Closing the Loop: Developing and Validating a Next-Generation Cyber-Physical Energy Management System from Situational Awareness to Risk Mitigation

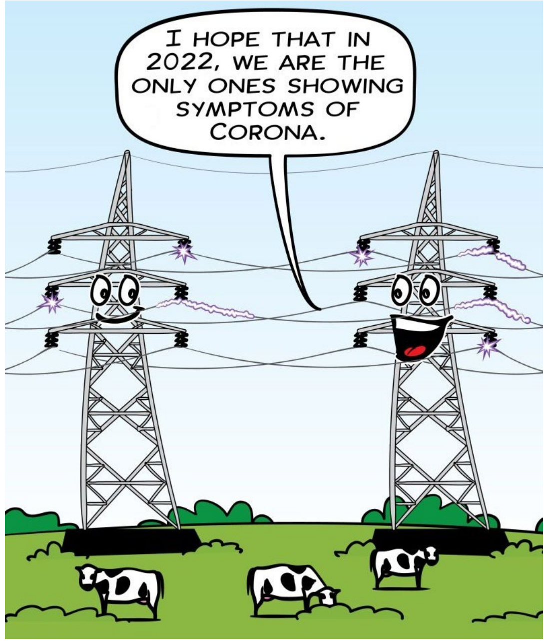
Dr. Kate Davis
TEES Young Faculty Fellow
Assistant Professor
katedavis@tamu.edu

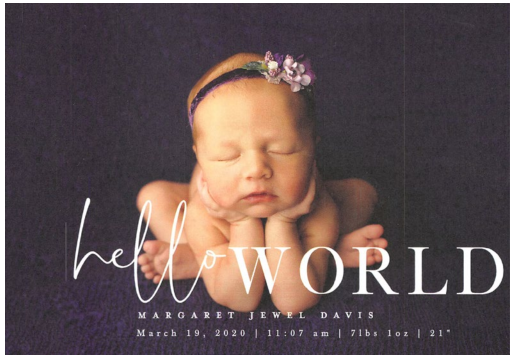
PSERC Webinar - Aug. 31, 2022

PSERC

TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

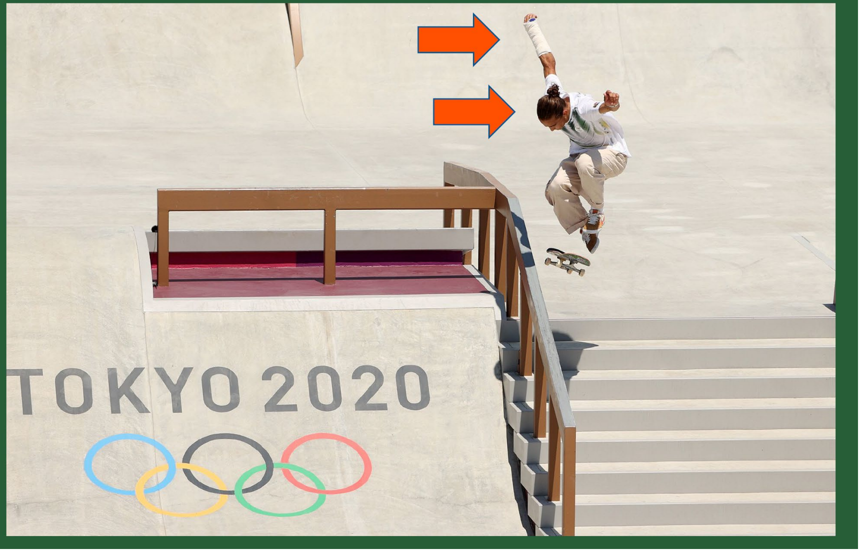
HOWDY!





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

(*) Dan Smith, LCRA, "Transmission Resilience and Winter Storm Uri," 53rd NAPS 2021 Keynote.

Jan. 2022

Feb. 2022

My recent first hand experience with resilience.

It's great to be back to normal!

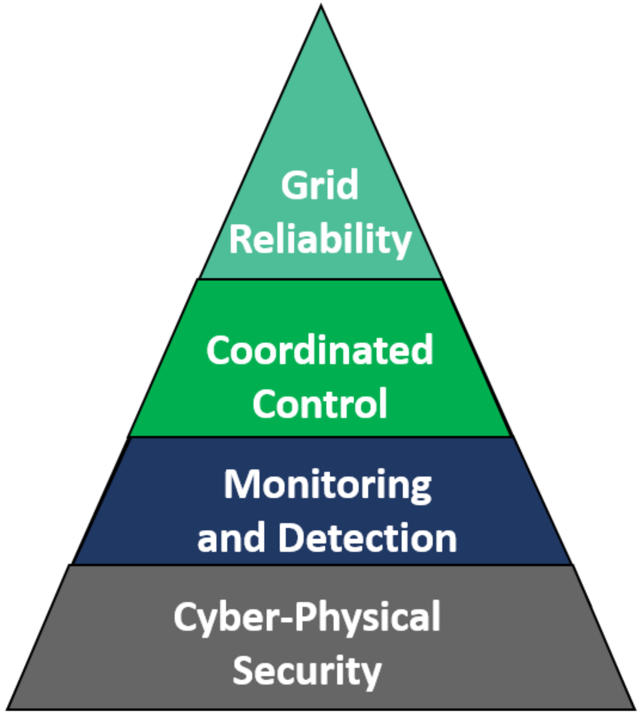
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

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.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Grid Resilience is a Cyber-Physical Problem!

The system is complicated.

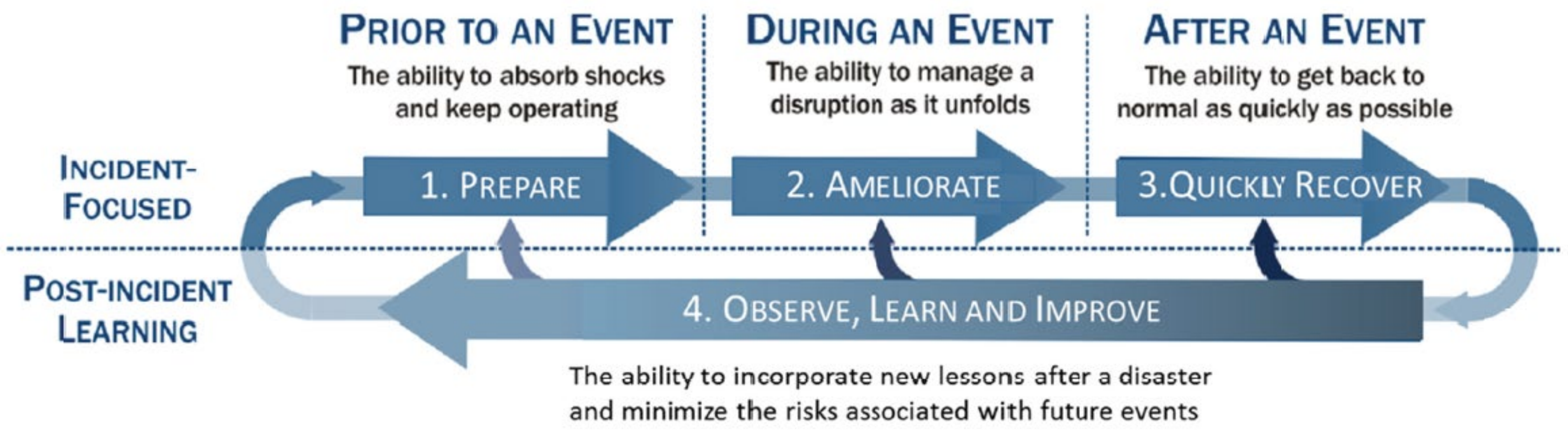
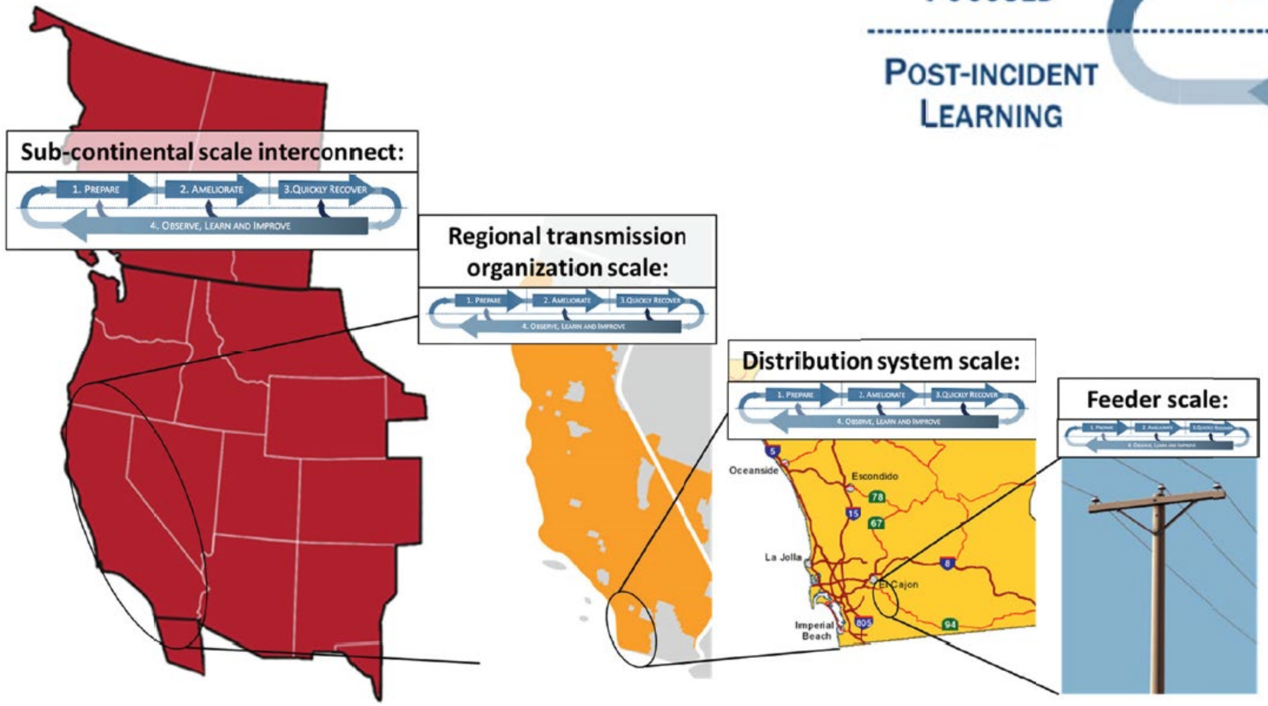


Fig. 1.2 (A), p. 36



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

Fig. 1.2 (C), p. 36

The National Academies “Enhancing the Resilience of the Nation’s Electricity System,” July 2017.

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

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

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

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Threat Categories

Natural

Accidental

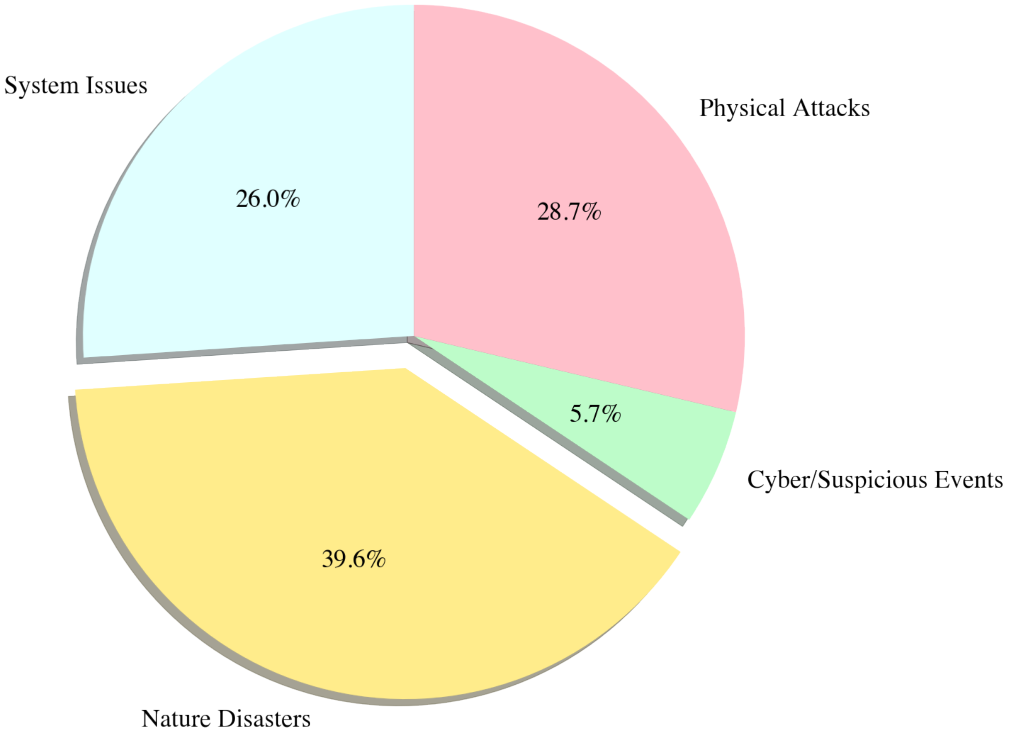
Ex. Humans on a keyboard

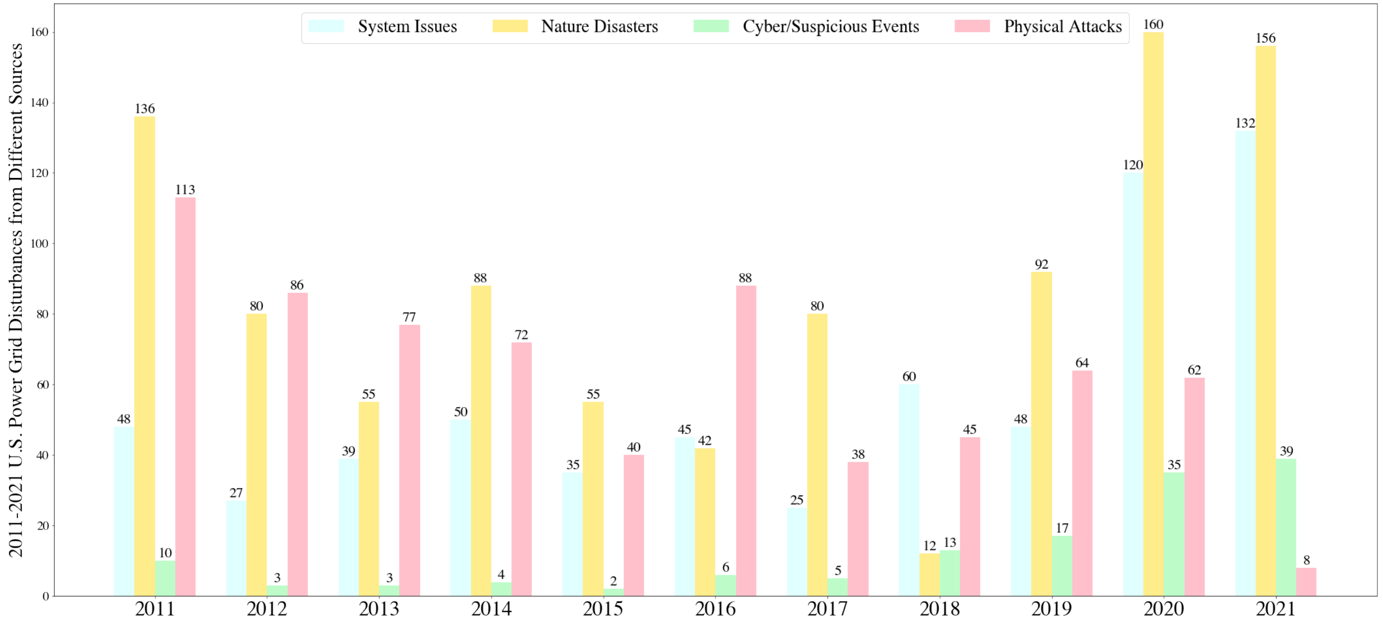
Which categories are cyber-relevant?

