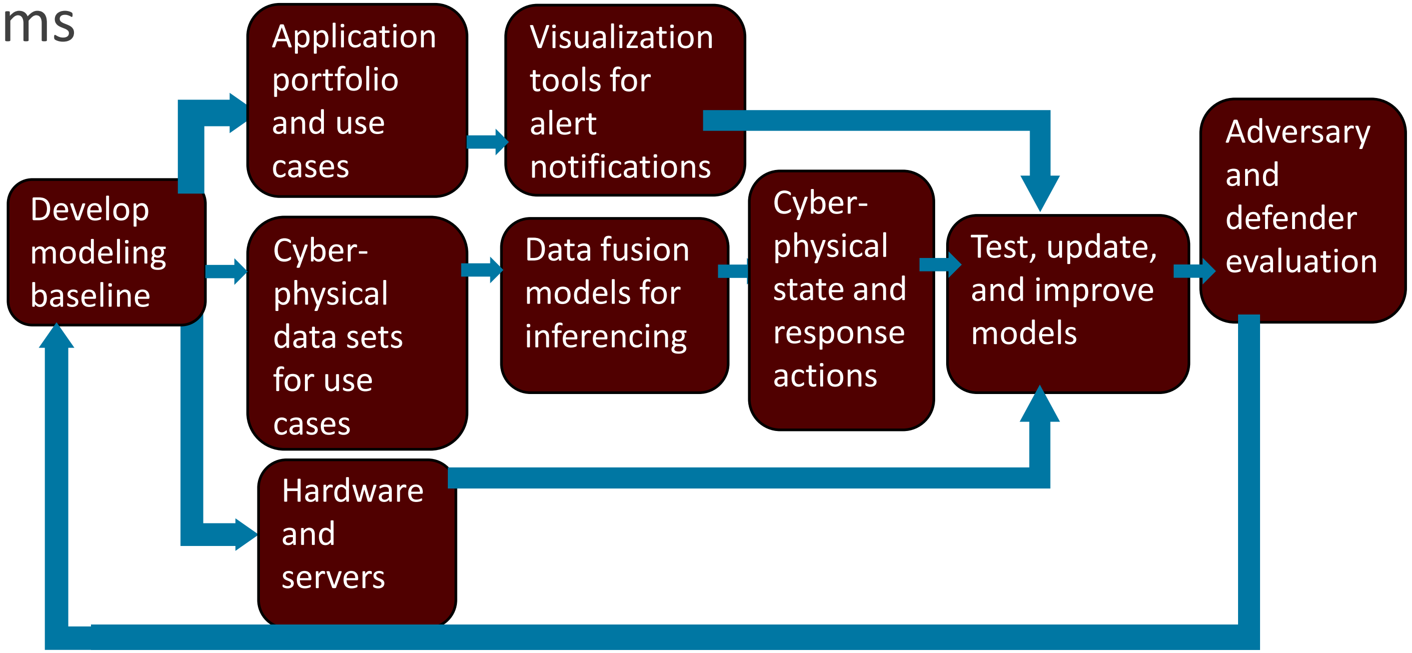
- Recommend cyber-physical actions
- Mitigations, countermeasures



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

Modeling, Emulation, and Testing for Power Grid Cyber-Physical Security Studies

- Create designs that guide modeling in **Resilient Energy Systems Lab (RESLab) testbed**
- Representations of planned systems and scenarios
  - Diagrams of the network
  - The emulation/simulation testbed architecture
- The designs and use cases are updated more information is learned
- RESLab is **a safe proving ground** for experiments of threats to power system resilience

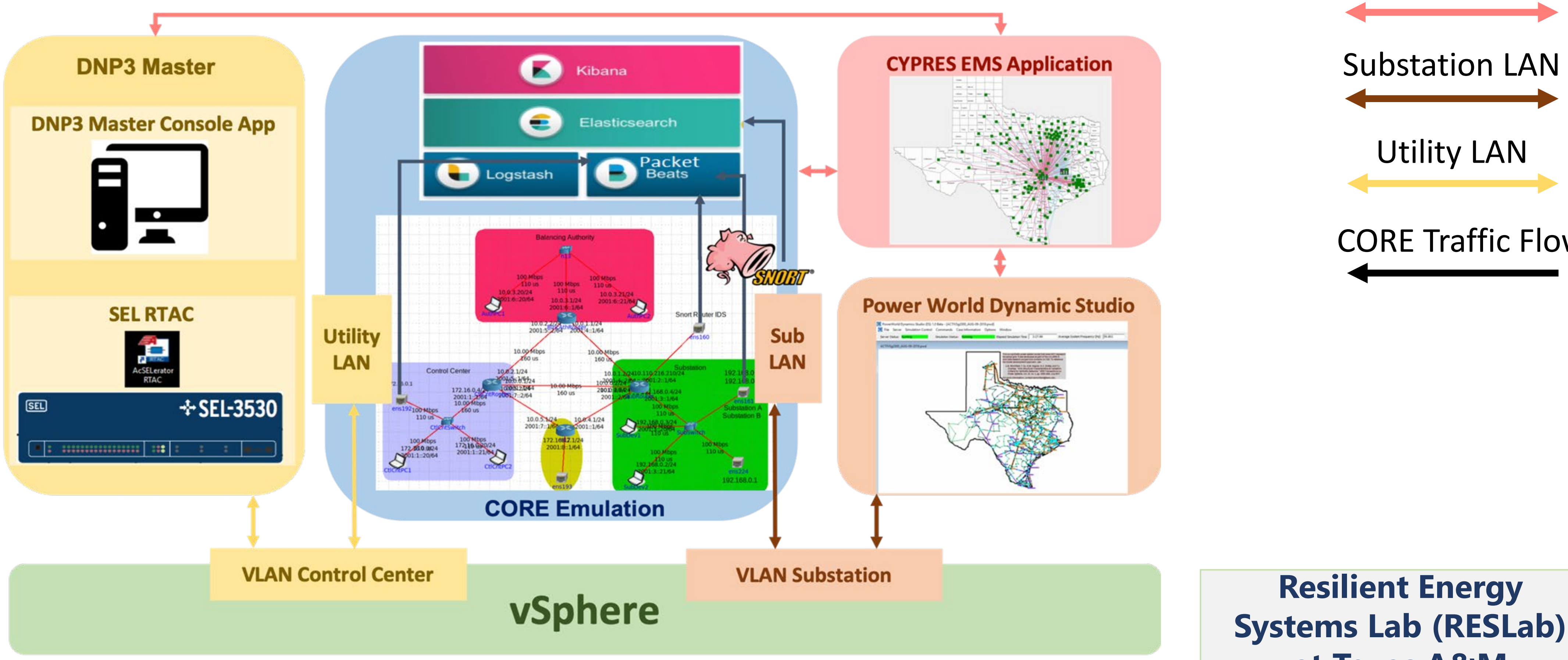


Our Agile Design and Development Cycle

(*) A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, S. Zonouz, "Design and Evaluation of a Cyber-Physical Resilient Power System Testbed," *IET Cyber-Physical Systems*, June 2021.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Overview of RESLab Testbed



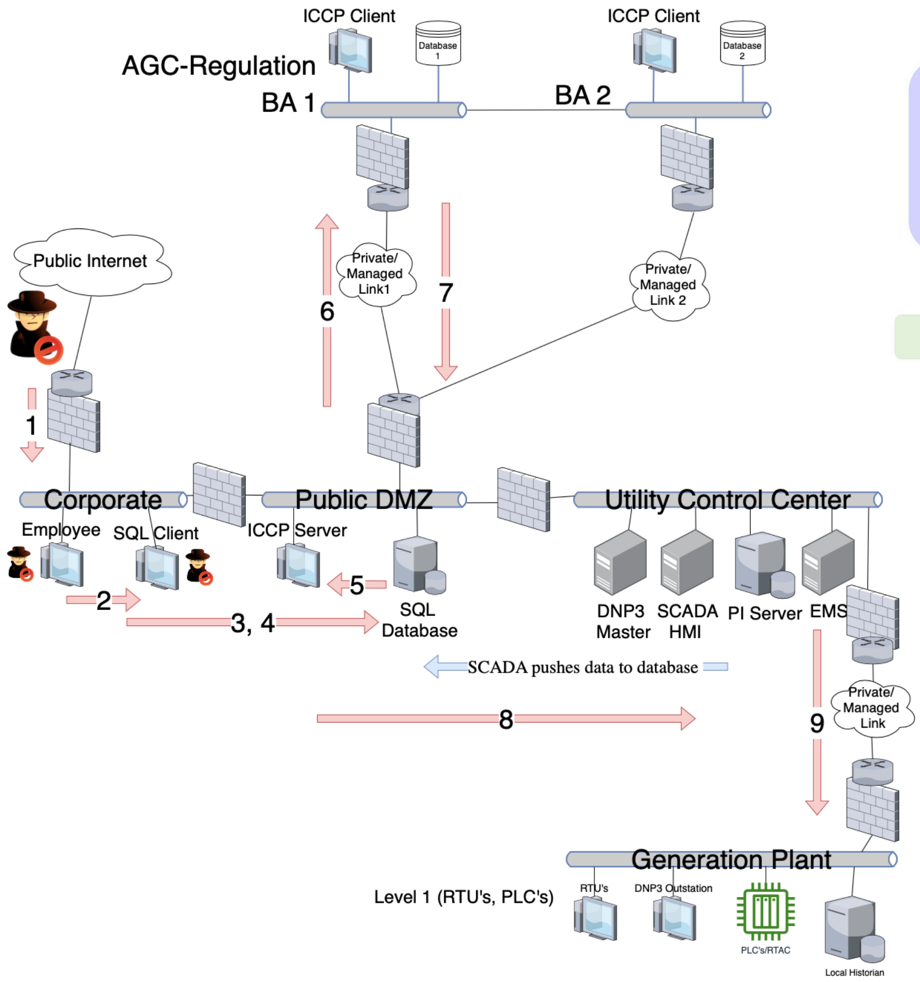
Resilient Energy Systems Lab (RESLab) at Texas A&M

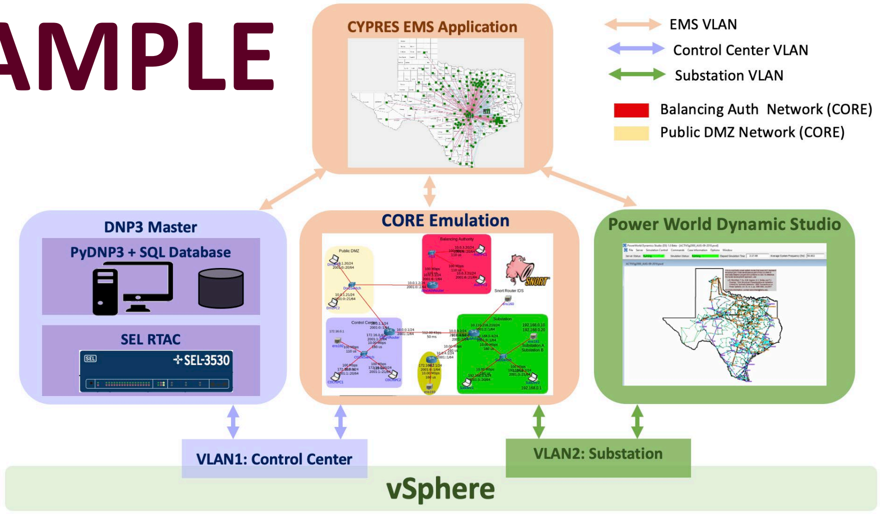
Resilient Energy System Lab (RESLab) is a cyber-physical power system consisted of emulated communication network, real-time power system simulation and power system control and protection devices.