Intentional

TEXAS A&M UNIVERSITY
Department of Electrical
& Computer Engineering

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

Design Requirements & Challenges

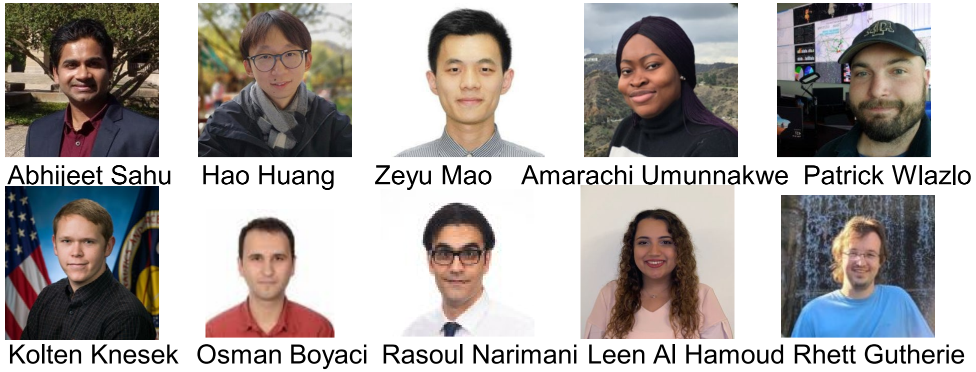
- Solutions need to be
  - Scalable
  - Automatic
  - Work for real world systems
  - Promote openess of the algorithms to understand capabilities and limitations
- **Resilient Energy Systems Lab (RESLab) Testbed**
  - Proving ground for cyber-physical control systems of the future

Texas A&M Electric Grid Control Room

Our Grid Cyber-Physical Security Research

Texas A&M's DOE CyberForce Competition team

Texas A&M Researchers showing RESLab to Students



Texas A&M Cyber-Physical Student Team and Recent Grads

- **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/

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

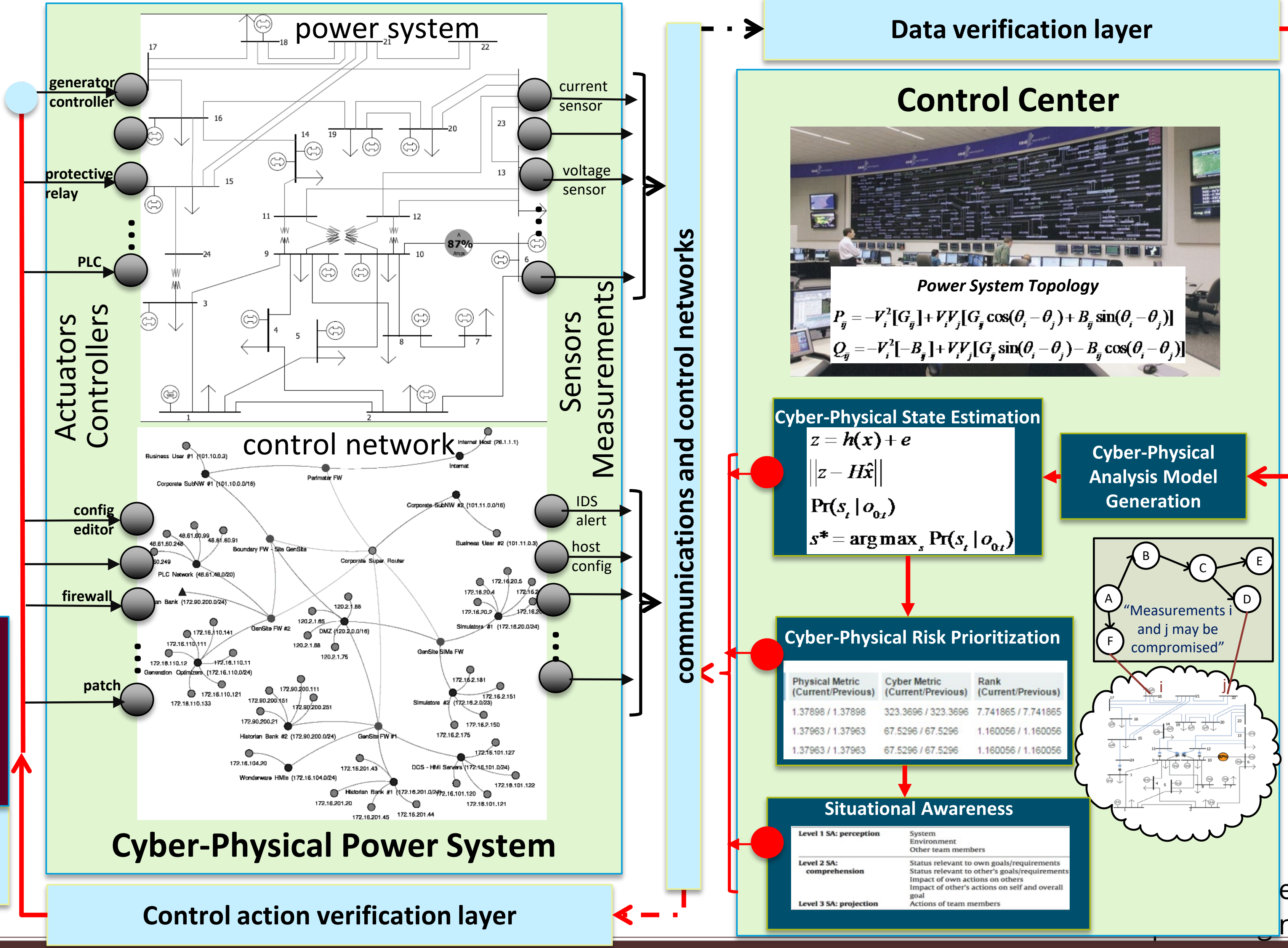
Model — Cyber-physical model

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

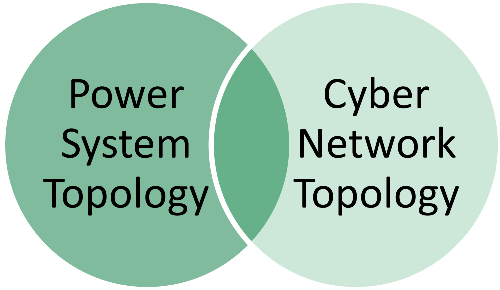
Cyber-Physical Resilient Energy Systems (CYPRES) https://cypres.engr.tamu.edu/

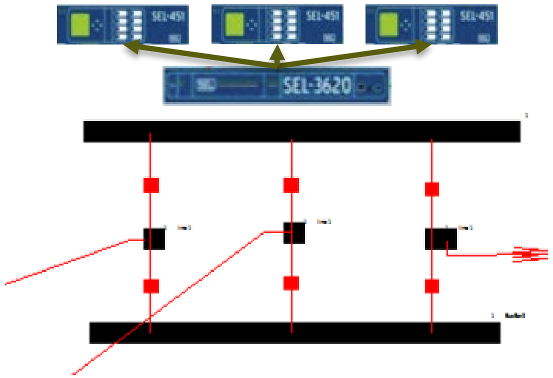


ectrical
neering

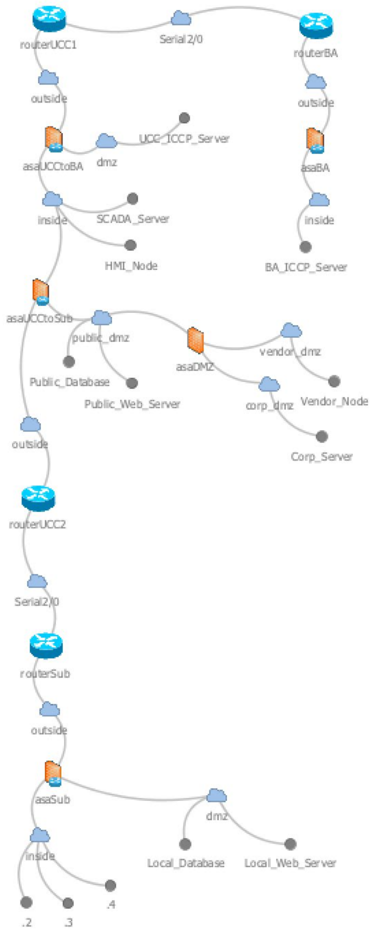
Part 1: Understand Your System

- 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



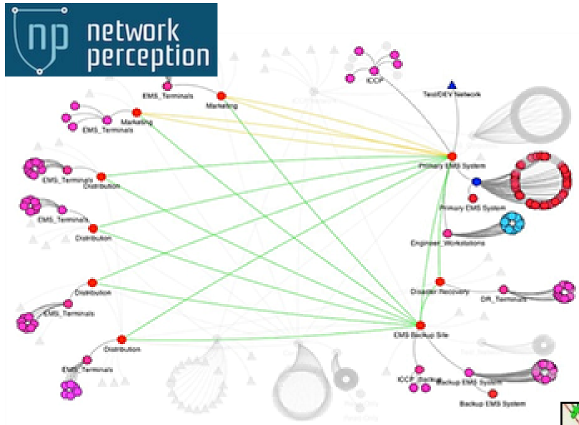
P. Wlazlo, et al, “A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid,” *IPTComm* 2019.

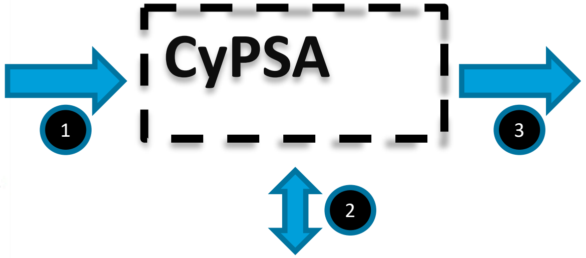
N. Gaudet, et al, “Firewall Configuration and Path Analysis for Smart Grid Networks,” *IEEE CQR* 2020.

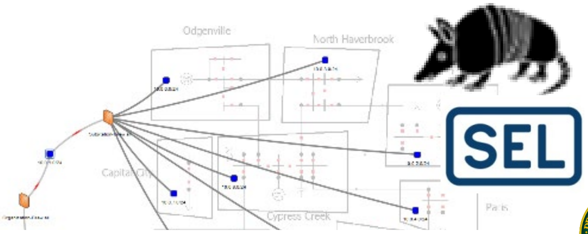
M. R. Narimani, et al, “Generalized Contingency Analysis Based on Graph Theory and Line Outage Distribution Factor,” *IEEE Systems Journal*, 2021.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

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

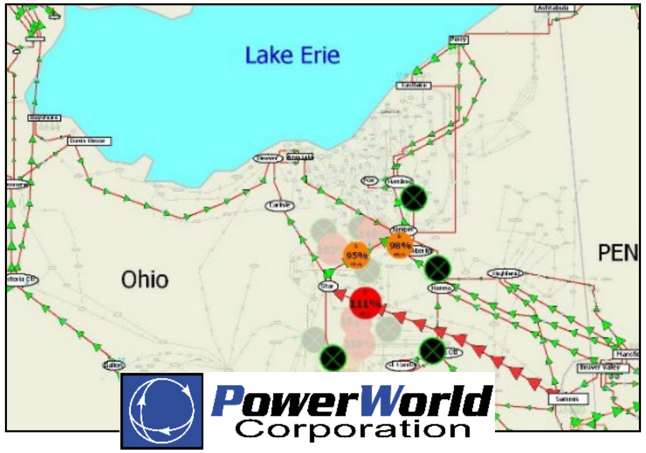






ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776
5	10.31.1.101	10.31.1.101	3.622776

Cyber-Physical Situational Awareness (CyPSA) Framework



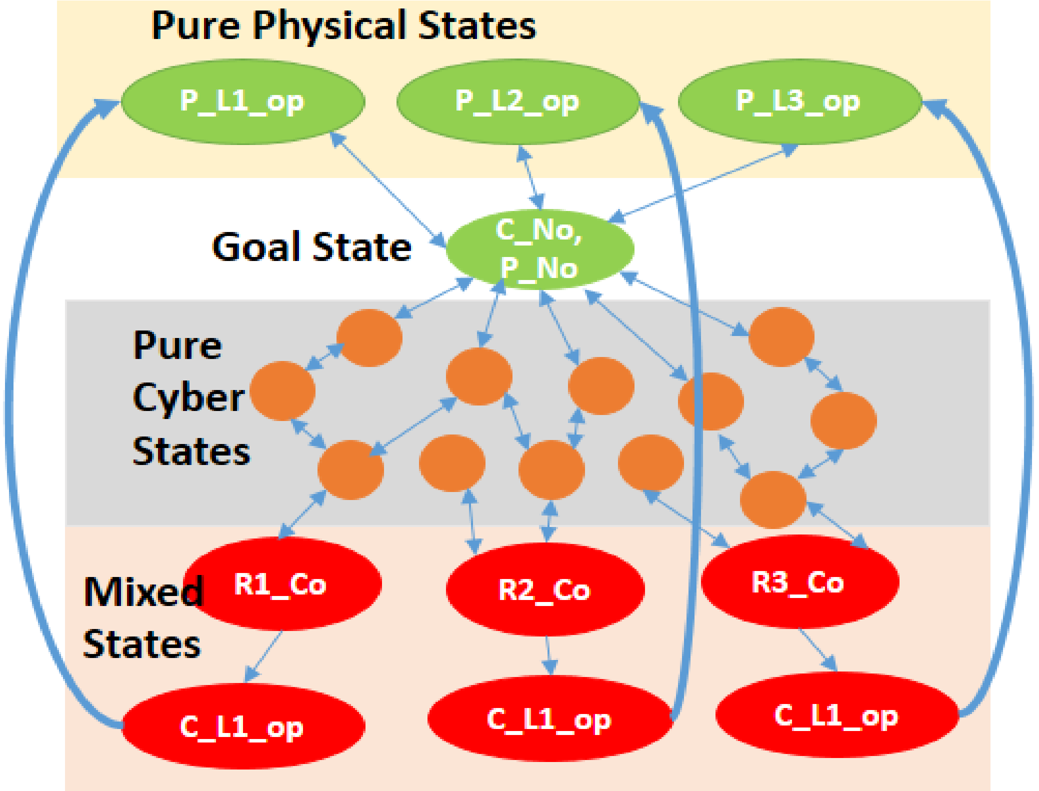
Results identify "high-risk" cyber-attack induced outages

U.S. DEPARTMENT OF ENERGY
arpa·e
ILLINOIS UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
RUTGERS UNIVERSITY
PowerWorld Corporation
Oregon State UNIVERSITY

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.

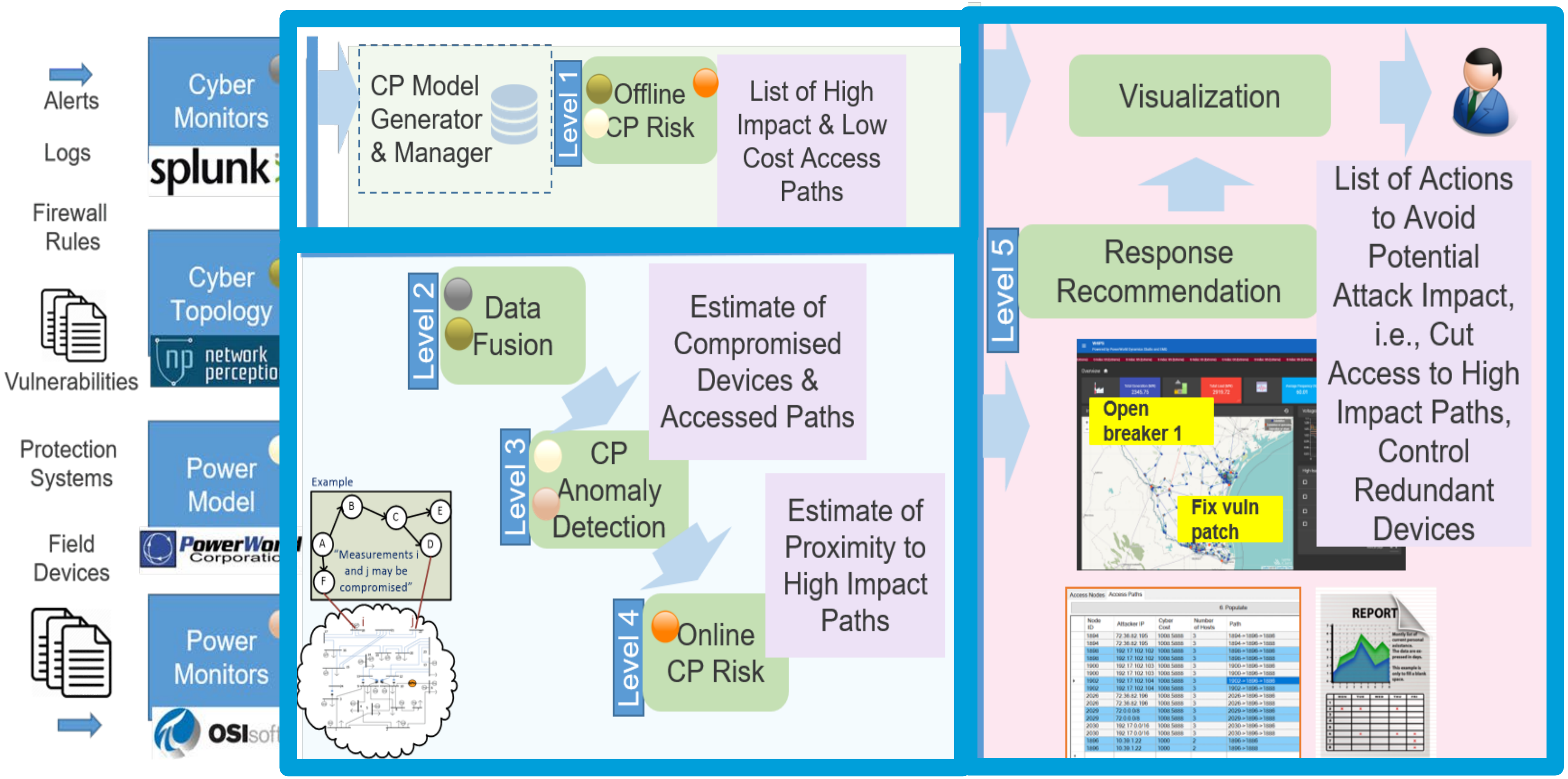
Part 3: Recommend Coordinated Cyber-Physical Response