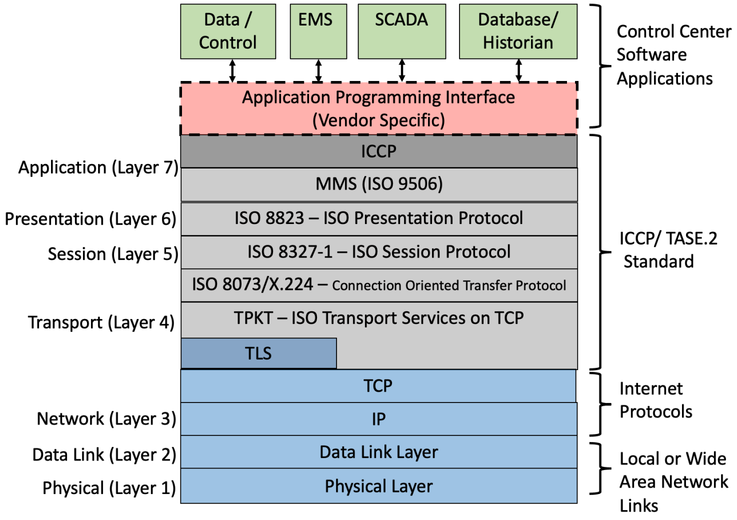
(*) A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, S. Zonouz, “Design and Evaluation of a Cyber-Physical Resilient Power System Testbed,” *IET Cyber-Physical Systems*, June 2021.

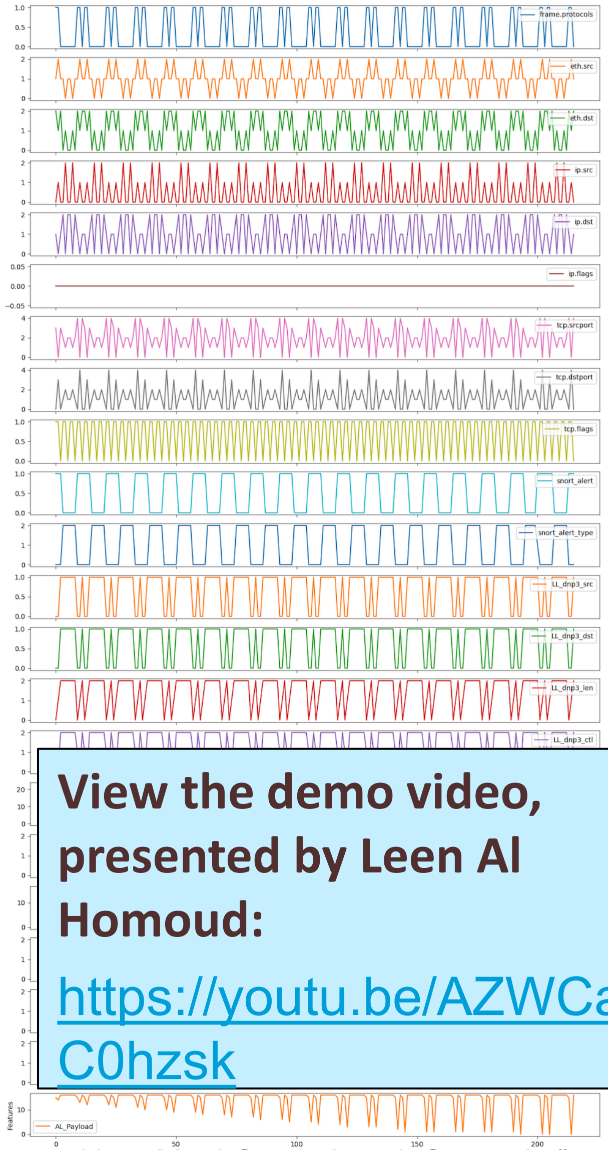
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Threat Model Example









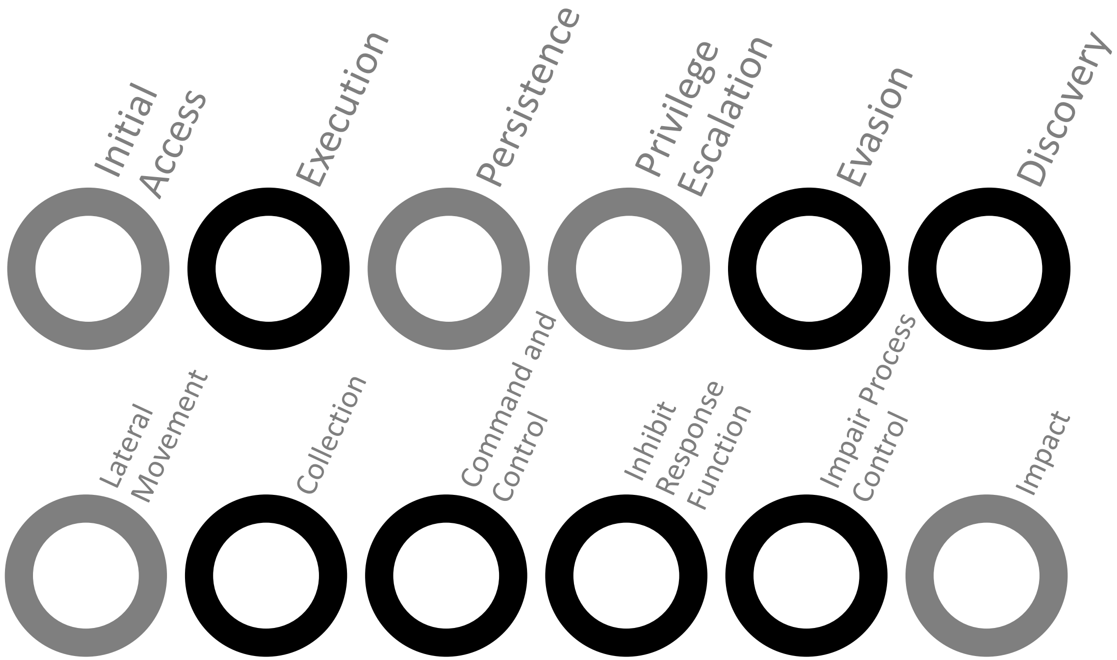
View the demo video, presented by Leen Al Homoud: https://youtu.be/AZWCaC0hzsk

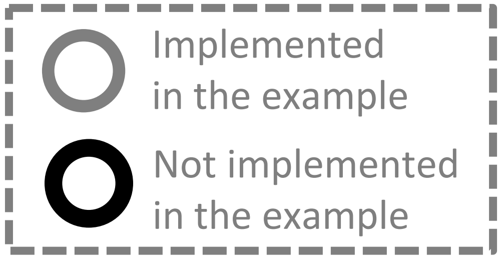
(*) L. Al Homoud, N. Barpanda, A. Goulart, K. Davis, M. Rice, "On Grid Resiliency: Cyber-Physical Detection Tool Evaluated in a Multi-Stage Attack Scenario," *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2023.

Dataset (IEEE DataPort): https://dx.doi.org/10.21227/21zx-9a54

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

MITRE ATT&CK Framework





[*] "Mitre ATT&CK®," *MITRE ATT&CK®.* [Online]. Available: https://attack.mitre.org/.
[*] "ATT&CK® for Industrial Control Systems," *attackics*. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page.
[*] "Technique matrix," *Technique Matrix - attackics*. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Technique_Matrix.
[*] "Man in the middle," *Man in the Middle, Technique T0830 - ICS | MITRE ATT&CK®*. [Online]. Available: https://attack.mitre.org/techniques/T0830/.