- 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

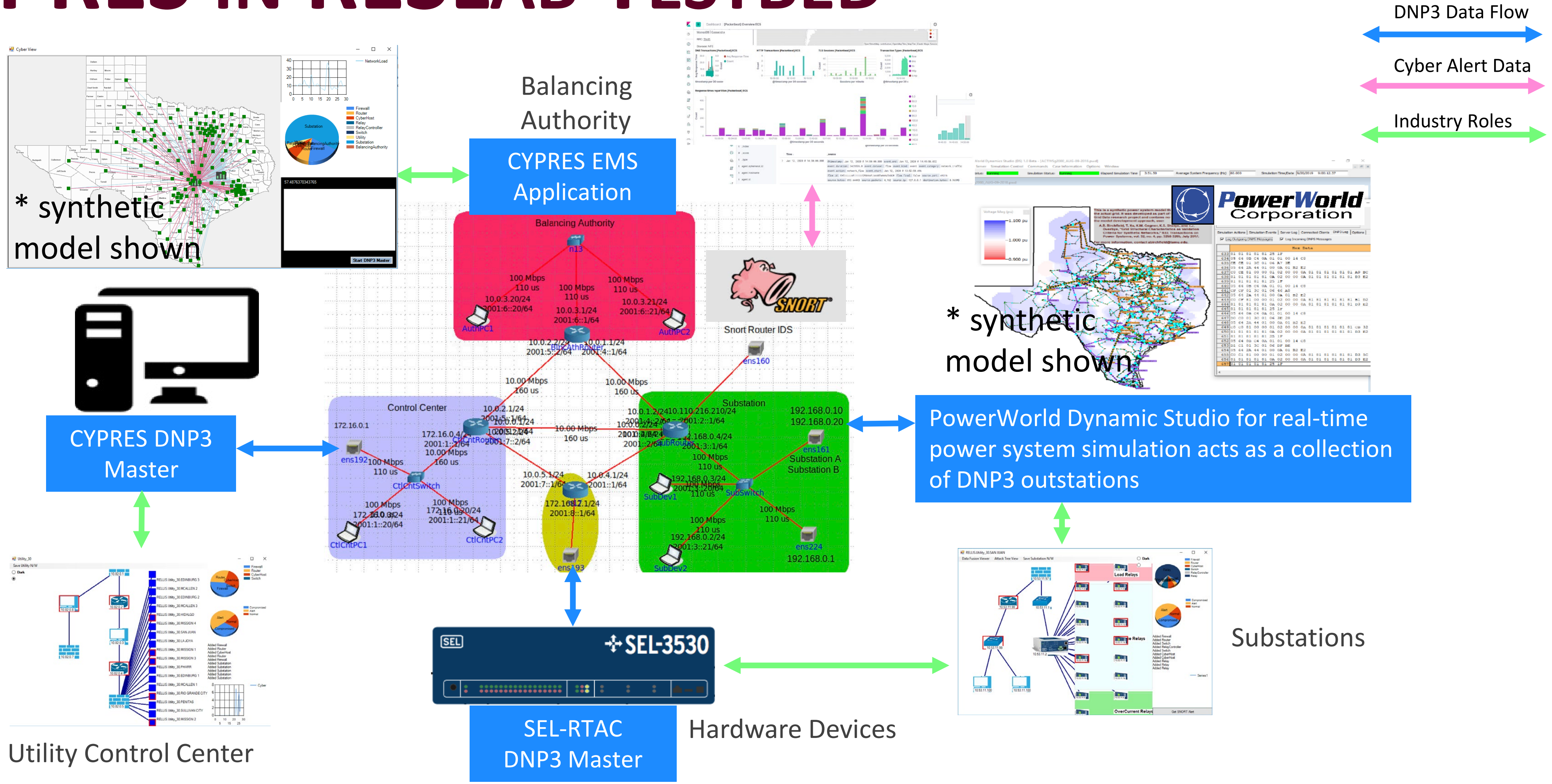


A. Sahu, et al, "SCORE: A Security-Oriented Cyber-Physical Optimal Response Engine," *IEEE SmartGridComm,* 2019.

CYPRES EMS Modeling & Workflow



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.

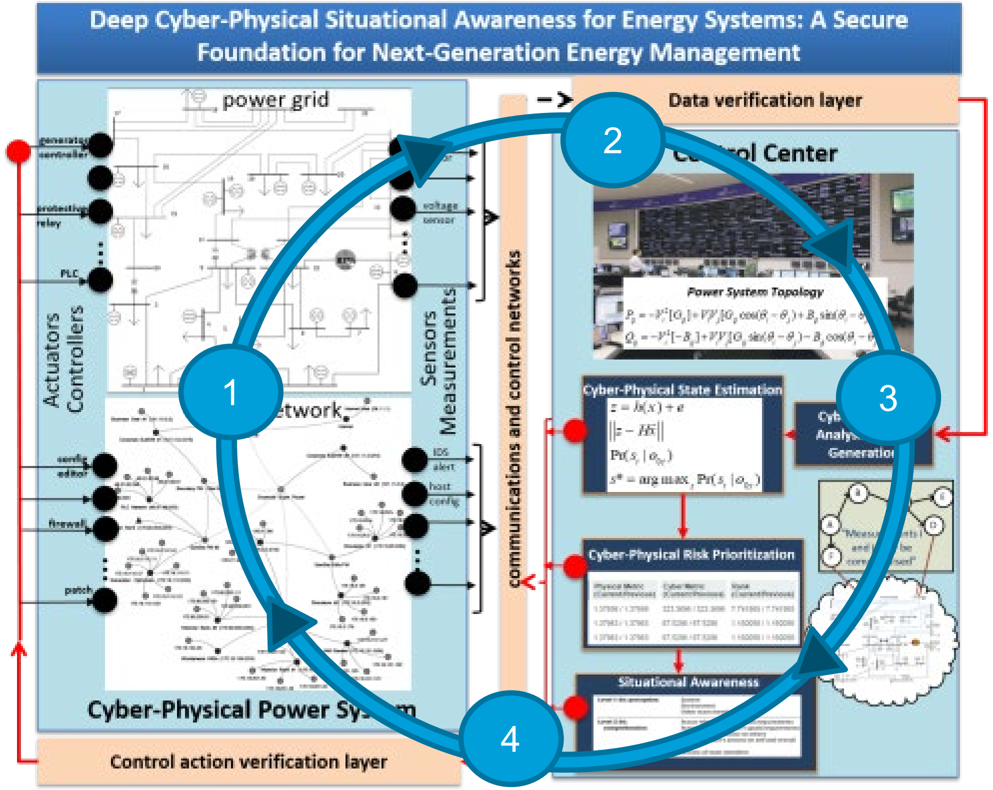
“CLOSING THE LOOP” WITH A UNIFIED MODEL

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

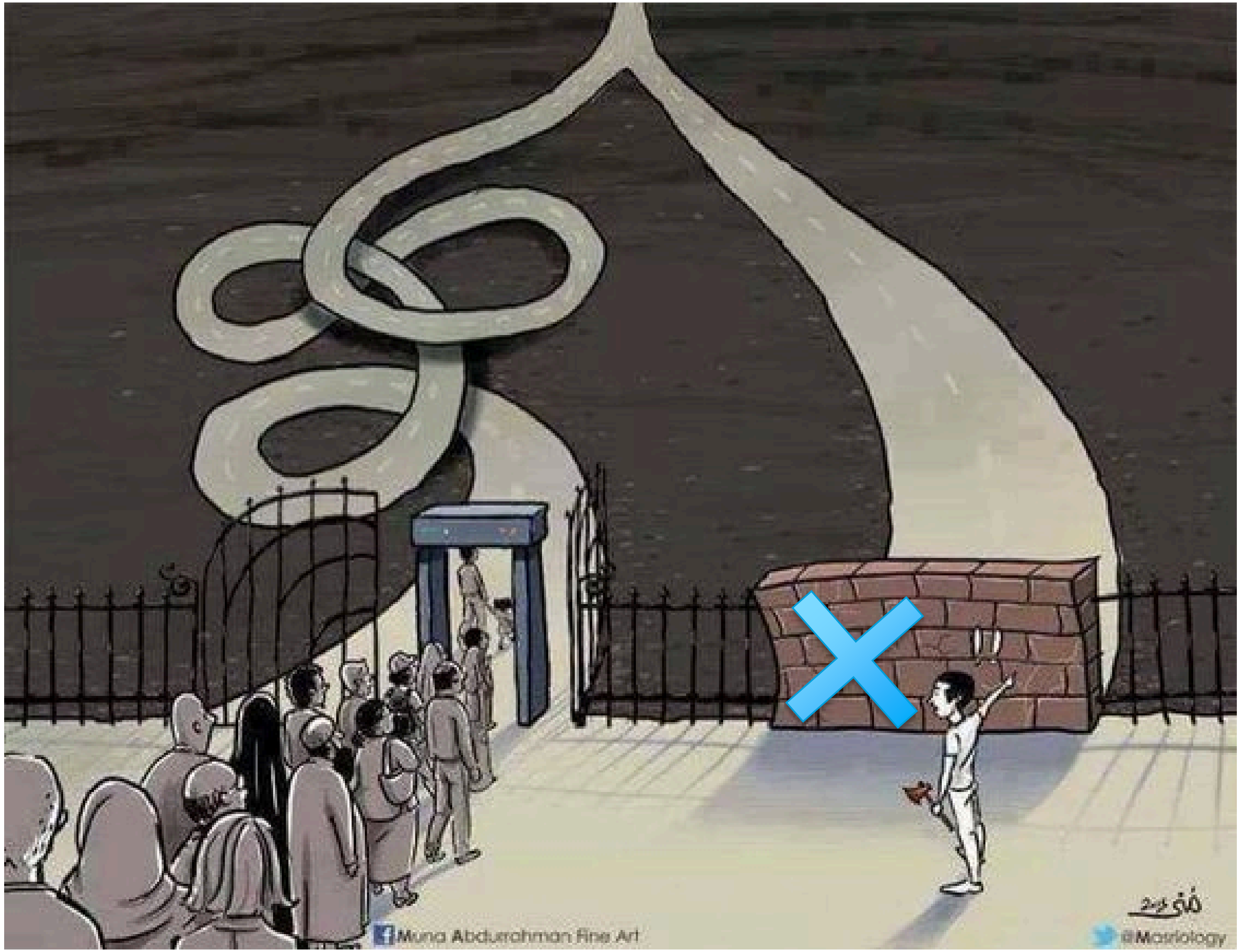
4. Verify and Control
- Recommend cyber-physical actions
- Mitigations, countermeasures



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

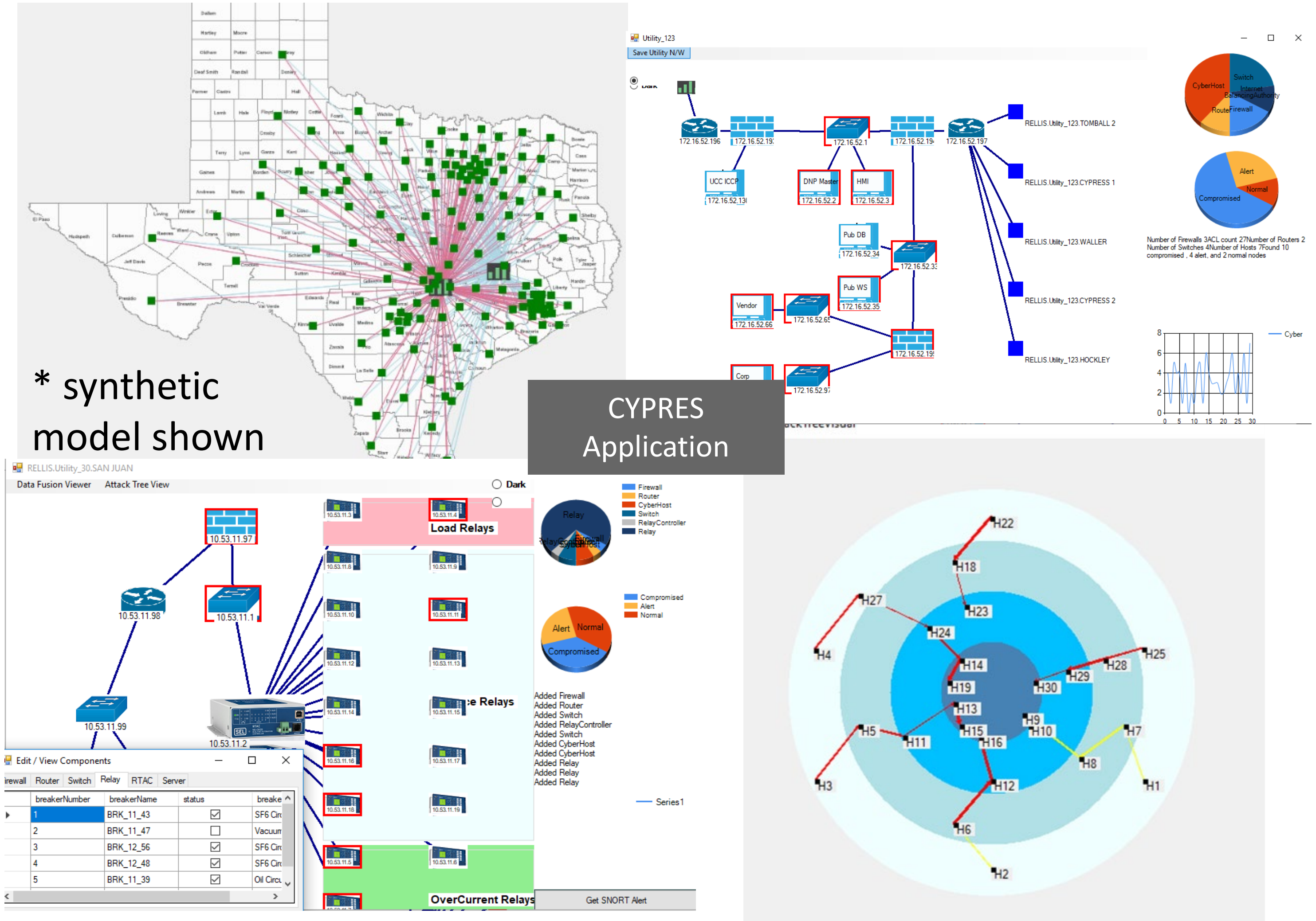
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

THE OLD WAY VS. THE NEW WAY



WHAT I TELL MY STUDENTS!

CYPRES EMS Research & Development



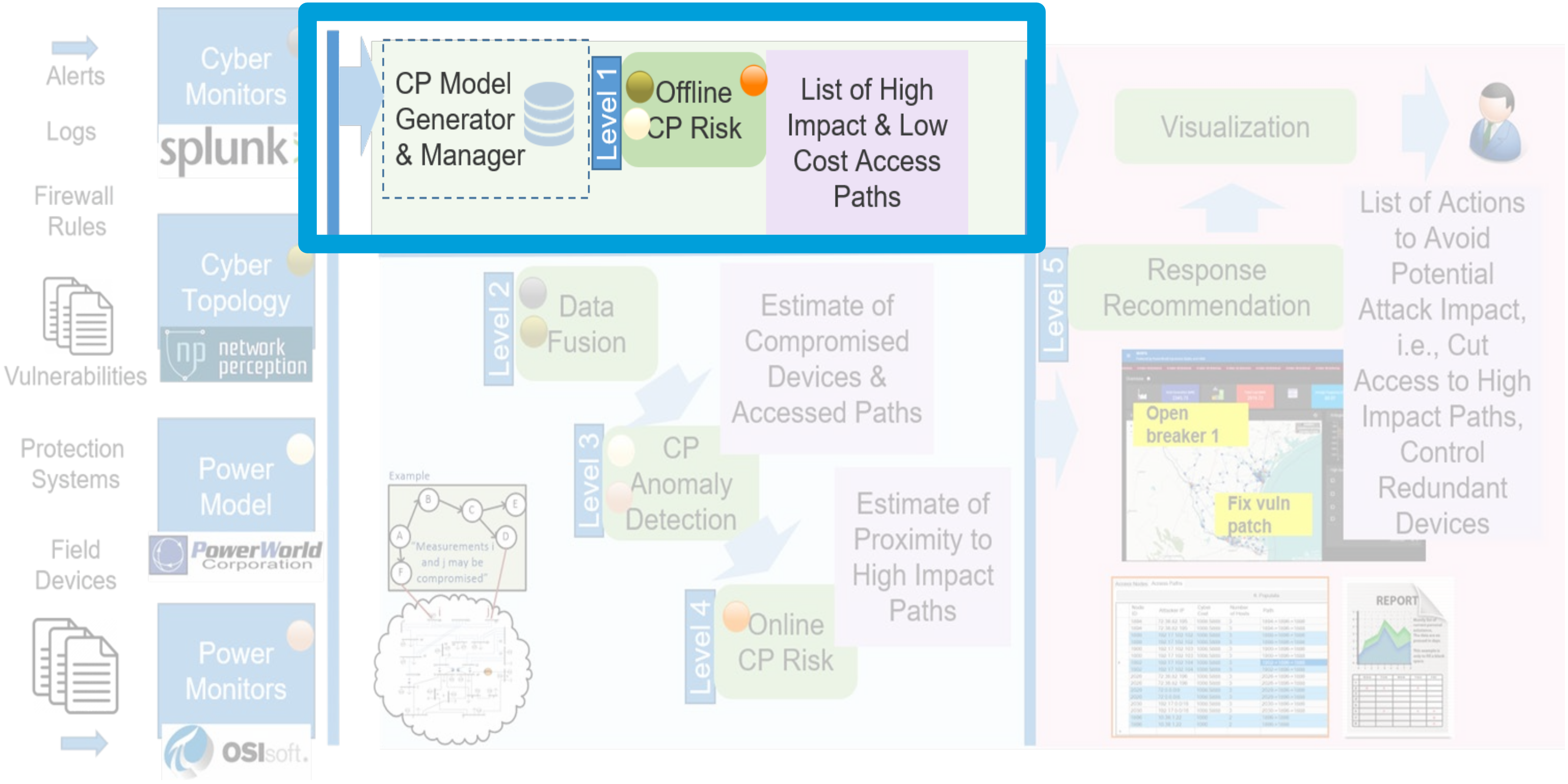
CYPRES EMS Application

- 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/

CYPRES Modeling and Workflow

Offline CPS Risk

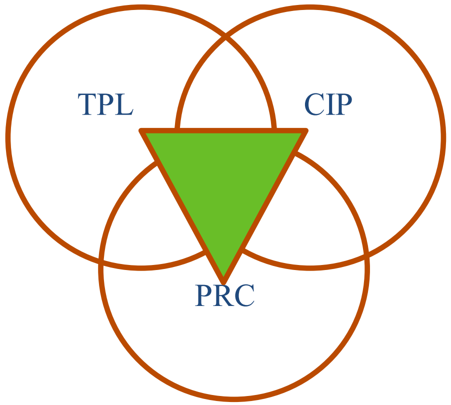


Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

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

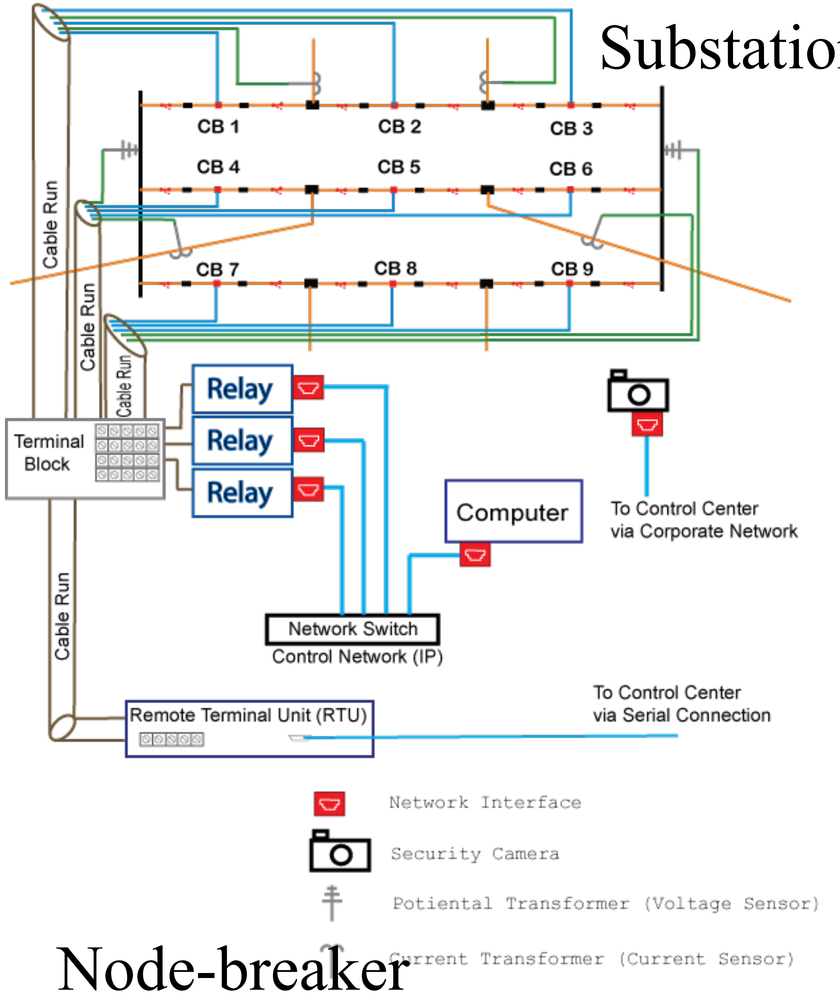


(TPL) Transmission Planning
(PRC) Protection and Control
(CIP) Critical Infrastructure Protection

Risk Assessment

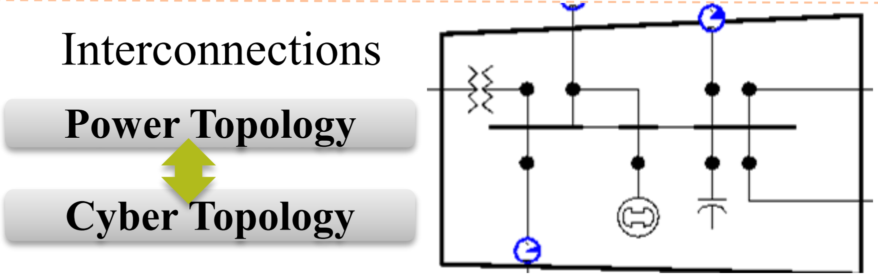
Risk = Likelihood x Impact
Likelihood = Threat x Vulnerability
Threat = Capability x Intent

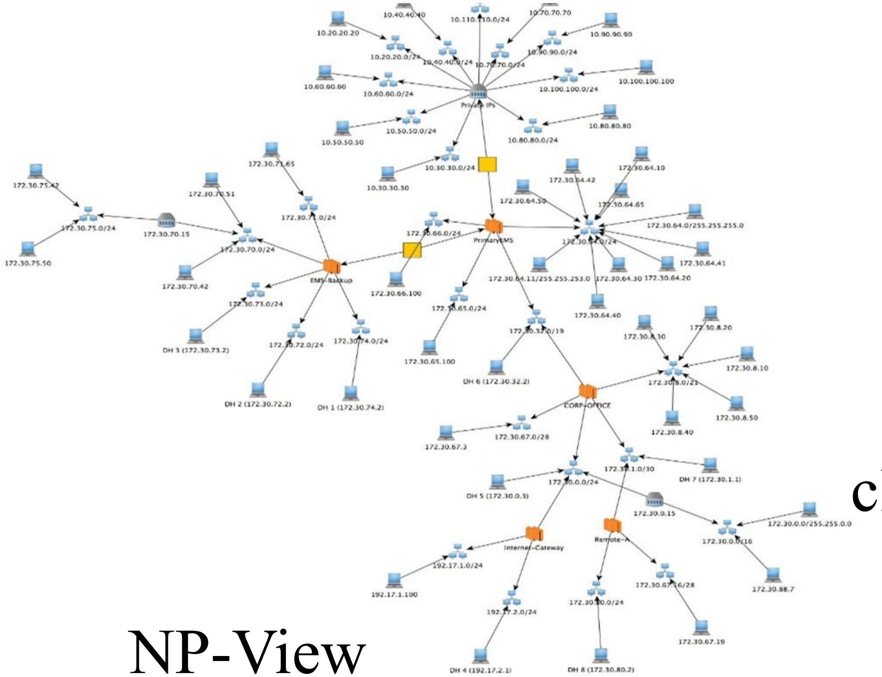
Substation



Node-breaker

Interconnections





NP-View

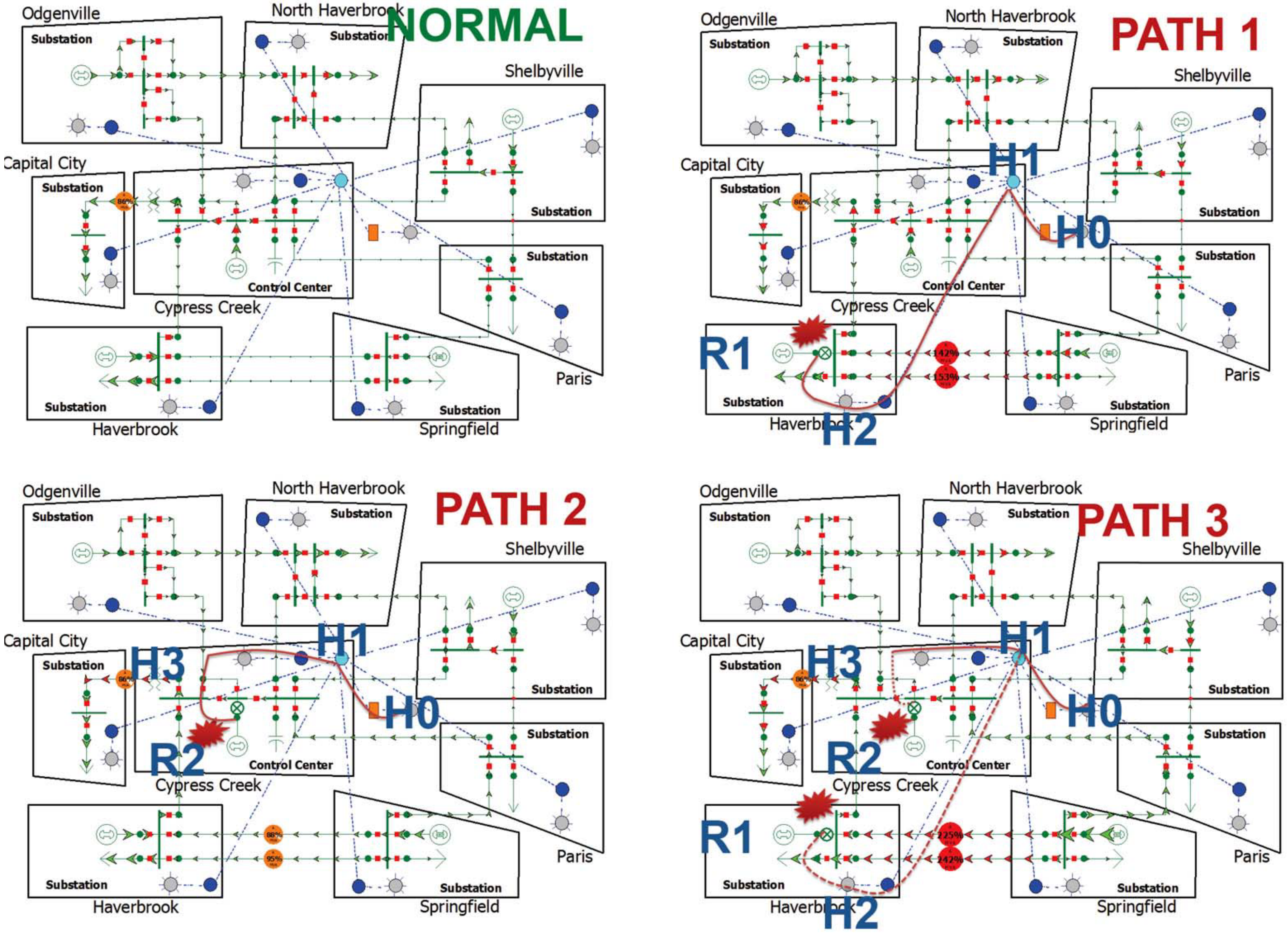
Adversary classifications

Assessing Assets: What's Really Out There?

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Model-Based CPS Risk

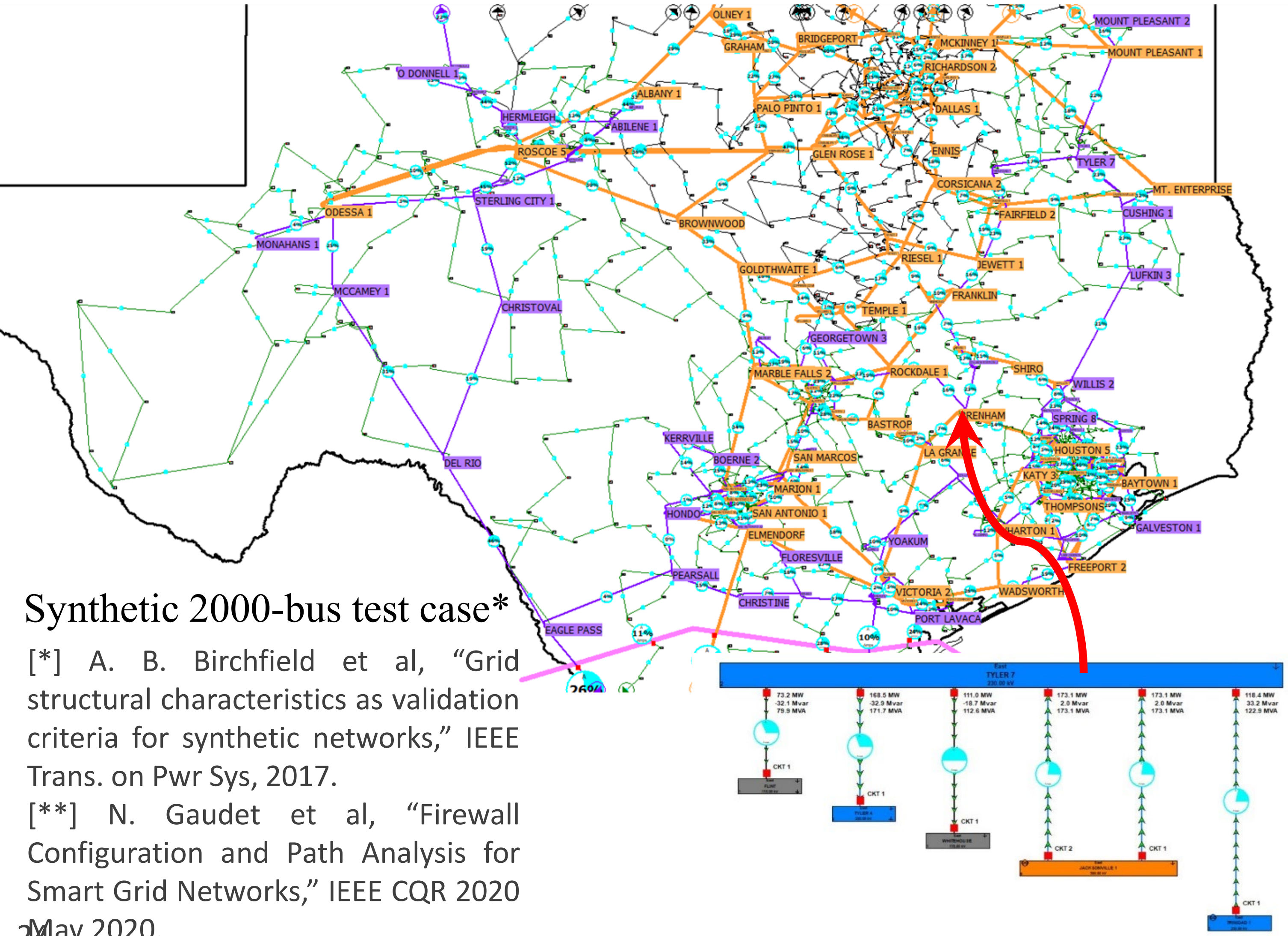
Offline CPS Risk



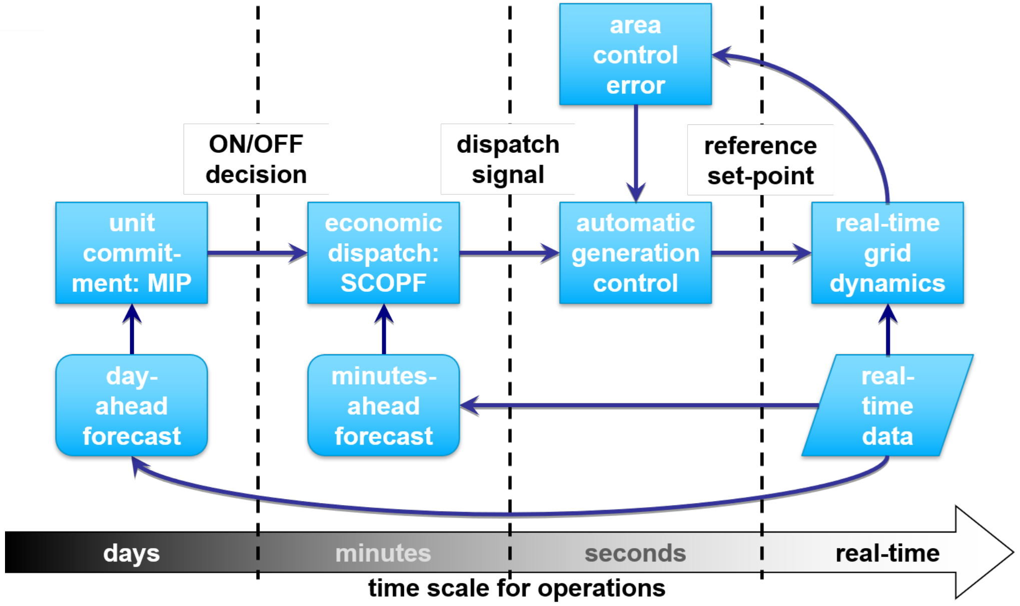
(*) K. R. Davis, et. al, “A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures,” *IEEE Transactions on in Smart Grid*, 2015.