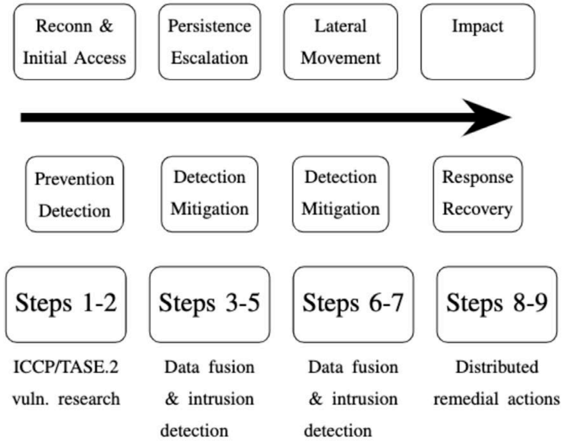
Mapping New Use Cases to ATT&CK

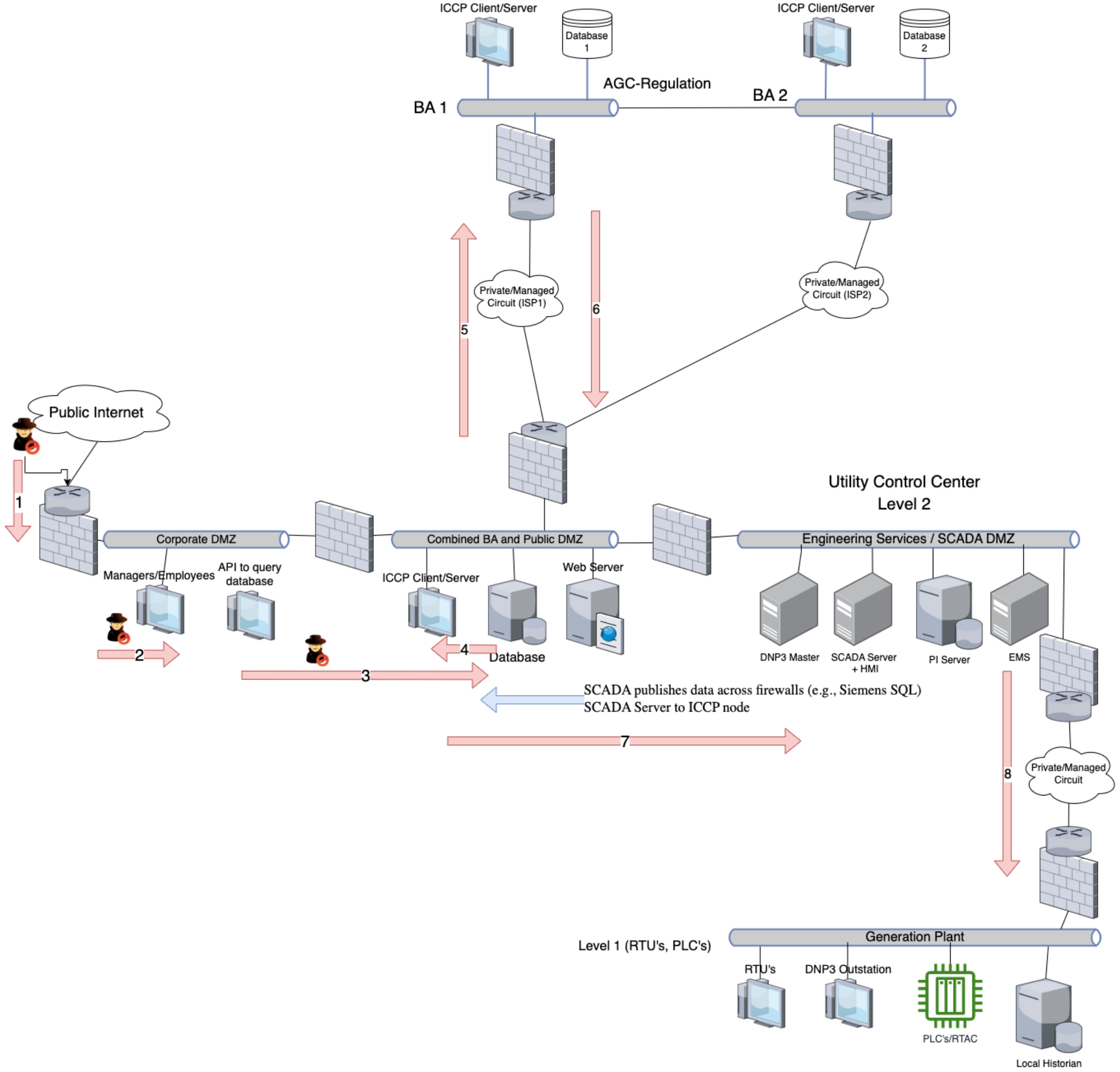
Reconnaissance and Initial Access	Persistence and Privilege Escalation	Lateral Movement	Impact
Detection, Prevention	Detection, Mitigation	Detection, Mitigation	Recovery, Response
Steps 1 and 2	Steps 3 – 6	Steps 3 – 7	Steps 8 and 9

CYPRES modeling tools to use in Cyber-Physical Resilient Power System Testbed (RESLab) [5]

- Vulnerabilities of ICCP/TASE.2 Protocol. - Sets the stage for the next phase.	- Intrusion Detection [9]. - Data Fusion for Cyberattack Detection [11]. - Man-in-The-Middle Attacks [12]. - Denial of Service [13].	- Intrusion Detection [9]. - Data Fusion for Cyberattack Detection [11]. - Man-in-The-Middle Attacks [12]. - Denial of Service [13].	- Remedial Action Schemes [7]. - Distributed Controller Defense [8]. - SCORE [6].

NETWORK DIAGRAM: MULTI-STAGE THREAT





(*) L. Al Hamoud, N. Barpanda, A. Goulart, K. Davis, M. Rice, "On Grid Resiliency: Cyber-Physical Detection Tool Evaluated in a Multi-Stage Attack Scenario," *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2023.

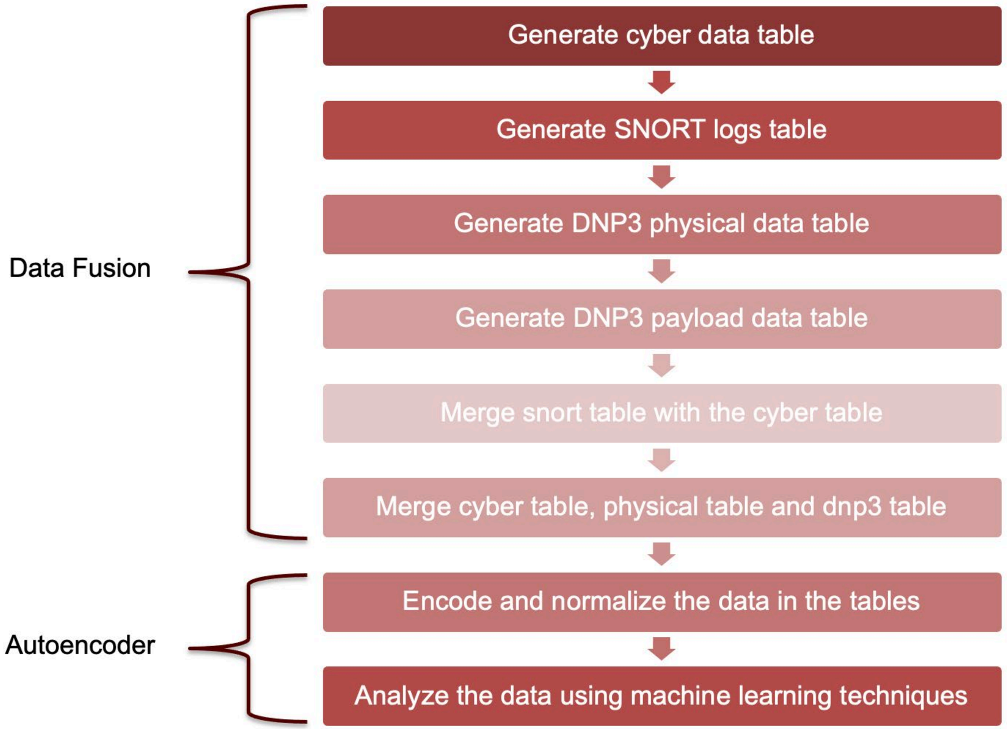
SQL INJECTION AND DEFENSE

Algorithm 1 SQL Injection on Generator SQL Server

1. *Client sends query to log in*
2. *SELECT * FROM users WHERE username = 'X' AND password = 'example' OR 'a'='a'*
3. *Server returns TRUE. Bypass authentication.*
4. *Client accesses data and modifies one column*
5. *Use Postman API to change gen2 columnn*

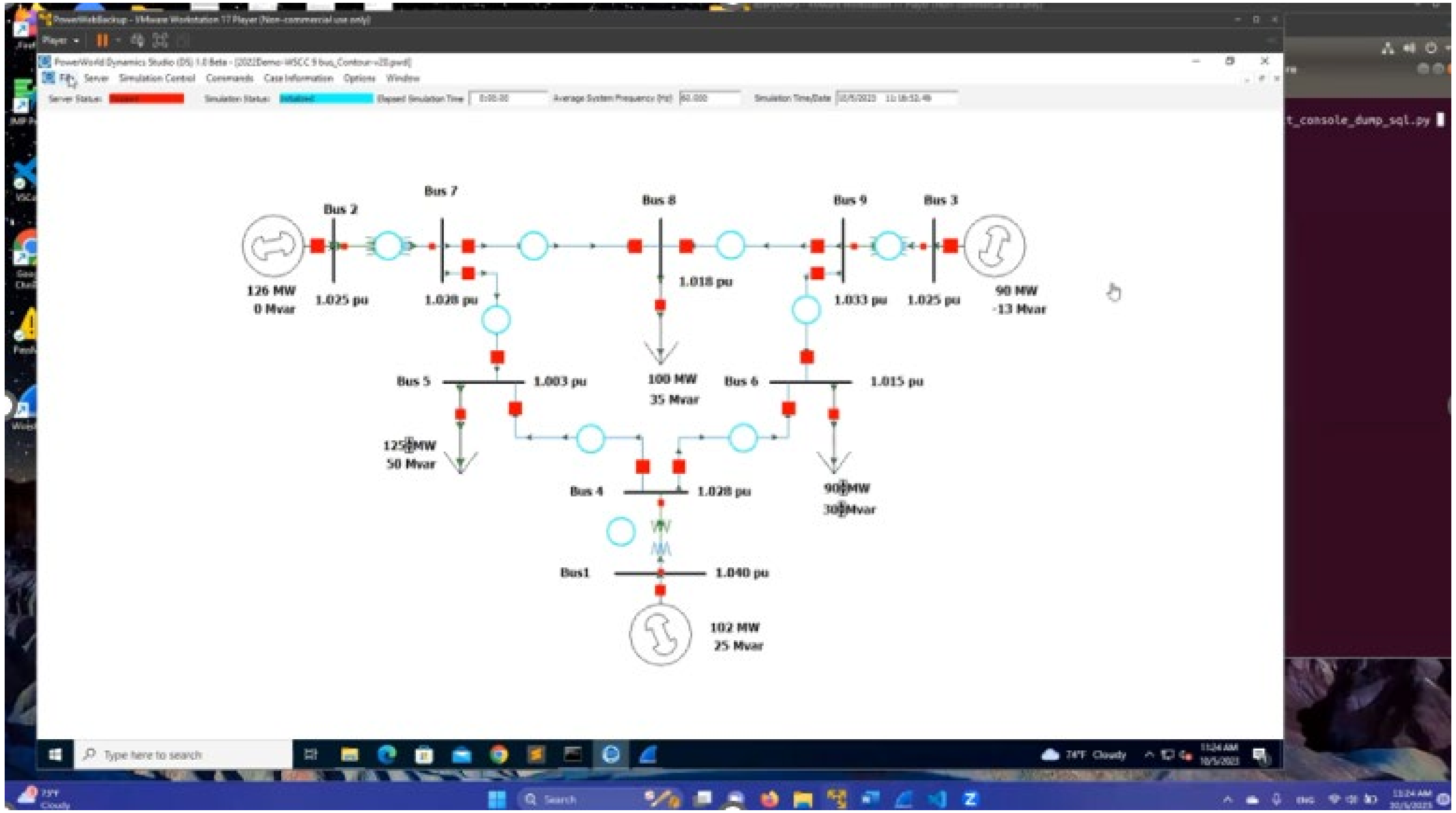
id	time	gen2	gen3	ACEgen2	ACEgen3	spGen2	spGen3
1	12:20:59	250	90	0	0	126.335	90
2	12:20:59	250	90	0	0	126.335	90
3	12:21:04	250	90	0.0001	0.0001	126.335	89.9998
4	12:21:09	250	90	0.0001	-0.00000000000000710543	126.335	90
5	12:21:14	250	90	0	0.0001	126.335	89.9998
6	12:21:19	250	90	0.0001	0.0001	126.335	89.9998
7	12:21:24	250	90	0.0001	-0.00000000000000710543	126.335	90
8	12:21:29	250	90	0.0001	-0.00000000000000710543	126.335	90
9	12:21:34	250	90	0.0001	-0.00000000000000710543	126.335	90
10	12:21:39	250	90	0.0001	-0.00000000000000710543	126.335	90
11	12:21:44	250	90	-0.0000...	-0.00000000000000710543	126.335	90

Figure: SQL database



(*) L. Al Hamoud, N. Barpanda, A. Goulart, K. Davis, M. Rice, "On Grid Resiliency: Cyber-Physical Detection Tool Evaluated in a Multi-Stage Attack Scenario," *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2023.