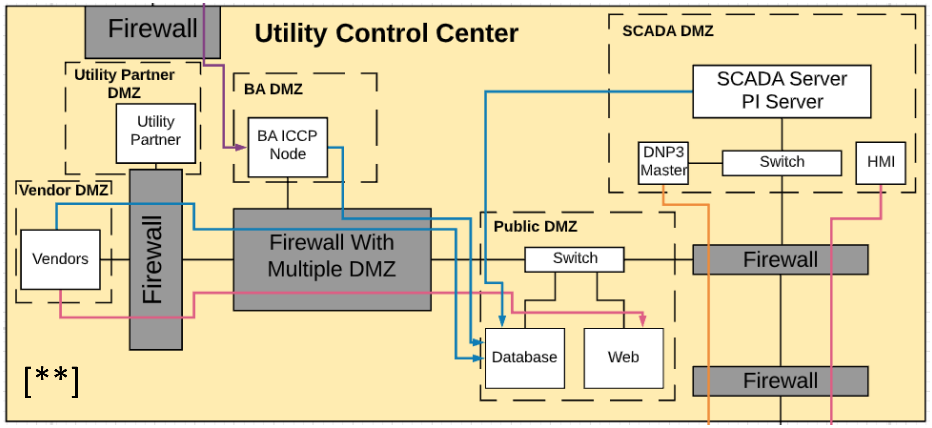
A Power System as a Cyber-Physical System

Offline CPS Risk



Synthetic 2000-bus test case*





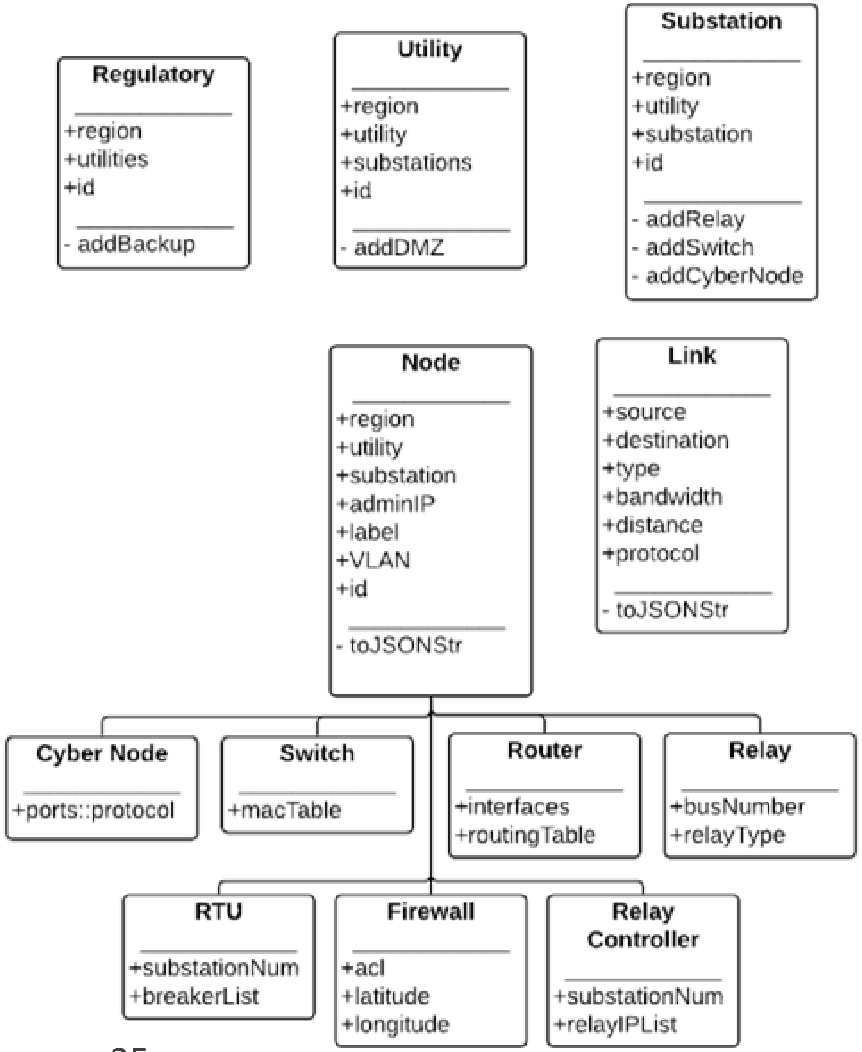
[*] A. B. Birchfield et al, "Grid structural characteristics as validation criteria for synthetic networks," IEEE Trans. on Pwr Sys, 2017.

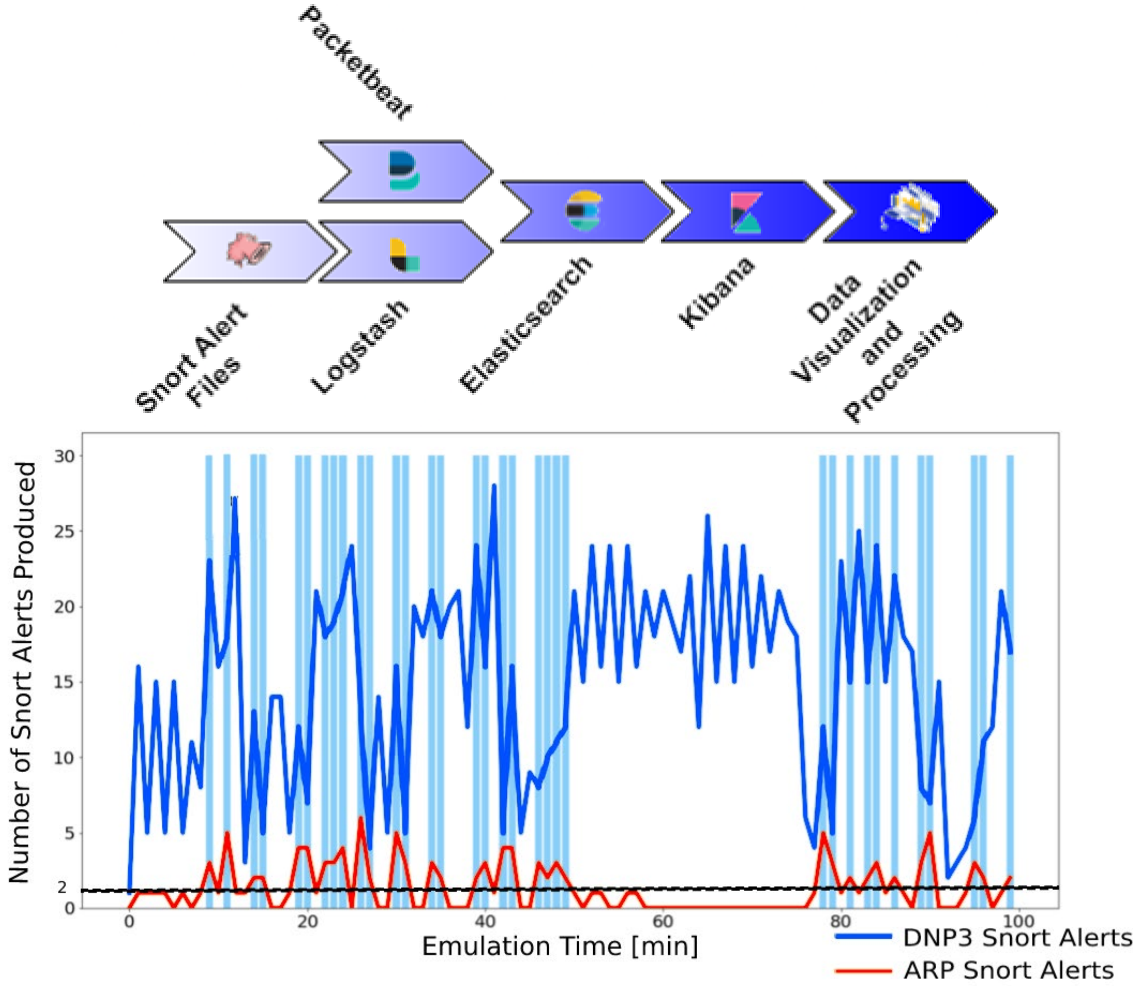
[**] N. Gaudet et al, "Firewall Configuration and Path Analysis for Smart Grid Networks," IEEE CQR 2020 May 2020.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Cyber-Physical Classes & Data Flows

Offline CPS Risk





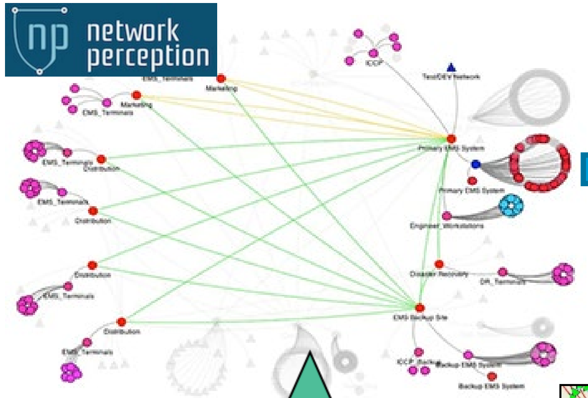
[*] P. Wlazlo, et al, "A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid," *IPTComm* 2019.

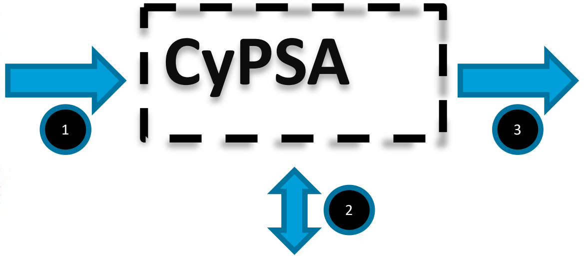
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

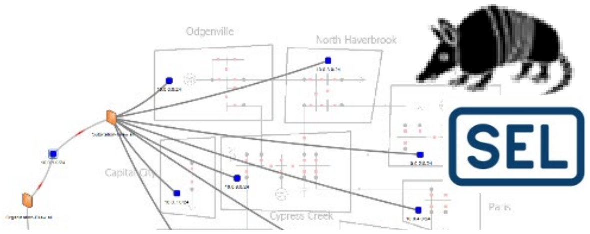
EXPANDING CPS RISK FRAMEWORK

Offline CPS Risk

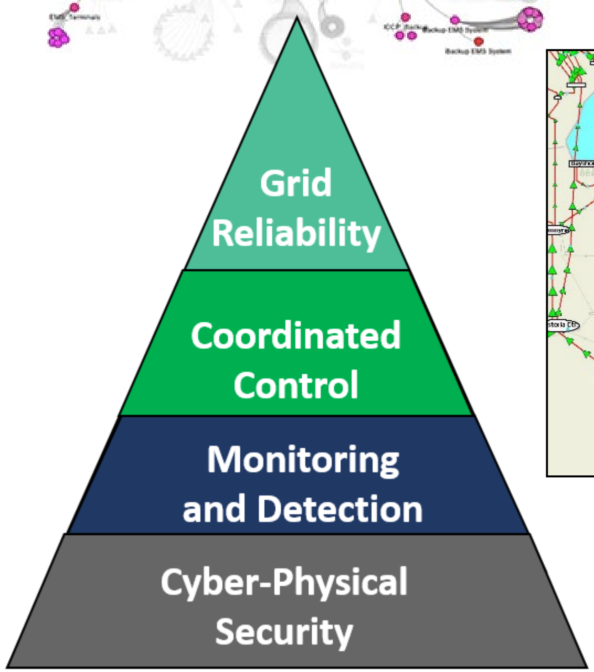
Cyber-Physical Situational Awareness (CyPSA) and its model comparisons

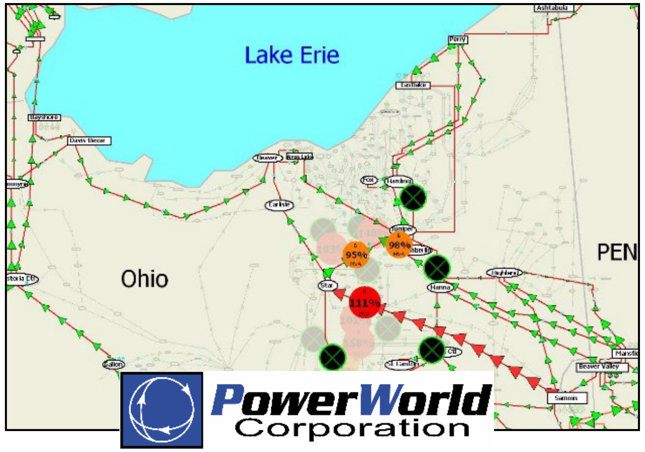






ID	Asset Name	IP Address	Rank
1	Cypress Creek-BRK-1519	10.31.1.102	3.622776
2	Cypress Creek-BRK-1925	10.31.1.103	3.622776
3	Cypress Creek-BRK-2325	10.31.1.104	3.622776
4	Cypress Creek-BRK-2225	10.31.1.105	3.622776





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

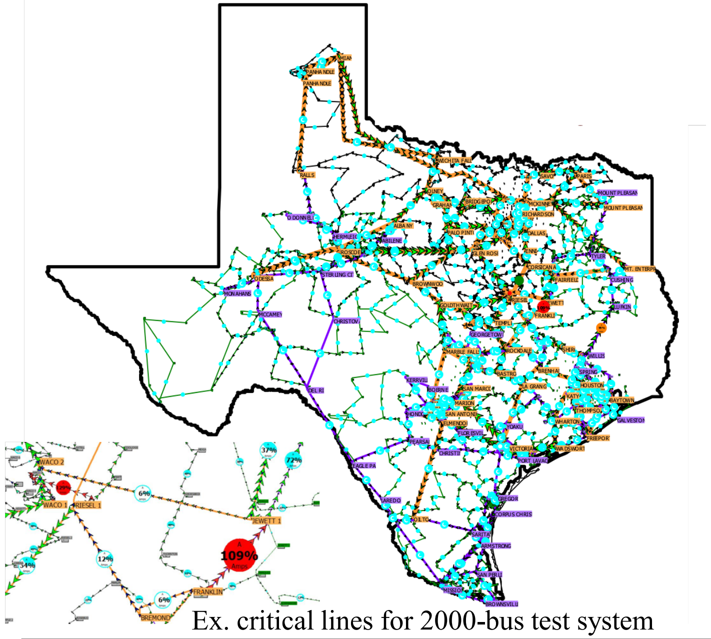
U.S. DEPARTMENT OF ENERGY
arpa-e

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.

Expanding CPS Risk Framework

Offline CPS Risk

- 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



Ex. critical lines for 2000-bus test system

x	Critical Lines	Violation Type	Number of Violations
3	[7099, 7095],[7098, 7095],[7058, 7095]	Reserve Limit	NA
4	[5262, 5260],[5263, 5260],[5317, 5260], [5358, 5179]	Overflow	4
5	[5262, 5260], [5263, 5260], [5317, 5260], [5358, 5179], [5260, 5045]	Overflow	6
6	[5362, 5260], [5363, 5260], [5317, 5260], [5358, 5179],[5260, 5045],[5179, 5380]	Overflow	6
7	[5262, 5260], [5263, 5260], [5360, 5358], [5303, 5295], [5302, 5295], [5317, 5260], [5358, 5179]	Overflow Undervoltage	5 14
8	[5262, 5260],[5263, 5260],[5360, 5358], [5303, 5295],[5302, 5295],[5317, 5260], [5358, 5179],[5260, 5045]	Overflow Undervoltage	5 14

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

A. Umunnakwe, et al, "Cyber-physical Component Ranking for Risk Sensitivity Analysis using Betweenness Centrality," *IET Cyber-Physical Systems*, 2021.

Cascading Failure Analysis in Cyber-Physical Power Systems

Offline CPS Risk

- 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***


TEXAS A&M UNIVERSITY at QATAR
SGRE22
Best Paper Award
Spatio-Temporal Failure Propagation in Cyber-Physical Power Systems
by
Osman Boyaci, M. Rasoul Narimani, Katherine Davis, Erchin Serpedin
Presented during the 3rd International Conference on Smart Grid and Renewable Energy
Doha, Qatar, 20-22 March 2022
Prof. Mariusz Malinowski
General Co-Chair
Assoc. Prof. Sertac Bayhan
General Co-Chair

$$(\forall i \in \mathcal{N},\ \forall (l,m) \in \mathcal{L})$$

$$P_i^g - P_i^d = g_{sh,i} V_i^2 + \sum_{\substack{(l,m)\in\mathcal{L},\\ \text{s.t. } l=i}} P_{lm} + \sum_{\substack{(l,m)\in\mathcal{L},\\ \text{s.t. } m=i}} P_{ml},$$

$$Q_i^g - Q_i^d = -b_{sh,i} V_i^2 + \sum_{\substack{(l,m)\in\mathcal{L},\\ \text{s.t. } l=i}} Q_{lm} + \sum_{\substack{(l,m)\in\mathcal{L},\\ \text{s.t. } m=i}} Q_{ml},$$

$$P_{lm} = g_{lm} V_l^2 - g_{lm} V_l V_m \cos(\theta_{lm}) - b_{lm} V_l V_m \sin(\theta_{lm}),$$

$$Q_{lm} = -(b_{lm} + b_{c,lm}/2) V_l^2 + b_{lm} V_l V_m \cos(\theta_{lm}) - g_{lm} V_l V_m \sin(\theta_{lm}),$$