MULTISTAGE USE CASE



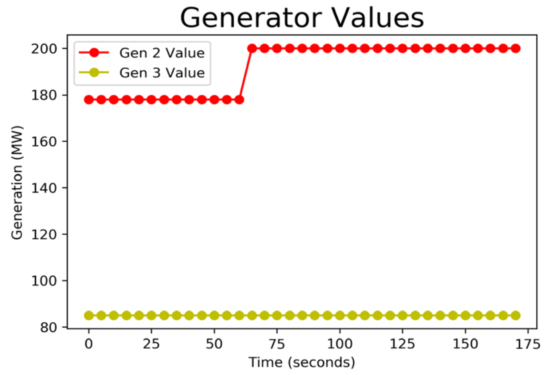
Demo Video:
https://youtu.be/AZWCaC0hzsk

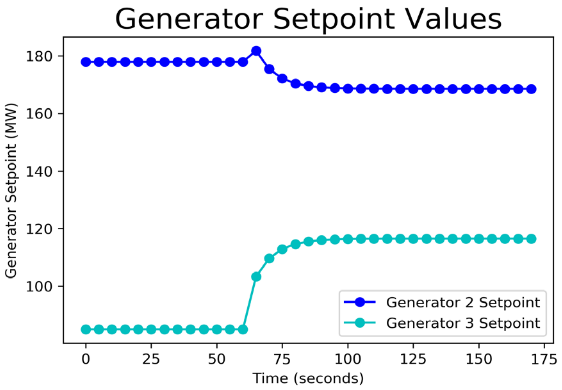
Dataset (IEEE DataPort):
https://dx.doi.org/10.21227/21zx-9a54

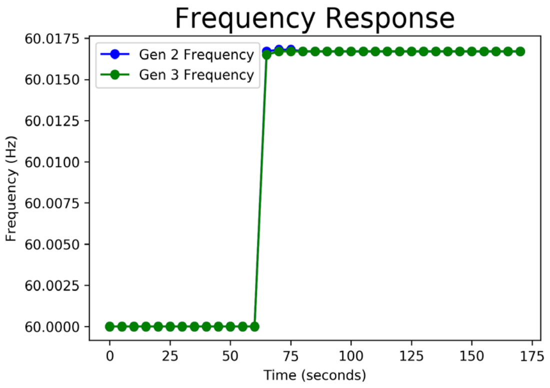
(*) L. Al Hamoud, N. Barpanda, A. Goulart, K. Davis, M. Rice, "On Grid Resiliency: Cyber-Physical Detection Tool Evaluated in a Multi-Stage Attack Scenario," *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2023.

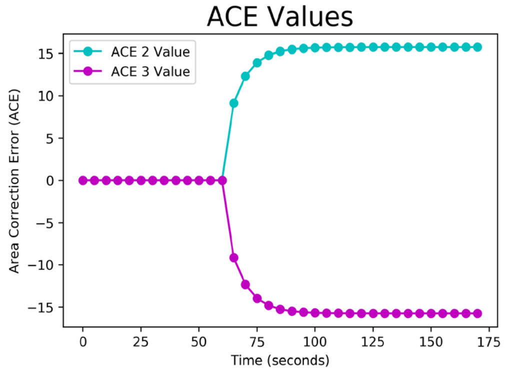
To subscribe: https://www.youtube.com/@cypres4272

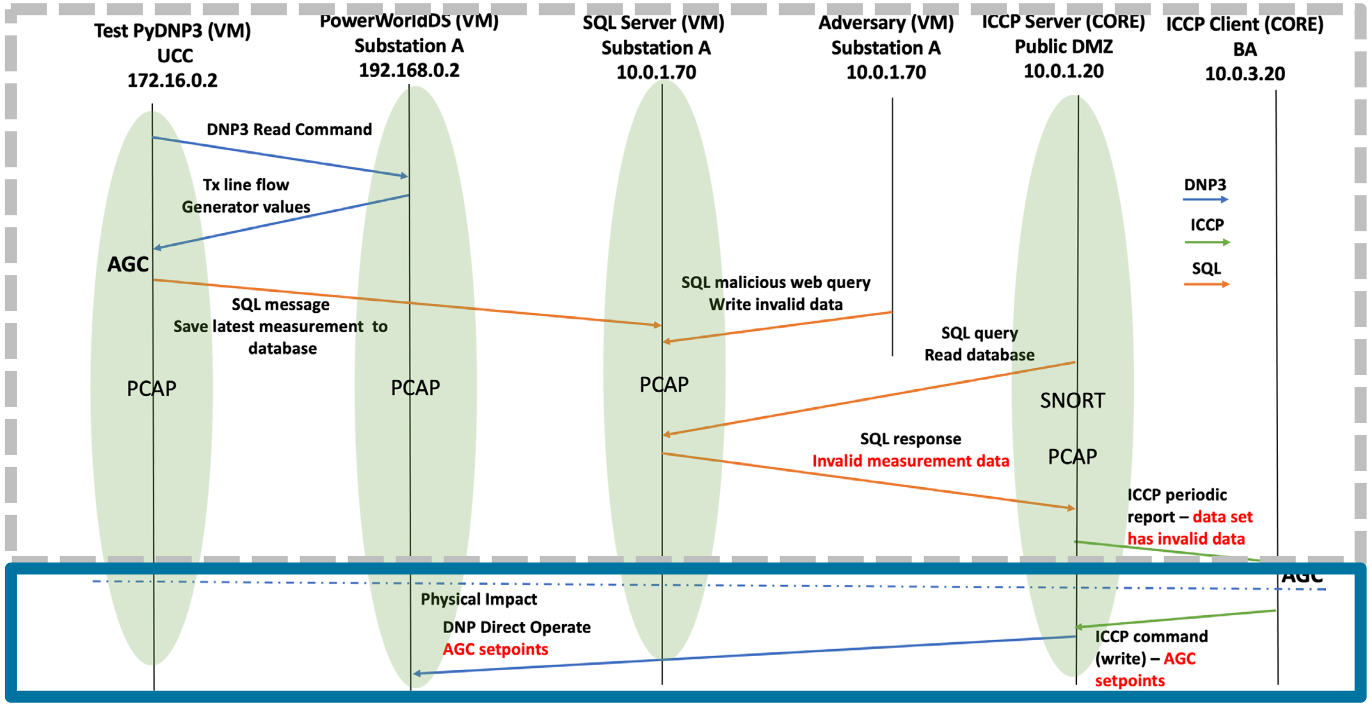
PHYSICAL RESPONSE





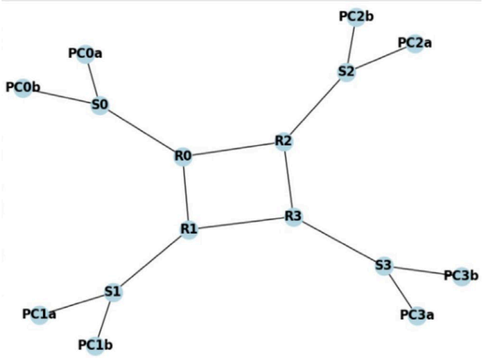


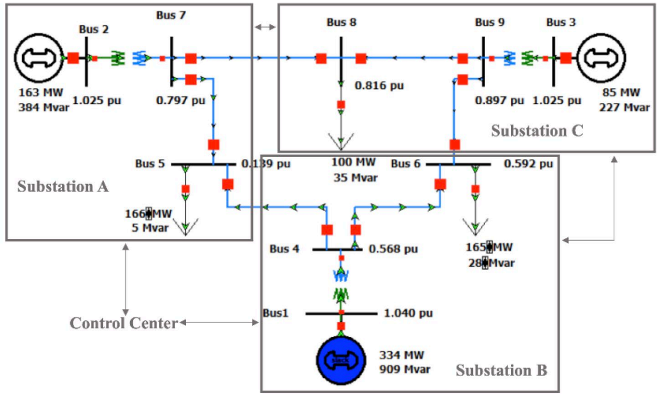


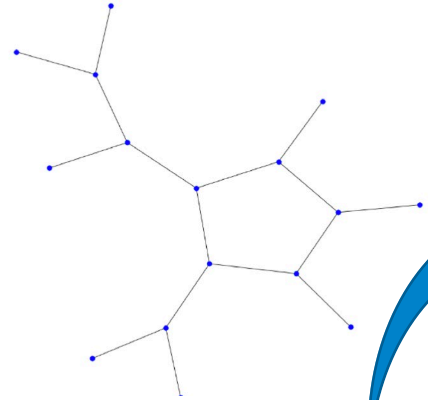


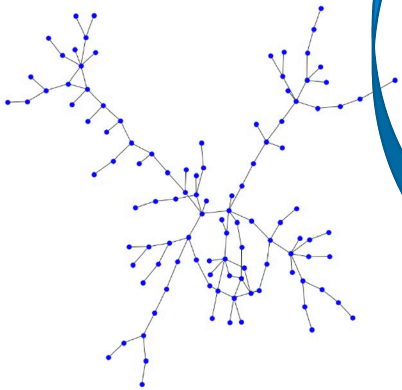
(*) L. Al Homoud, et. al, “Analyzing a Multi-Stage Cyber Threat and Its Impact on the Power System,” *IET Cyber-Physical Systems: Theory and Applications*, 2024.

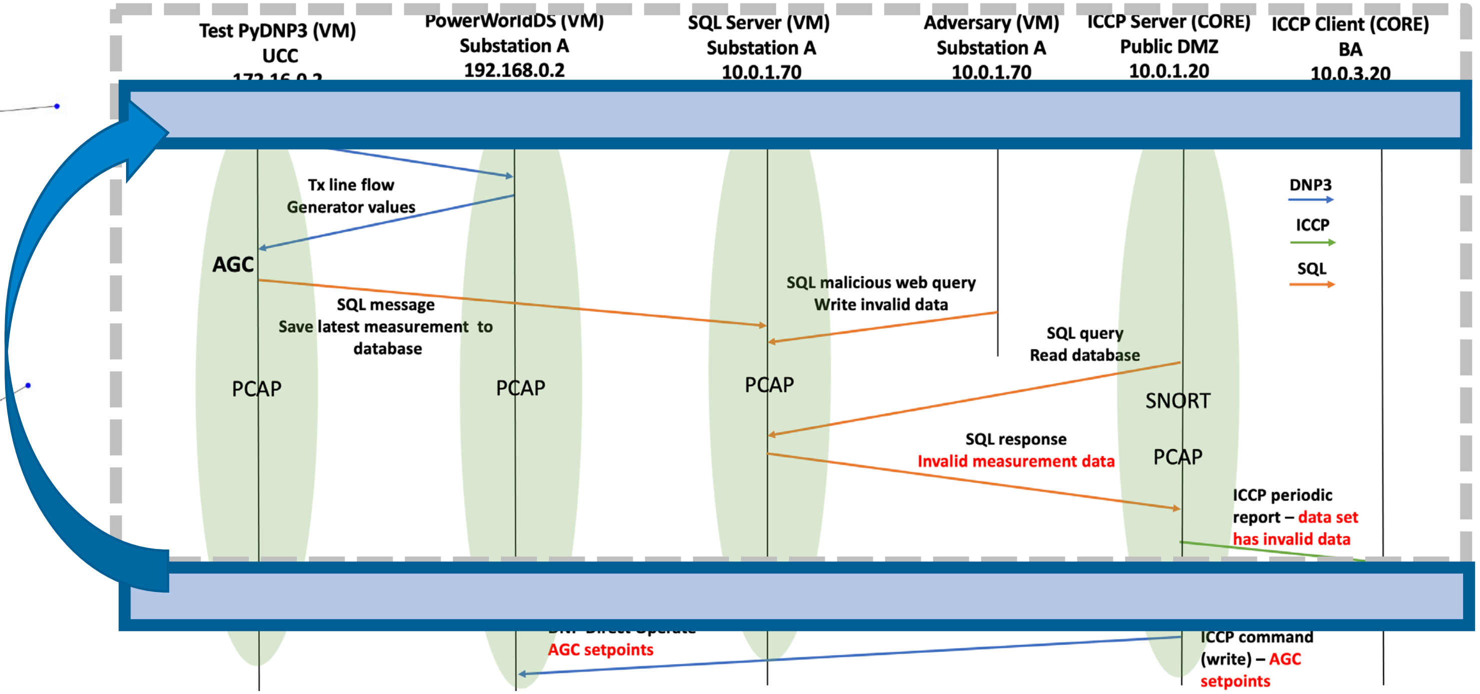
NETWORK RECONFIGURATION









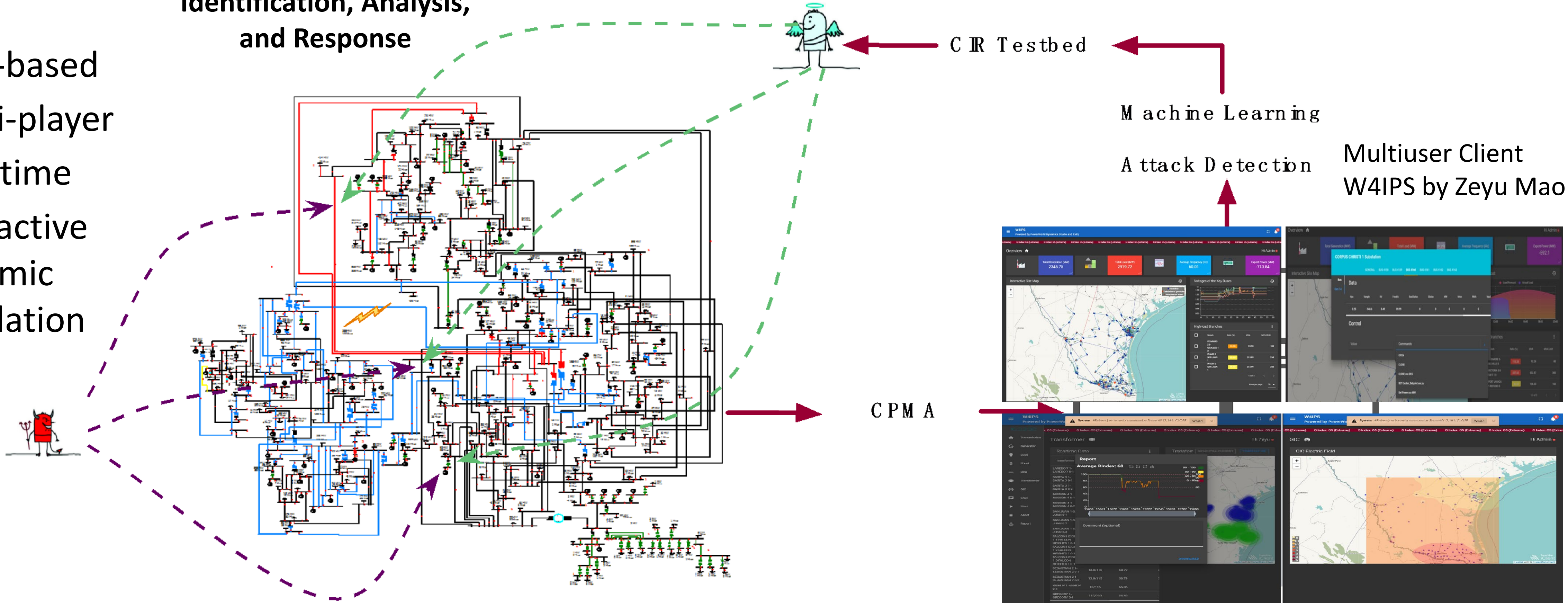


(*) L. Al Homoud, et. al, "Analyzing a Multi-Stage Cyber Threat and Its Impact on the Power System," *IET Cyber-Physical Systems: Theory and Applications*, 2024.
(*) X. Huo, H. Huang, K. R. Davis, H. V. Poor, Mingxi Liu, "A Review on Scalable and Privacy-Preserving Multi-Agent Frameworks for Distributed Energy Resource Control," *Advances in Applied Energy*, 2024.
(*) X. Huo, S. Sun, K. A. Haque, L. Al Homoud, K. R. Davis, "Cooperative optimization of grid-edge cyber and physical resources for resilient power system operation," *IEEE PESGM*, July 2025.

TESTBEDS FOR INTERACTIVE GRID DEFENSE

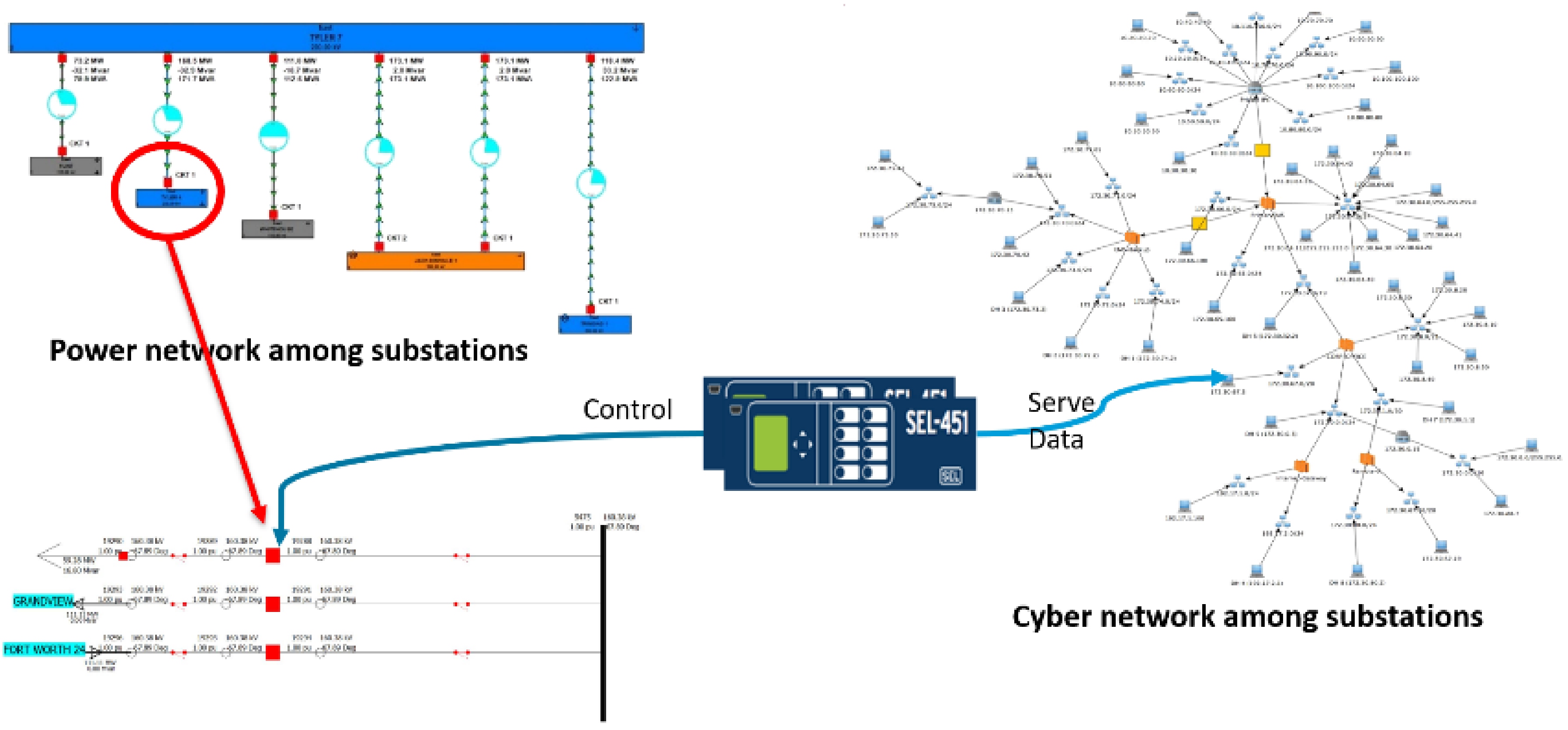
- Web-based
- Multi-player
- Real-time
- Interactive dynamic simulation

Cyber Attack Risk Identification, Analysis, and Response



(*) Z. Mao, H. Huang, K Davis, "W4IPS: A web-based interactive power system simulation environment for power system security analysis," *HICSS 2020*.
(**) A. Sahu et al, "Data Processing and Model Selection for Machine Learning-based Network Intrusion Detection," *IEEE CQR 2020*.