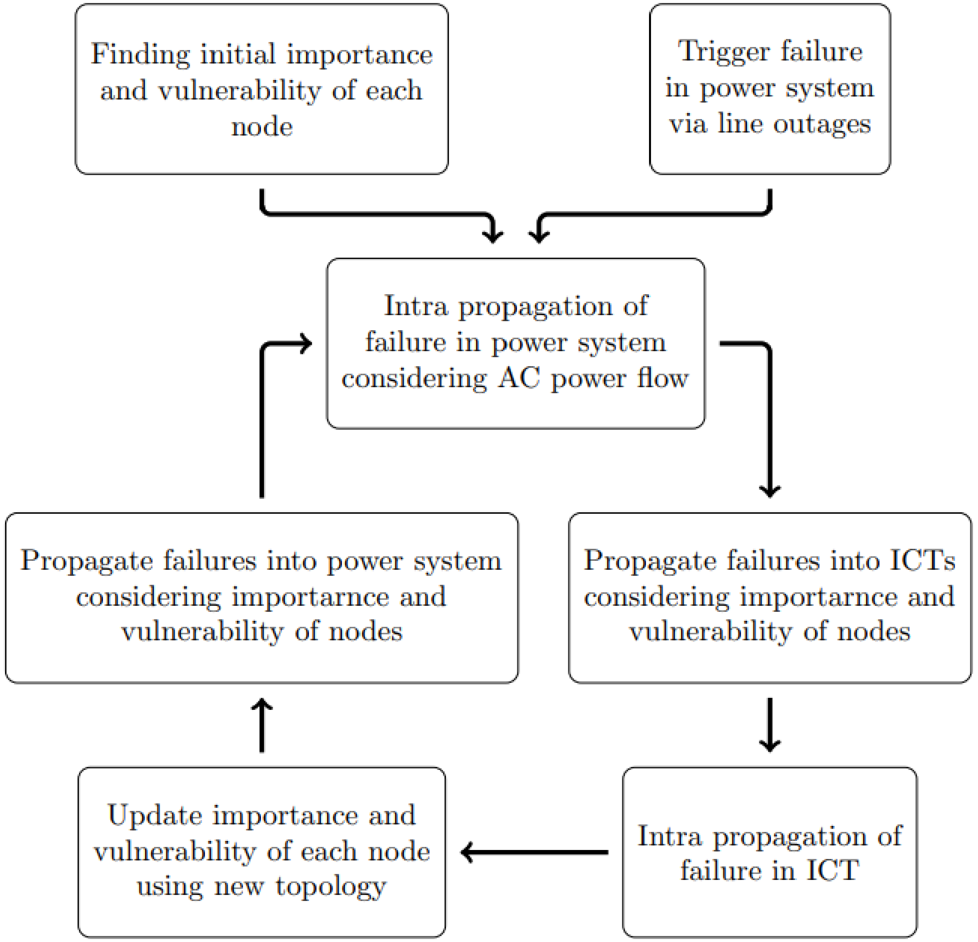
$$P_{ml} = g_{lm} V_m^2 - g_{lm} V_l V_m \cos(\theta_{lm}) + b_{lm} V_l V_m \sin(\theta_{lm}),$$

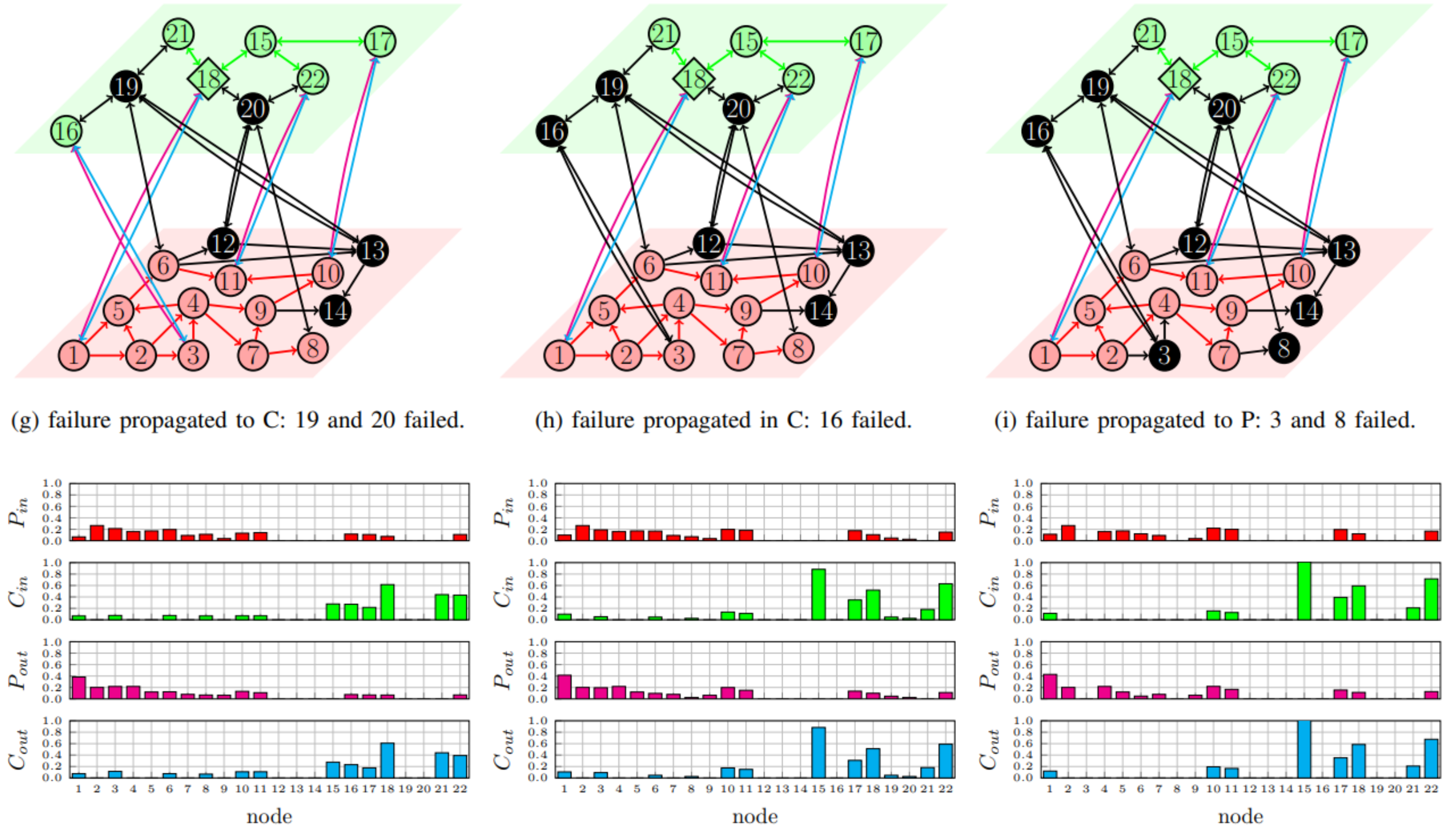
$$Q_{ml} = -(b_{lm} + b_{c,lm}/2) V_m^2 + b_{lm} V_l V_m \cos(\theta_{lm}) + g_{lm} V_l V_m \sin(\theta_{lm}).$$

O. Boyaci, M. R. Narimani, K. Davis, and E. Serpedin, “Spatio-Temporal Failure Propagation in Cyber-Physical Power Systems,” *3rd International Conference on Smart Grid and Renewable Energy (SGRE) 2022 (Best Paper Award)*

FAILURE PROPAGATION ANALYSIS

Offline CPS Risk





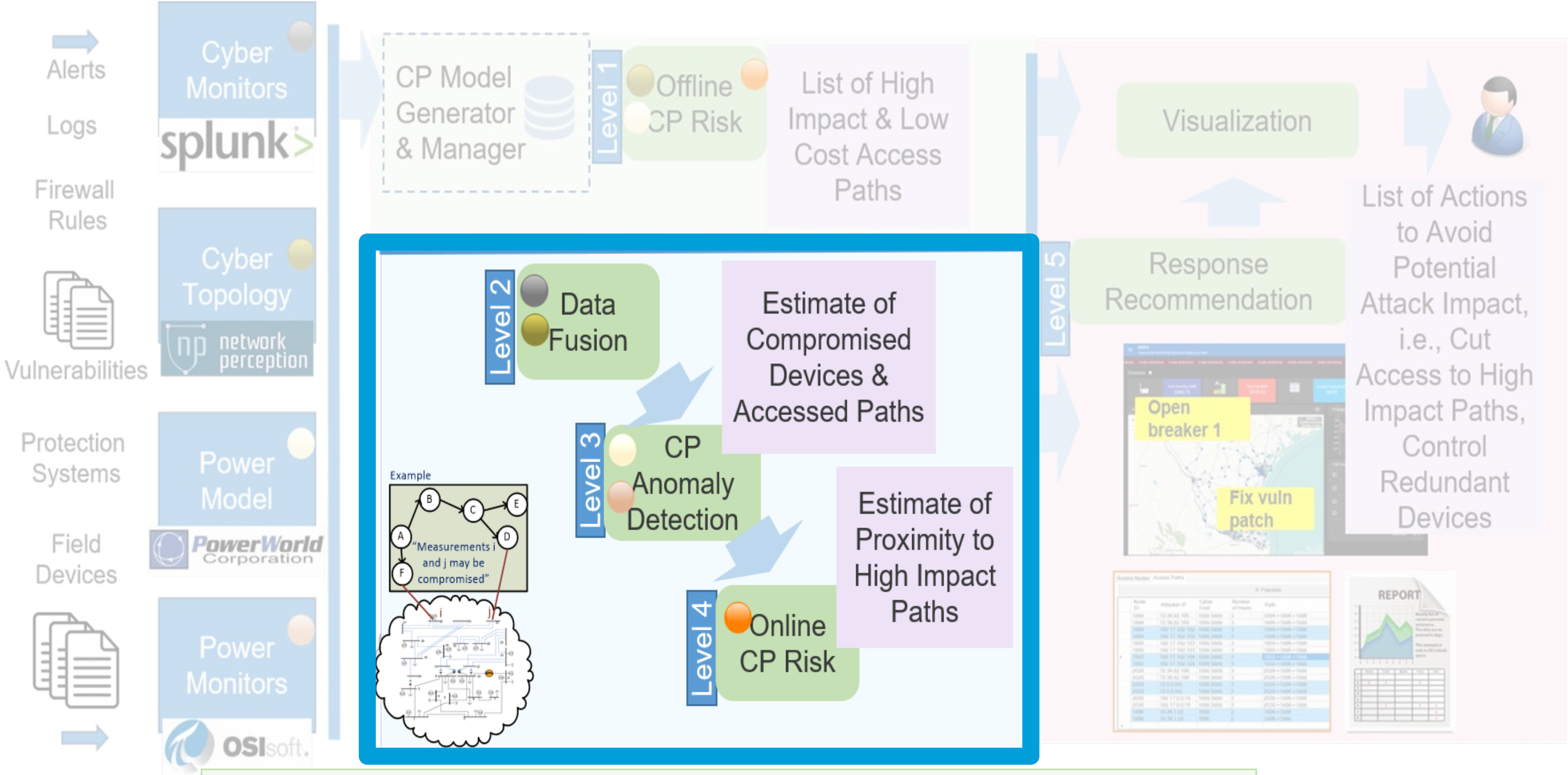
(g) failure propagated to C: 19 and 20 failed.
(h) failure propagated in C: 16 failed.
(i) failure propagated to P: 3 and 8 failed.

(j) metrics after failure propagated to C.
(k) metrics after failure propagated in C.
(l) metrics after failure propagated to P.

O. Boyaci, M. R. Narimani, K. Davis, and E. Serpedin, "Spatio-Temporal Failure Propagation in Cyber-Physical Power Systems," *3rd International Conference on Smart Grid and Renewable Energy (SGRE) 2022 (Best Paper Award)*

CYPRES Modeling & Workflow

Online CPS Risk

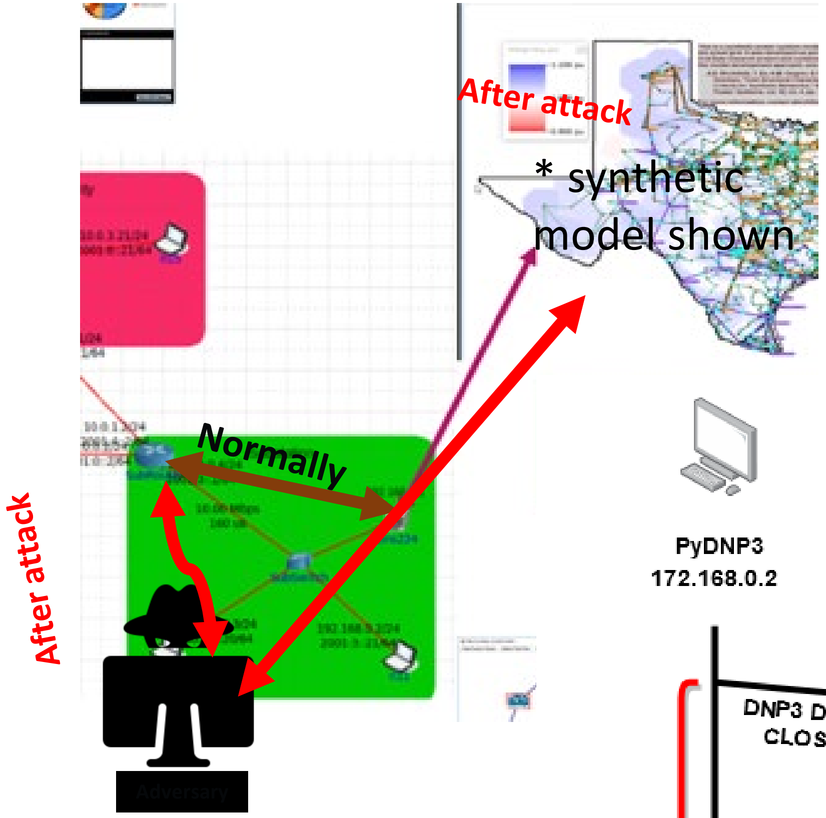


Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

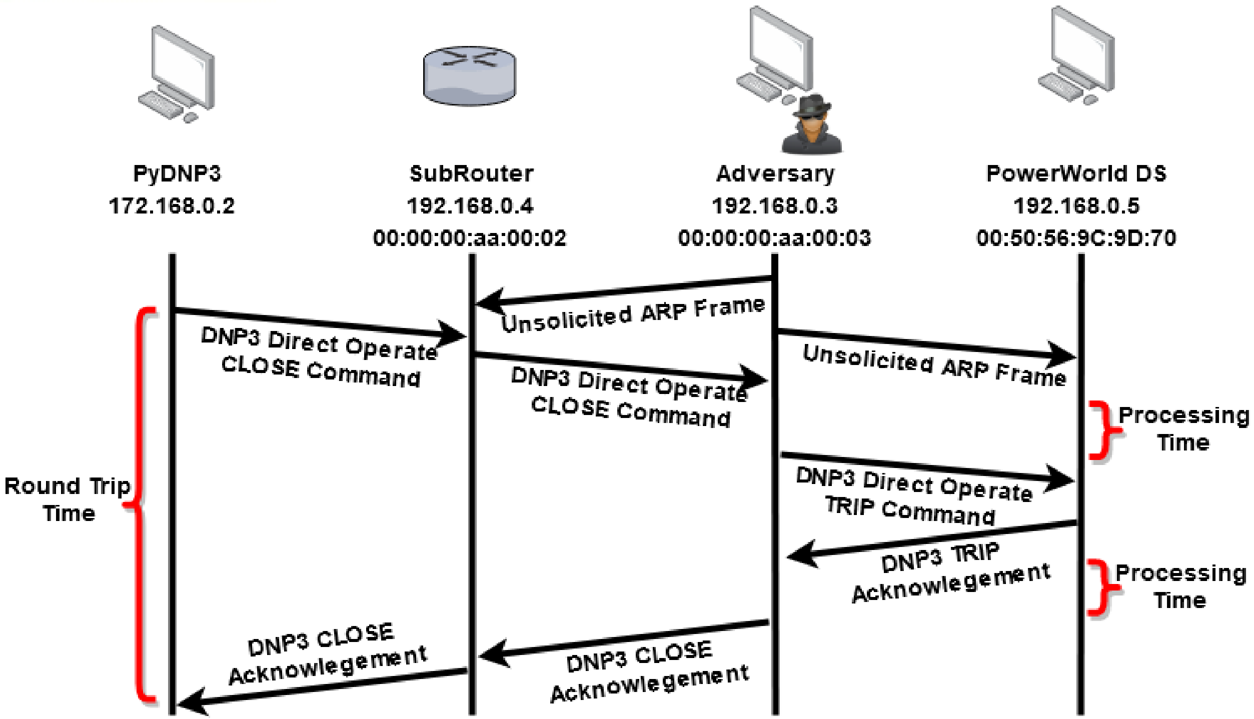
Intrusion and Detection in the Loop

Online CPS Risk



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.