Understanding Substation and Control Network Technology Drivers

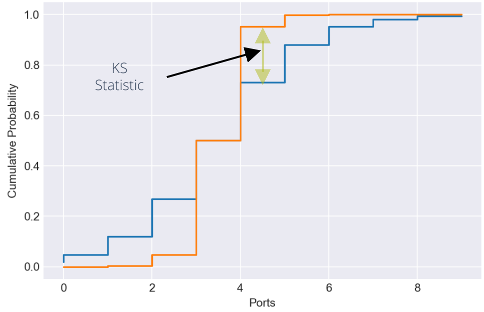


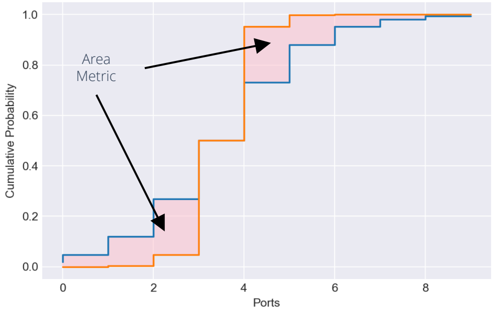
Detailed Node-Breaker Topology within Substation

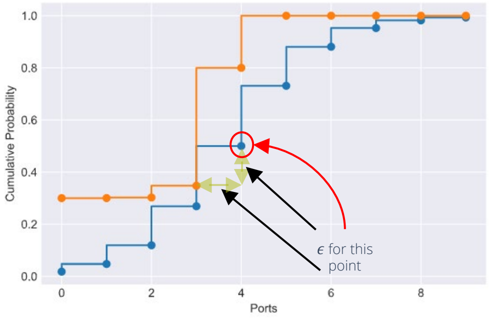
- Develop and evaluate cybersecurity technology use cases for substations and control networks in our Resilient Energy Systems Lab (RESLab)
- Study technologies in CYPRES risk analysis and response framework
- Guide cyber-physical security investment and insurance decisions

Understanding How to Quantitatively Compare Grid Cyber-Physical Security Experiments (with Sandia)

Repeatability:
How to claim an experiment has been successfully replicated or reproduced?





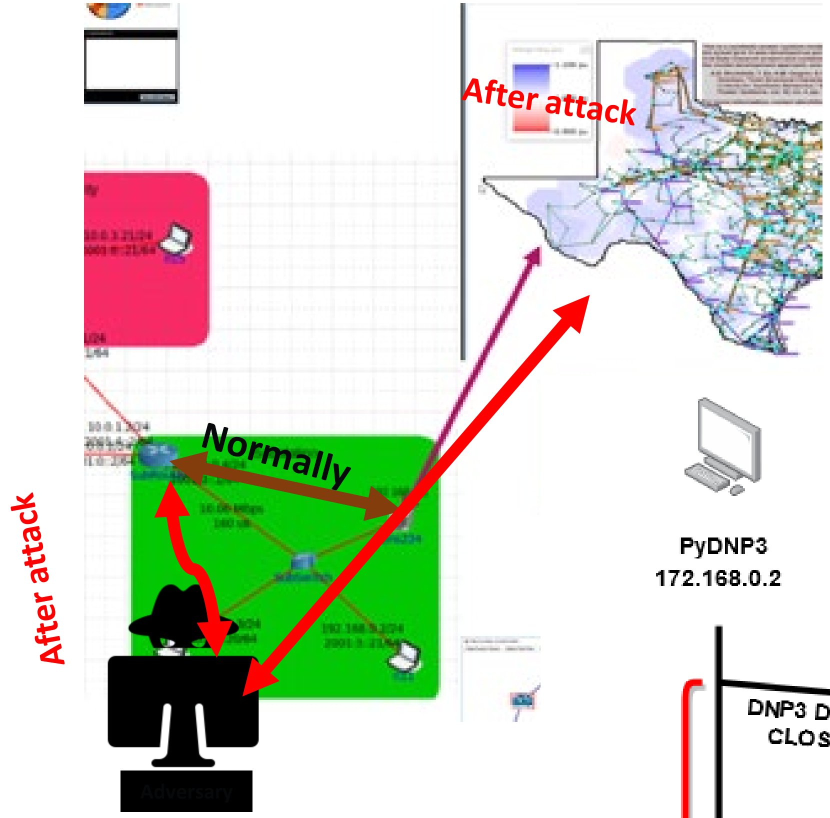


Metric	Comparison	Identical if
t-test	Means of two groups	p-value = 1
Kolmogorov-Smirnov (KS)	Distributions (max difference between CDFs)	p-value = 1
Area	Distributions (sum of the pointwise differences between CDFs; area between the two CDF curves)	Area = 0
Relative Hausdorff	Similar to the area metric but you get to "wiggle" the distribution in both x and y directions	Relative Hausdorff distance = 0

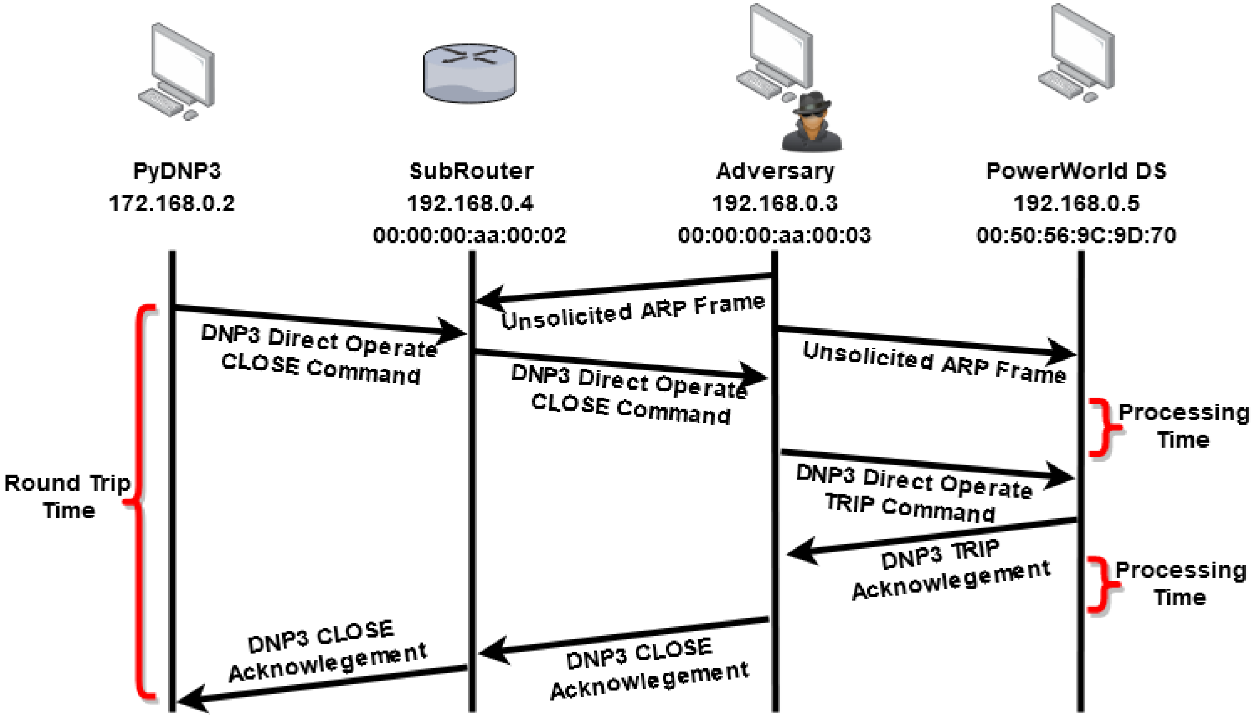
[*] T. Tarman, T. Rollins, L. Swiler, J. Cruz, E. Vugrin, H. Huang, A. Sahu, P. Wlazlo, A. Goulart, K. Davis, "Comparing Reproduced Cyber Experimentation Studies Across Different Emulation Testbeds," *ACM 14th Workshop on Cyber Security Experimentation and Test (CSET'21)*, Aug. 2021.
[**] K.A. Maupin, L.P. Swiler, N.W. Porter, "Validation Metrics for Deterministic and Probabilistic Data," *Journal of Verification, Validation and Uncertainty Quantification*, Vol. 3, Sept. 2018.
[***] O. Simpson, C. Seshadhri, and A. McGregor, Catching the head, tail, and everything in between: A streaming algorithm for the degree distribution, in *IEEE International Conference on Data Mining*, 2015.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Intrusion and Detection in the Loop



The intruder can
1. Sniff traffic
2. Modify measurement
3. Modify commands
4. Cause network congestion