Contact us for a live demo (virtual) in our testbed

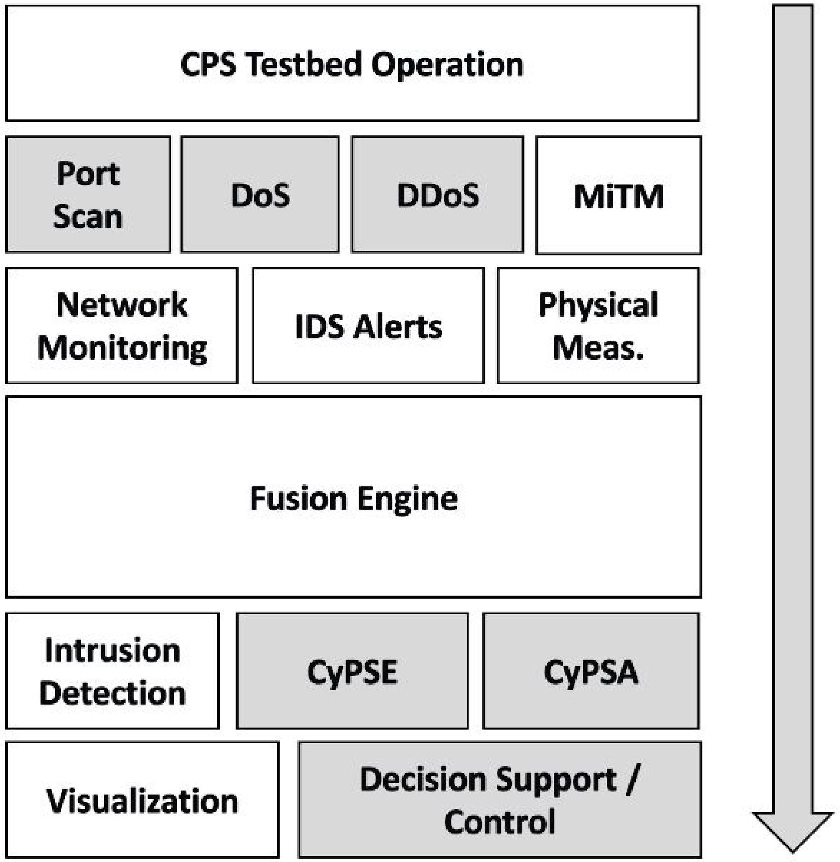
INFERENCE USING ONLINE DATA

- 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

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

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

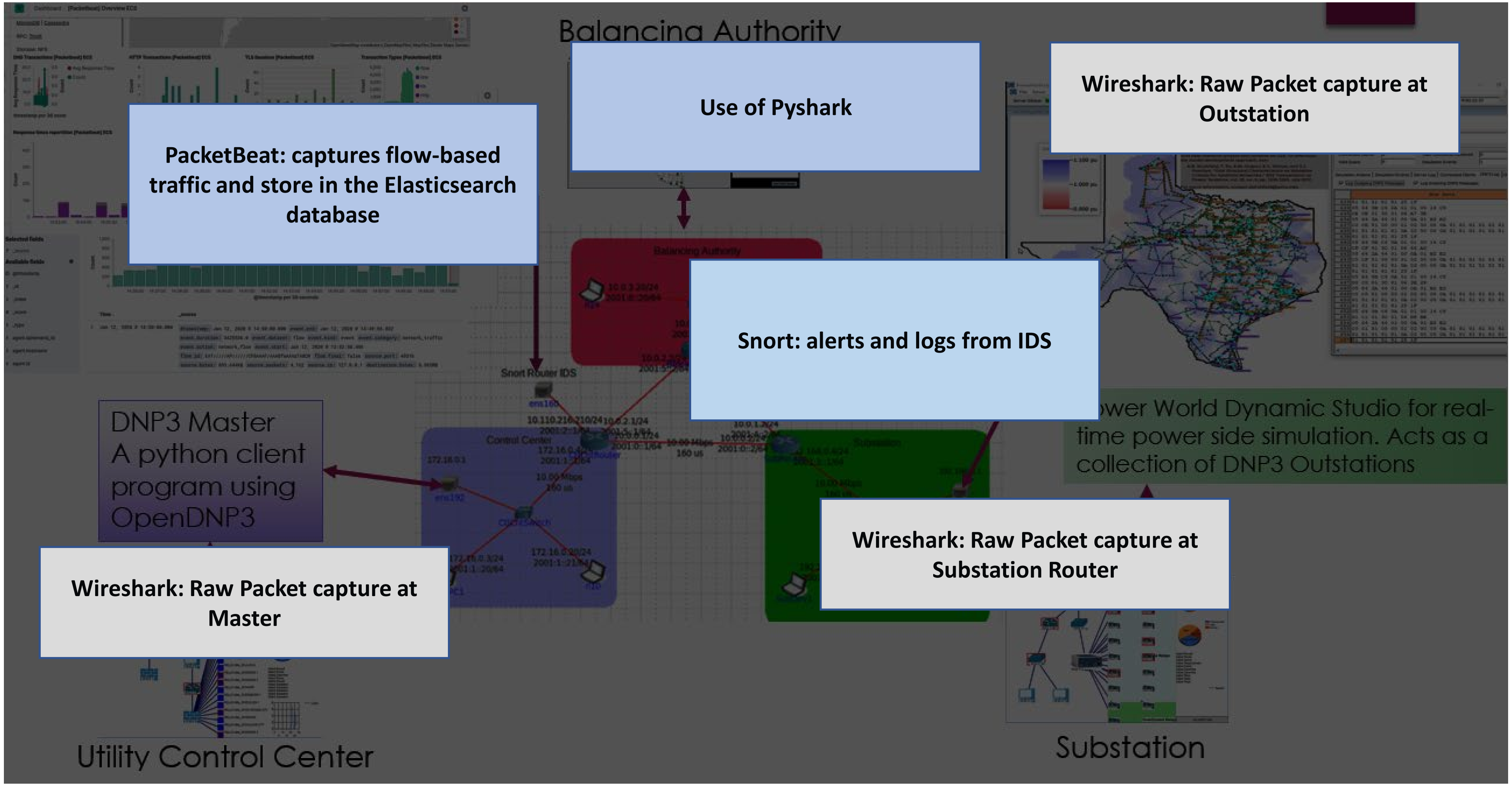


A. Sahu, et al. "Multi-Source Data Fusion for Cyberattack Detection in Power Systems." *IEEE Access*, 2021.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

DATA SOURCES

Online CPS Risk



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

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

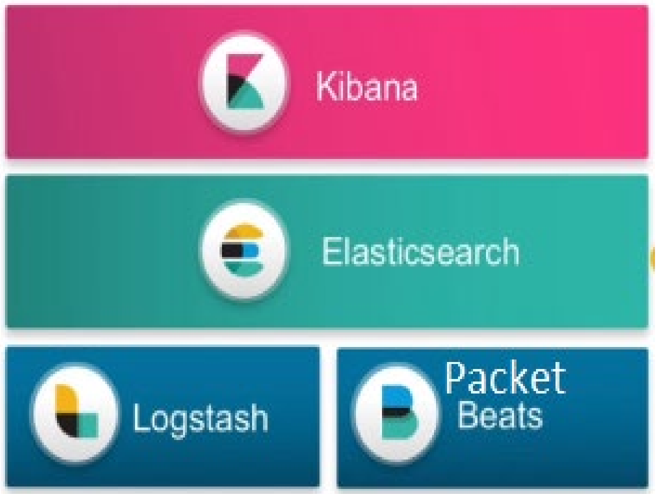
Processing
- Imputation of missing values
- Encoding of categorical features
- Visualization of merged features
- Feature reduction with PCA

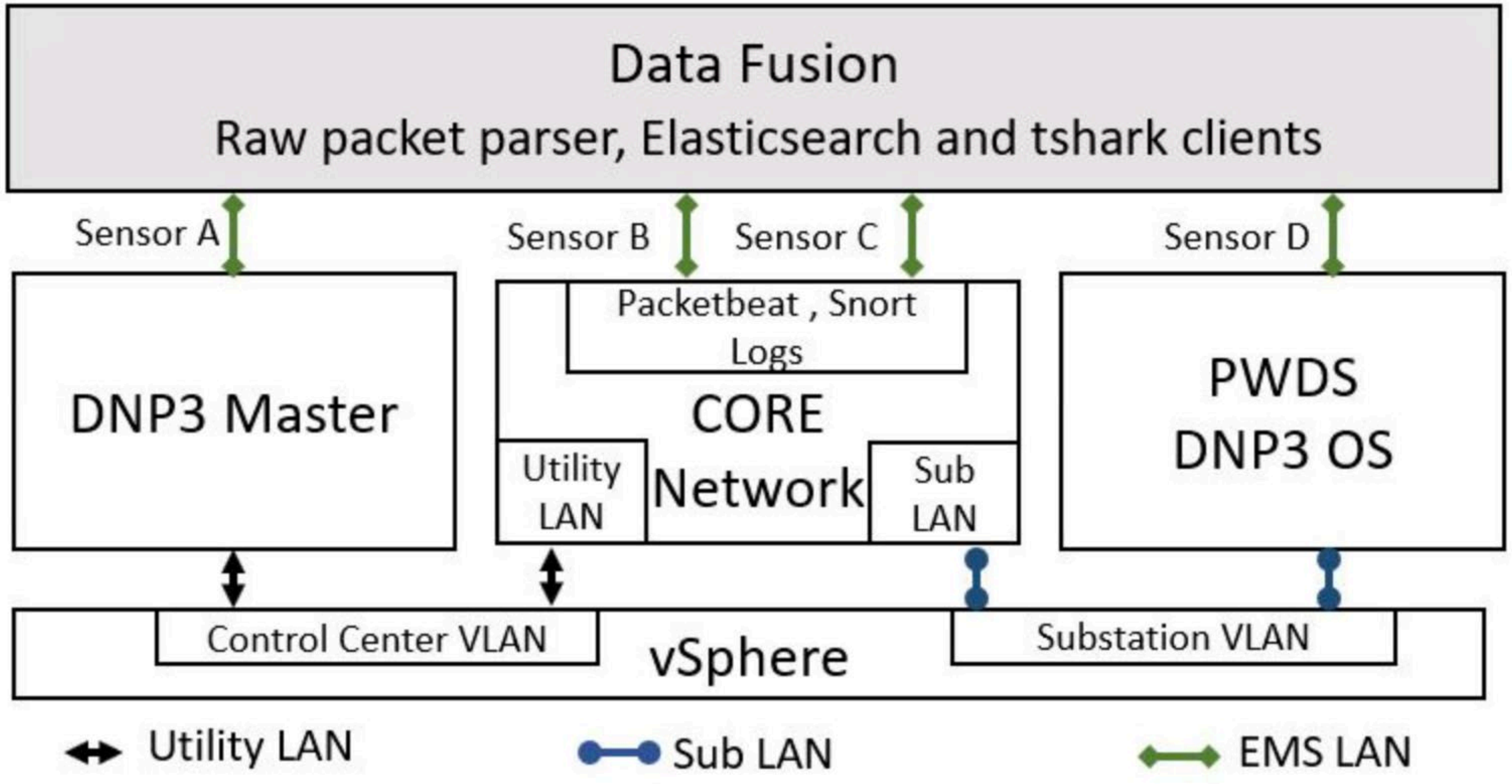
Detection
- Supervised Learning:
  - SVM, Naïve Bayes, RF, DT and MLP
- Semi-Supervised Learning:
  - Co-Training

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

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

Fusion Engine Paper & Dataset





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

Dataset: https://ieee-dataport.org/documents/cyber-physical-dataset-mitm-attacks-power-systems

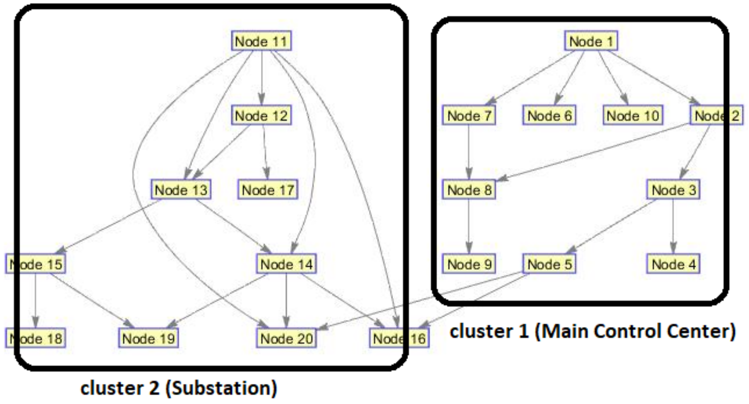
Estimating Cyber Physical State - Data Fusion Lab (Try on your own!)

- 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:

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

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



Comparisons of time and accuracy for learning the Bayesian Attack Graphs

Comparative study of learning techniques based on Scale, Data Dependency, Avg. Computation Time, and Accuracy

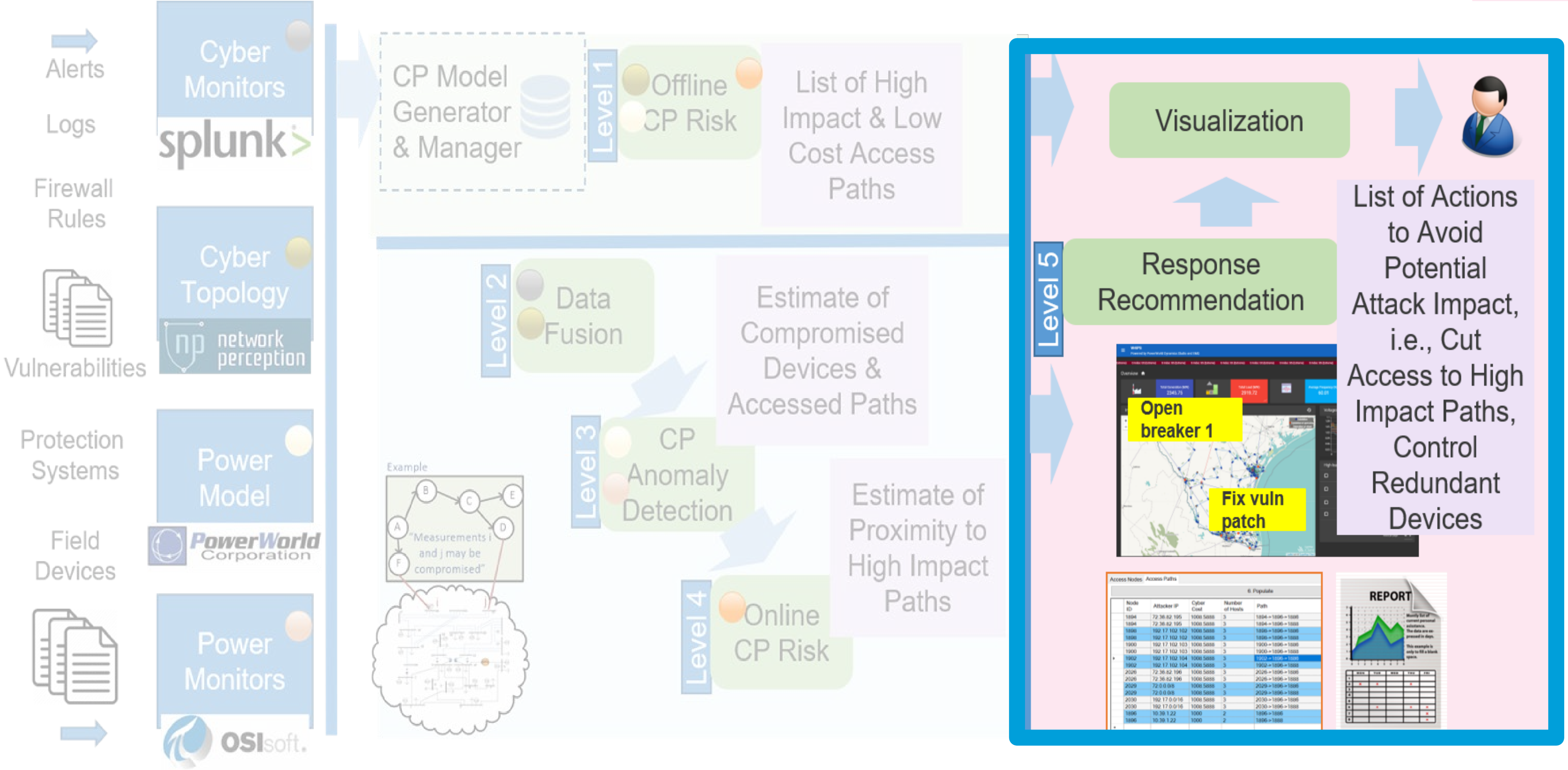
Technique	Scale	Data Dep.	c_t	acc
Cooper and Herskovits (K2)	✓	✗	✓	✓(1)
MCMC	✗	✓	✗	✓(3)
Chou Liu	✗	✗	✗	✓(2)
PDAG PC	✗	✗	✓	N.A

(*) A. Sahu, K. Davis, "Structural Learning Techniques for Bayesian Attack Graphs in Cyber Physical Power Systems," *TPEC*, 2021.

(**) A. Sahu, K. Davis, "Inter-Domain Fusion for Enhanced Intrusion Detection in Power Systems: An Evidence Theoretic and Meta-Heuristic Approach," *Sensors*, special issue "Sensors and Pattern Recognition Methods for Security and Industrial Applications (SPR-SIA)," 2022.