P. Wlazlo, et.al, “Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed,” *IET Cyber-Physical Systems*, 2021.

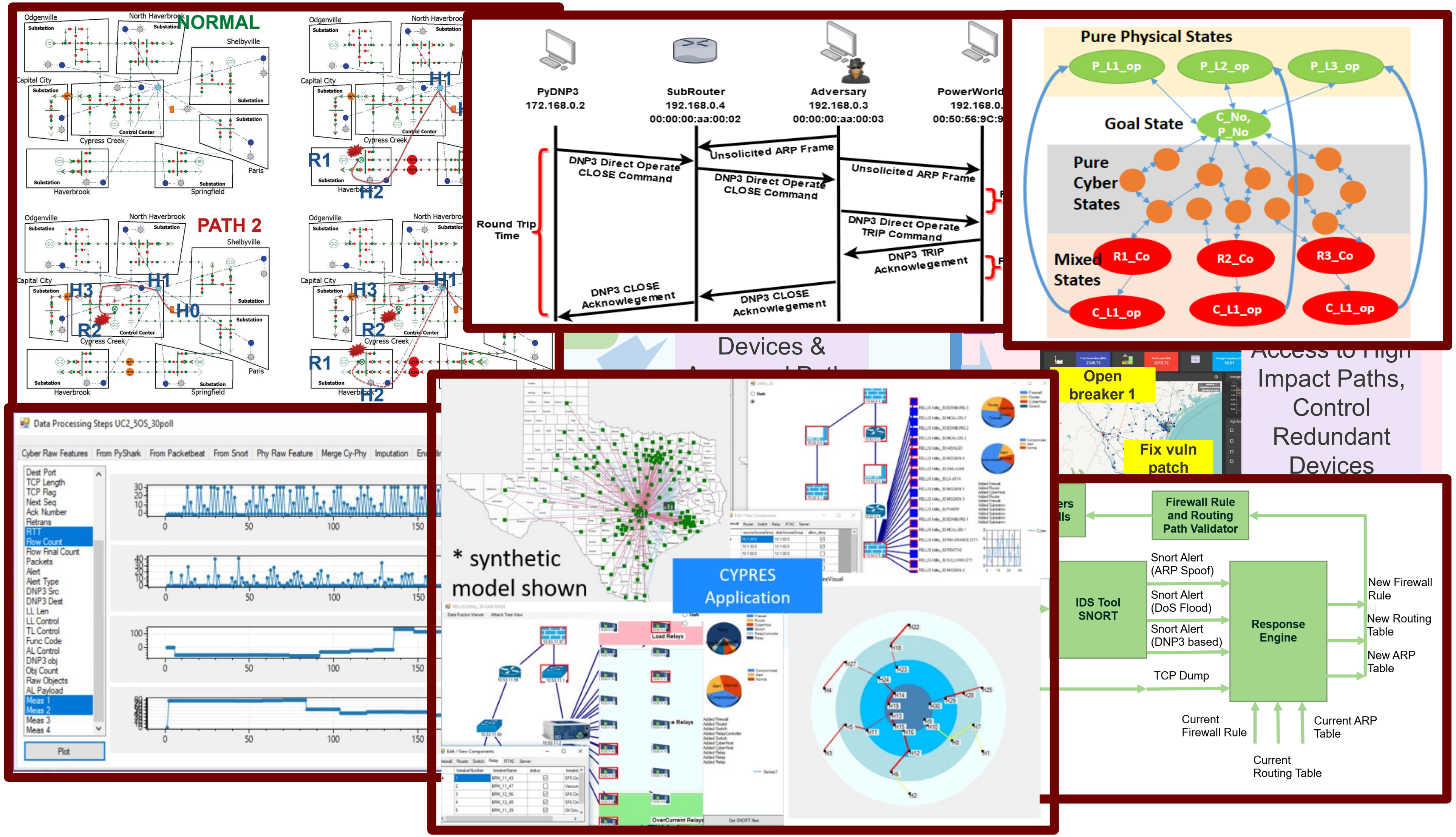
Dataset (IEEE Dataport):
https://dx.doi.org/10.21227/e4dd-2163

Estimating Cyber Physical State: Data Fusion Lab

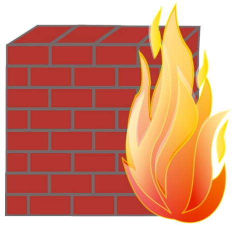
- Tutorials page on the CYPRES website to download the hands-on training materials:
  - https://cypres.engr.tamu.edu/tutorials/
  - cypres2023
- In the ***GridSecCon2021*** folder:
  - ***Tutorial2_Cyber_Physical_Data_Fusion***
- How to cite:

  A. Sahu, et al. "Multi-Source Data Fusion for Cyberattack Detection in Power Systems," *IEEE Access*, 2021.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering


NORMAL
PATH 2
Odgenville
North Haverbrook
Shelbyville
Capital City
Control Center
Cypress Creek
Paris
Haverbrook
Springfield
Substation
R1
R2
H0
H1
H2
H3
PyDNP3
172.168.0.2
SubRouter
192.168.0.4
00:00:00:aa:00:02
Adversary
192.168.0.3
00:00:00:aa:00:03
PowerWorld
Round Trip Time
DNP3 Direct Operate CLOSE Command
Unsolicited ARP Frame
DNP3 Direct Operate TRIP Command
DNP3 TRIP Acknowlegement
DNP3 CLOSE Acknowlegement
Pure Physical States
P_L1_op
P_L2_op
P_L3_op
Goal State
C_No, P_No
Pure Cyber States
Mixed States
R1_Co
R2_Co
R3_Co
C_L1_op
Devices &
Access to High Impact Paths, Control Redundant Devices
Open breaker 1
Fix vuln patch
Data Processing Steps UC2_5OS_30poll
Cyber Raw Features
From PyShark
From Packetbeat
From Snort
Phy Raw Feature
Merge Cy-Phy
Imputation
Dest Port
TCP Length
TCP Flag
Next Seq
Ack Number
Retrans
RTT
Flow Count
Flow Final Count
Packets
Alert
Alert Type
DNP3 Src
DNP3 Dest
LL Len
LL Control
TL Control
Func Code
AL Control
DNP3 obj
Obj Count
Raw Objects
AL Payload
Meas 1
Meas 2
Meas 3
Meas 4
Plot
* synthetic model shown
CYPRES Application
Firewall Rule and Routing Path Validator
Snort Alert (ARP Spoof)
Snort Alert (DoS Flood)
Snort Alert (DNP3 based)
TCP Dump
IDS Tool SNORT
Response Engine
New Firewall Rule
New Routing Table
New ARP Table
Current Firewall Rule
Current ARP Table
Current Routing Table

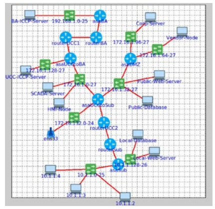
Mapping Real System Architectures and Technologies to the Emulated Environment



network perception

JSON

python



Network Data → NPView → Export JSON and Excel → OpenConduit → Core GUI

Network Data

Subnet Configuration

Firewall Rules

NPView

Parses configuration to vendor agnostic form

Data is available in internal JSON or exportable XLSX

Export JSON and Excel

JSON contains the devices and subnets

XLSX contains the firewall rules

OpenConduit

Adds tap interfaces for hardware in the loop

Converts network to graph with nodes for devices and subnets larger than /30

Links nodes together in CORE

Creates routes and firewall rules

Core GUI

Validate network setup

Recreate cyber attacks

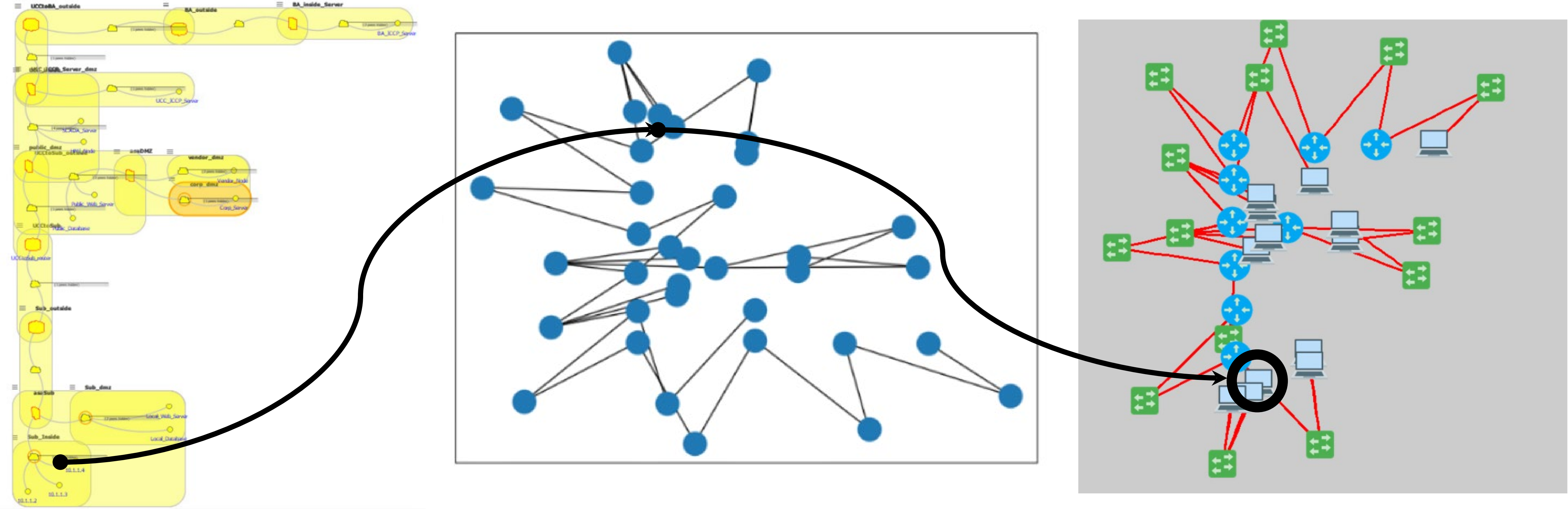
OpenConduit: NPView to CORE Data Pipeline

[*] Patrick Wlazlo MS thesis

(*) A. Umunnakwe, P. Wlazlo, et al., "OpenConduit: A Tool for Recreating Power System Communication Networks Automatically," *SmartGridComm* 2022.

Industry Defense Emulation Applications

NPView | NetworkX | core-pygui



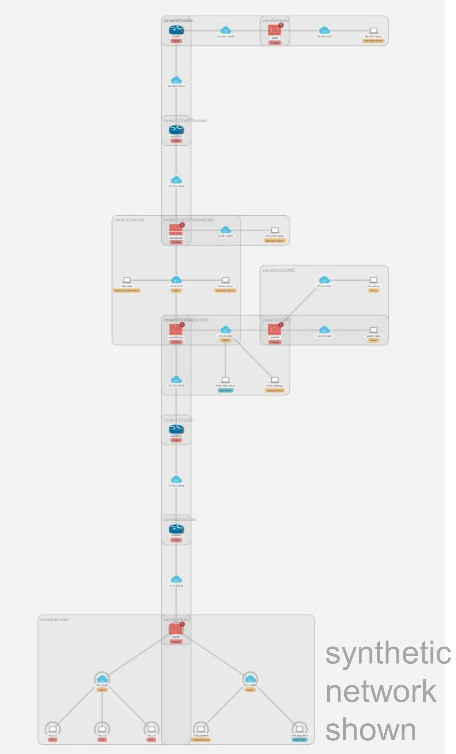
(The Advertisement) | (What the cook made) | (What got delivered by Uber)

OpenConduit: NPView to CORE Data Pipeline

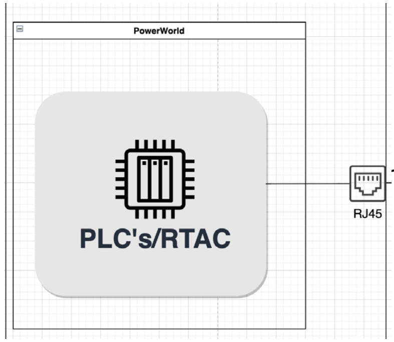
[*] Patrick Wlazlo MS thesis

(*) A. Umunnakwe, P. Wlazlo, et al., “OpenConduit: A Tool for Recreating Power System Communication Networks Automatically,” *SmartGridComm* 2022.

OpenConduit, Honeypot, and Digital Twins

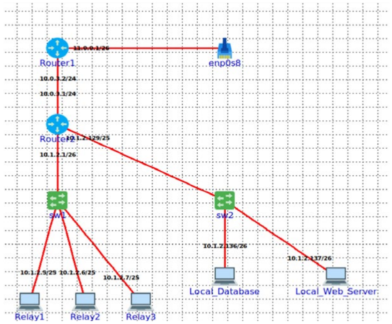


synthetic network shown

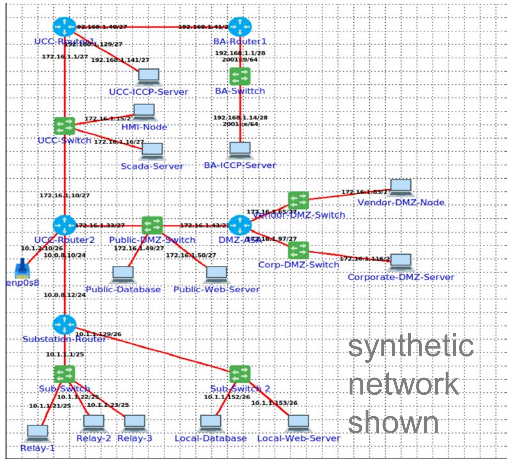


Physical Device

Honeypot Network VM



Utility Network



synthetic network shown

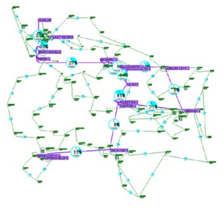
Demo Video: https://youtu.be/Fq9ZsUJYnWs

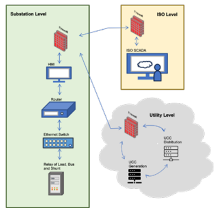
View recording of our workshop demo, presented by Ian Duncan!

(*) A. Umunnakwe, P. Wlazlo, et al., "OpenConduit: A Tool for Recreating Power System Communication Networks Automatically," *SmartGridComm* 2022.

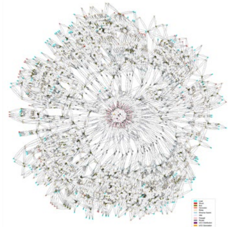
(*) B. Woody, I. Duncan, W. Watts, L. Nguyen, X. Zhuang, T. Knight, C. Acevedo, C. Harris, S. Israel, K. Davis, A. Goulart, "Demonstration of a Honeypot Use Case in a Cyber-Physical Power System Testbed," invited demo for *SmartGridComm Workshop on Testbed and Digital Twin*, 2023.

Scaling Up: Emulation-Ready Cyber-Physical Model Generation, CYPRES EMS, SCORE Back-End, DESTinE

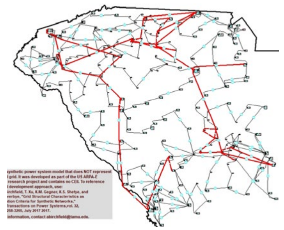

200 Bus Physical System

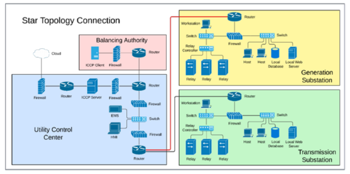


200 Bus Cyber system

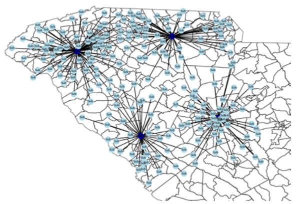

200 Bus Cyber-Physical Graph

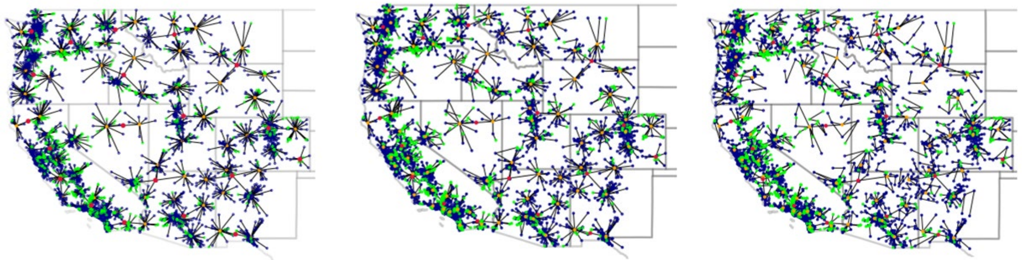
1,613 nodes and 5,995 edges


500 Bus Physical System

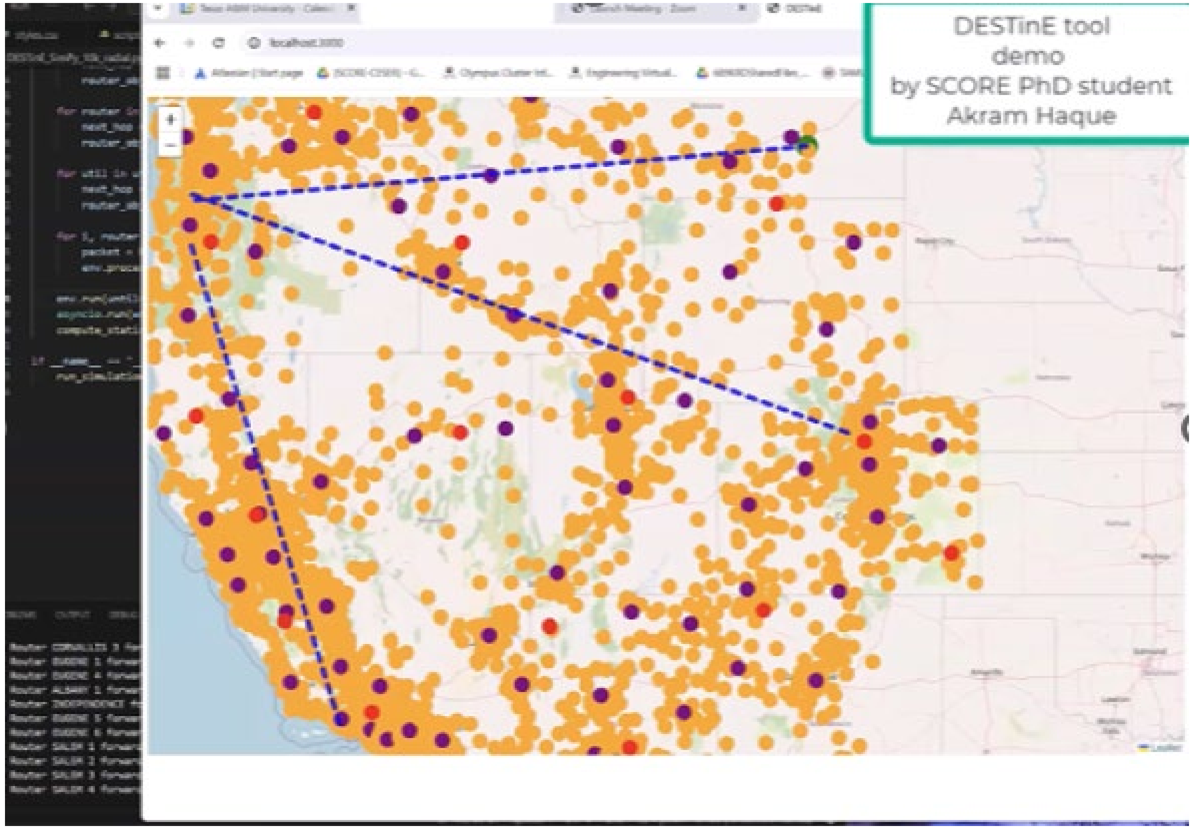


500 Bus Cyber system


500 Bus Cyber-Physical System


Three cyber models of the 10,000 bus Western United States case

Demo (model generation tool): https://youtu.be/8qecrx8ufZc



Cyber-Physical V&V: Key Points

Cyber-physical synthetic models and testbed emulation can significantly help the industry do repeatable research in our area

The idea is to use models of increasing sophistication and detail to develop power system cyber-physical defense tools

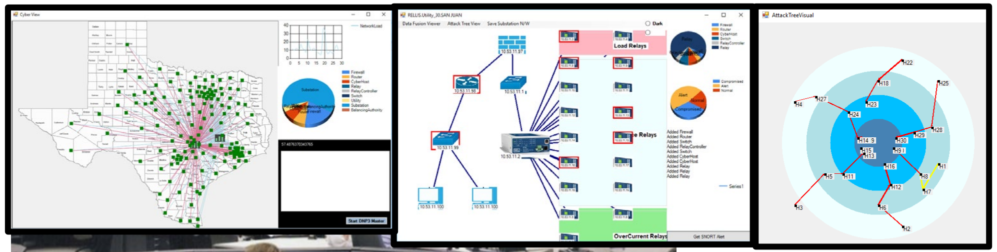
- Start with simple simulated models for testing
- Simulate/emulate in testbed
- Scale up to model more utilities and complexity

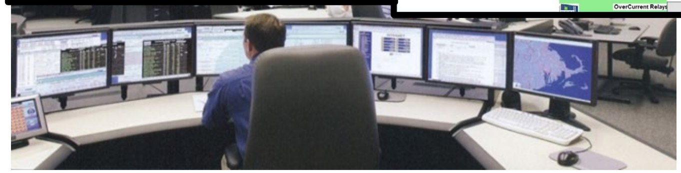
TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

Collaborations for Sector Defense: Q&A

Automatic Risk-Based Searching for Decision Intelligence

Anomaly and Sensor Integrity Inference





Dr. Kate Davis
katedavis@tamu.edu

HKN Officer Social at Dr. Davis's house, April 2025

- Target is to strengthen security and resilience of asset owners and regional reliability organizations
- Security-oriented cyber-physical energy management systems that are easily deployable
- Multi-disciplinary industry/academic team developing and testing proof-of-concepts together

This work is supported by the US Department of Energy under award numbers DE-OE0000895 and DE-CR0000018, the National Science Foundation under award numbers 1808064 and 2220347, and ERDC under W9132T239C007.