CYPRES Modeling and Workflow

Visualization & Response



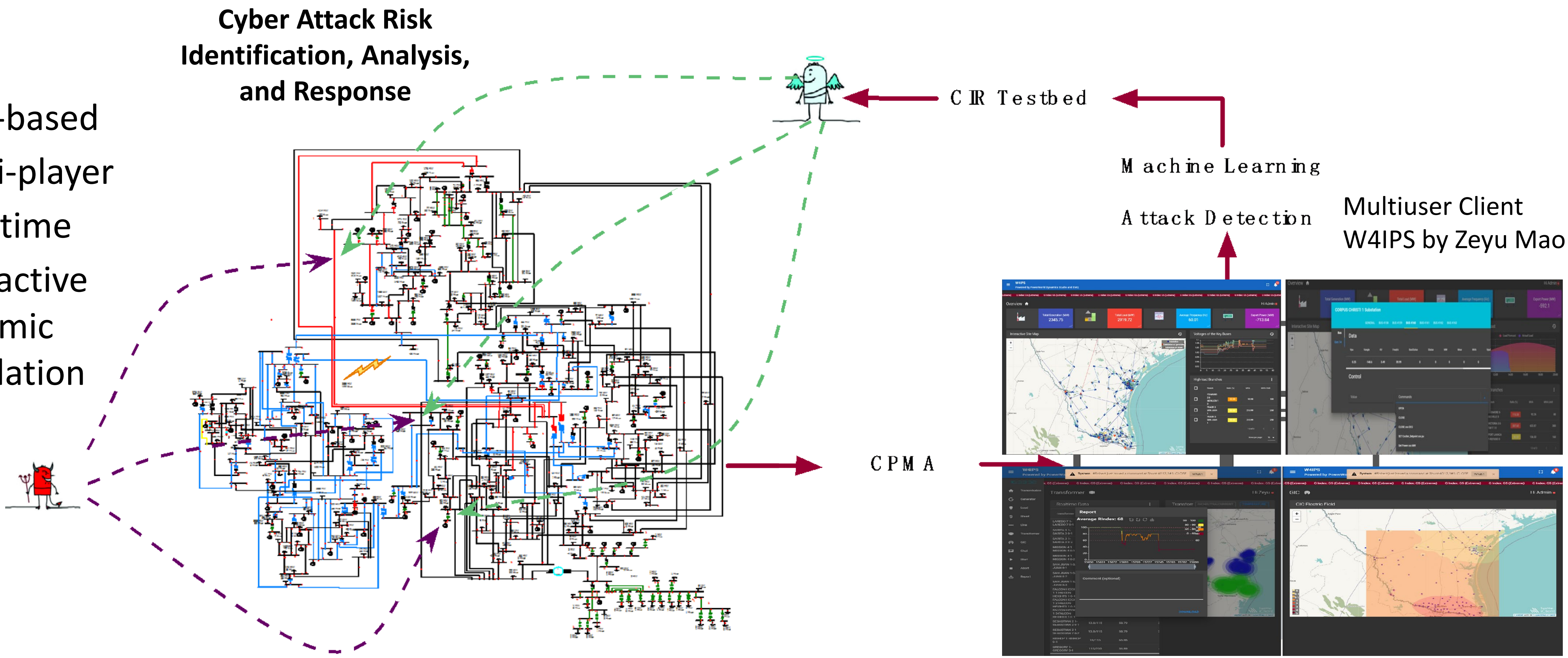
Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

INTERACTIVE GRID DEFENSE

Visualization & Response

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



(*) 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.*

Reconfiguration-Based Defense

Visualization & Response

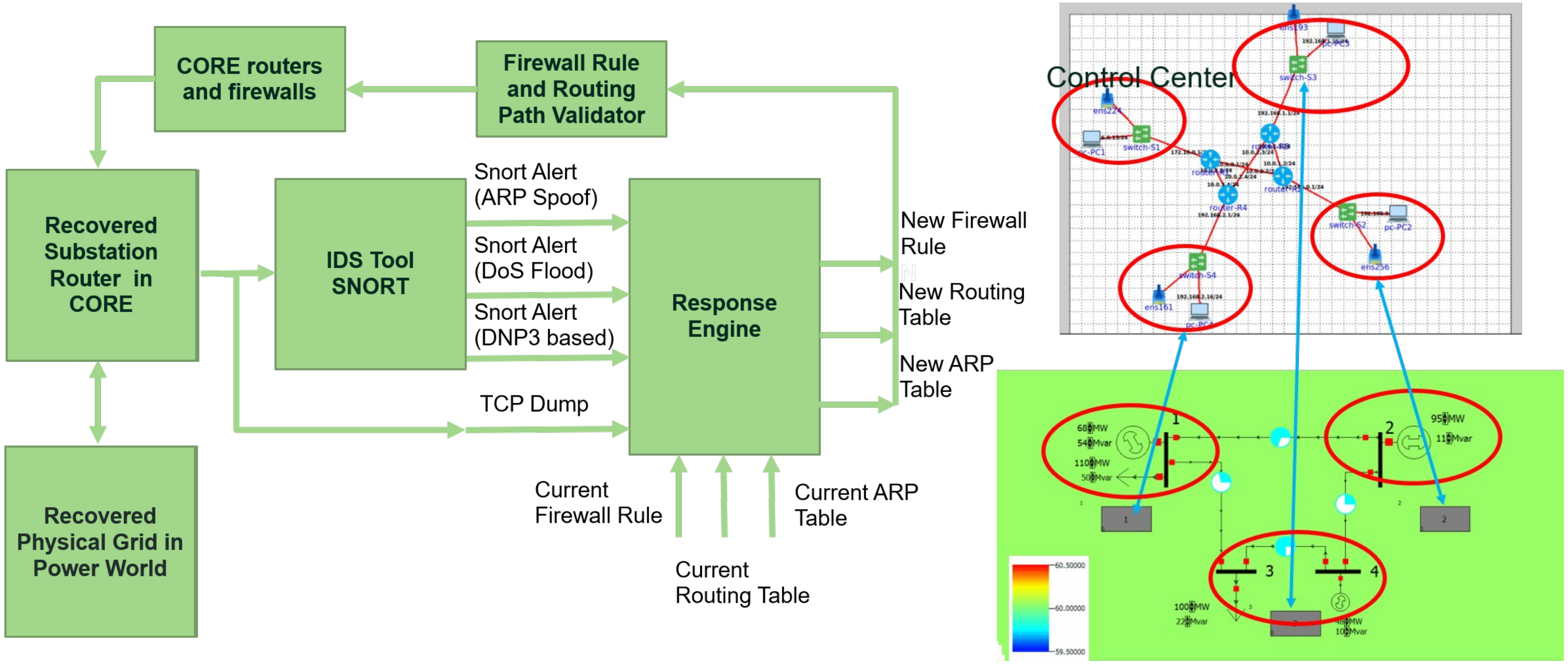
- **Detection Mechanism:**
- 1. SNORT : Use of Intrusion Detection Systems
- 2. Use of Tcp Dump
- 3. Detection based on Firewall rule hits
- 4. Use of Network Monitoring tools like Zabbix, Packetbeat or other SIEMS such as Splunk

- **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

DETECTION & RESPONSE ENGINE

Visualization & Response

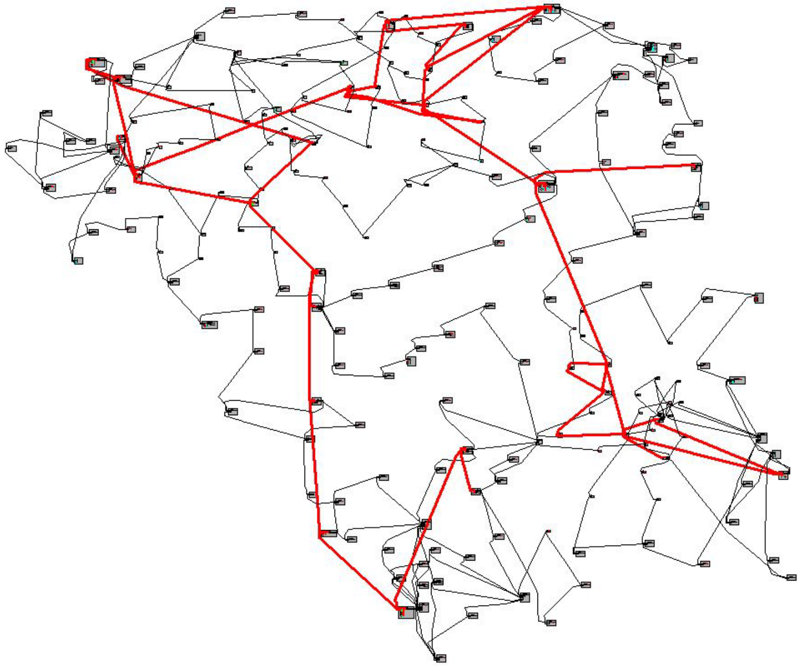


See demo on our website or contact us for live demo with updated threat use cases and validation approach

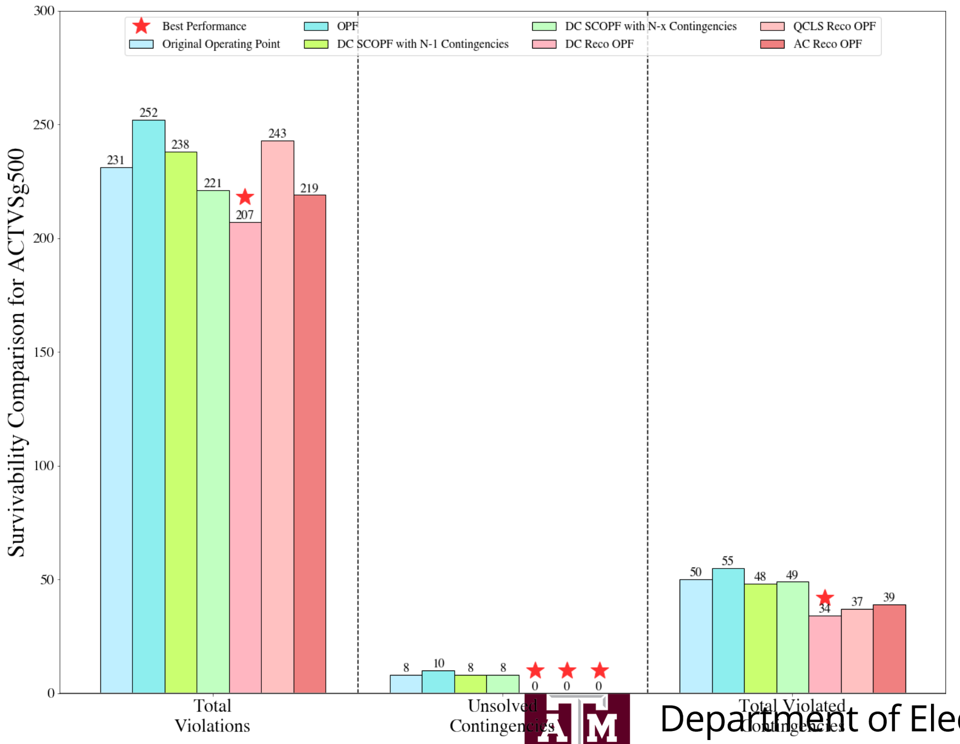
TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Resilience-oriented Optimal Operation & Design as a Solution

ACTIVSg500 System



Objective	Power Flow Model	Cost($/hr)	Total Violations	Total Unsolved	Violated Contingencies
ACTIVSg 500					
R_{ECO} OPF	DC ★	89,447.79	207	0	34
R_{ECO} OPF	QCLS	77,159.61	243	0	37
R_{ECO} OPF	AC	77,482.57	219	0	39
OPF	AC	66,287.91	252	10	55
SCOPF N-1	DC	80,025.06	238	8	48
SCOPF *N-x*	DC	94,438.72	221	8	49



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

Huang, H., Mao, Z., Layton, A., & Davis, K. R. (2022). An Ecological Robustness Oriented Optimal Power Flow for Power Systems' Survivability. *IEEE Trans. on Power Systems*.

RESILIENCE-ORIENTED OPTIMAL OPERATION & DESIGN AS A SOLUTION

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

Objective

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

R_{ECO} Formulation

$$[T] = f(P_{ij}, P_{gen_i}, P_{load_i}, P_{loss_i}, \alpha_{ij})$$

		Gen 1	. . .	Gen n	Bus 1	. . .	Bus m	Output	Dissipation
Input	0	$P_{gen\ 1}$	. . .	$P_{gen\ n}$	0	. . .	0	0	0
Gen 1	0	0	. . .	0	$P_{gen\ 1}$	. . .	0	0	0
.	.	.	. . .	.	.	. . .	.	.	.
.	.	.	. . .	.	.	. . .	.	.	.
.	.	.	. . .	.	.	. . .	.	.	.
Gen n	0	0	. . .	0	0	. . .	$P_{gen\ n}$	0	0
Bus 1	0	0	. . .	0	0	. . .	P_{1m}	$P_{load\ 1}$	$P_{loss\ 1}$
.	.	.	. . .	.	P_{i1}	. . .	.	.	.
.	.	.	. . .	.	.	P_{ij}	P_{im}	.	.
.	.	.	. . .	.	.	. . .	.	.	.
Bus m	0	0	. . .	0	P_{m1}	. . .	0	$P_{load\ m}$	$P_{loss\ m}$
	0	0	. . .	0	0	. . .	0	0	0
	0	0	. . .	0	0	. . .	0	0	0

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

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

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

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

Power System Operational Limits

$$v_i^l \leqslant V_i \leqslant v_i^u (\forall i \in \mathcal{M})$$

$$\theta_i^l \leqslant \theta_i \leqslant \theta_i^u (\forall i \in \mathcal{M})$$

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

$$s_{gen_i}^l \leqslant S_{gen_i} \leqslant s_{gen_i}^u (\forall i \in \mathcal{G})$$

Power Flow Equations

$$S = P + iQ$$

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

$$Q_{ij} = V_i^2[B_{ij}] + V_iV_j[G_{ij}sin(\theta_{ij}) - B_{ij}cos(\theta_{ij})](\forall (i,j) \in \mathcal{B})$$

$$P_{ij} = \alpha_{ij}V_i^2[-G_{ij}] + \alpha_{ij}V_iV_j[G_{ij}cos(\theta_{ij}) + B_{ij}sin(\theta_{ij})](\forall (i,j) \in \mathcal{NB})$$

$$Q_{ij} = \alpha_{ij}V_i^2[B_{ij}] + \alpha_{ij}V_iV_j[G_{ij}sin(\theta_{ij}) - B_{ij}cos(\theta_{ij})](\forall (i,j) \in \mathcal{NB})$$

$$\theta_{ij} = \theta_i - \theta_j (\forall (i,j) \in \mathcal{M})$$

$$P_i = P_{load_i} - P_{gen_i} = \sum_j P_{ij} (\forall j \in \mathcal{M})$$

$$Q_i = Q_{load_i} - Q_{gen_i} = \sum_j Q_{ij} (\forall j \in \mathcal{M})$$

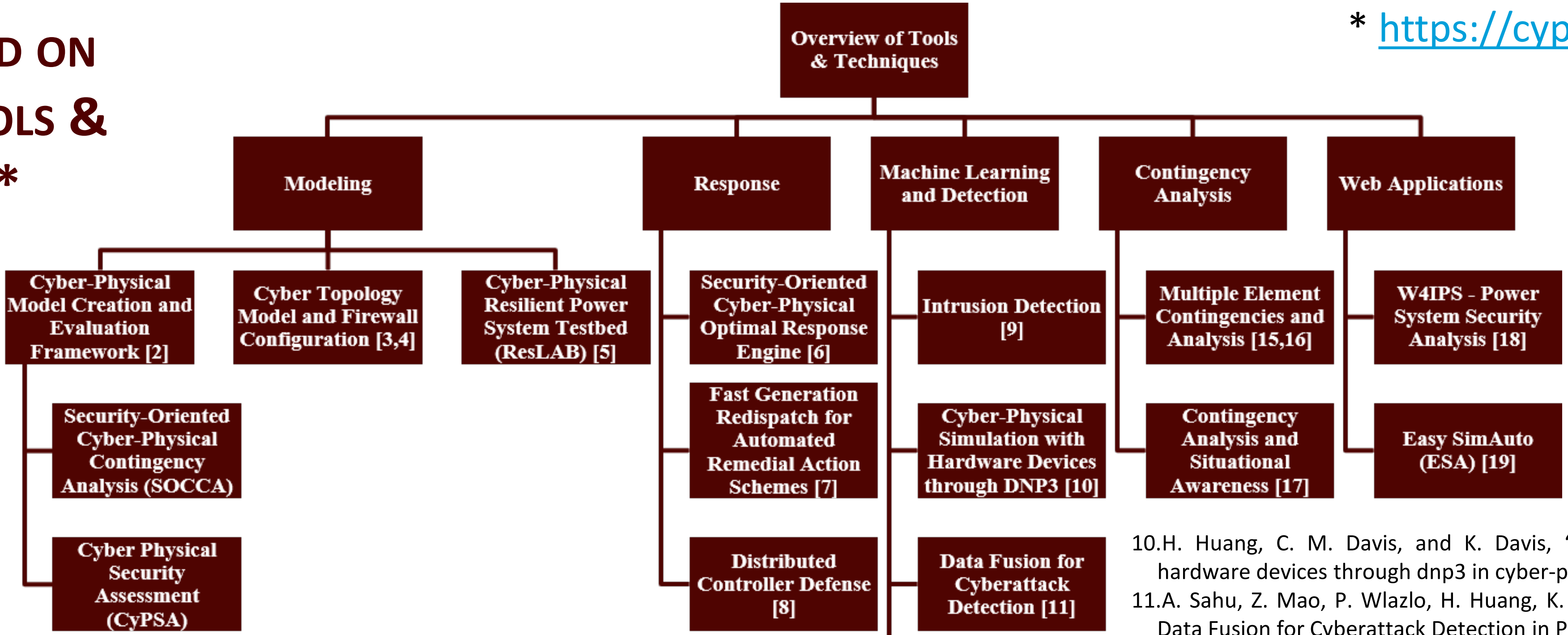
$$P_{loss_i} = \frac{1}{2}\sum_j (P_{ij}^2 + Q_{ij}^2)/(B_{ij}V_i^2)(\forall j \in \mathcal{M})$$

$\mathcal{M}$: Set of buses; $\mathcal{B}$: Set of branches; $\mathcal{NB}$: Set of candidate branches; $\mathcal{G}$: Set of generators

Huang, H., Mao, Z., Layton, A., & Davis, K. R. (2022). An Ecological Robustness Oriented Optimal Power Flow for Power Systems' Survivability. *IEEE Trans. on Power Systems*.

Background on Project Tools & Techniques*

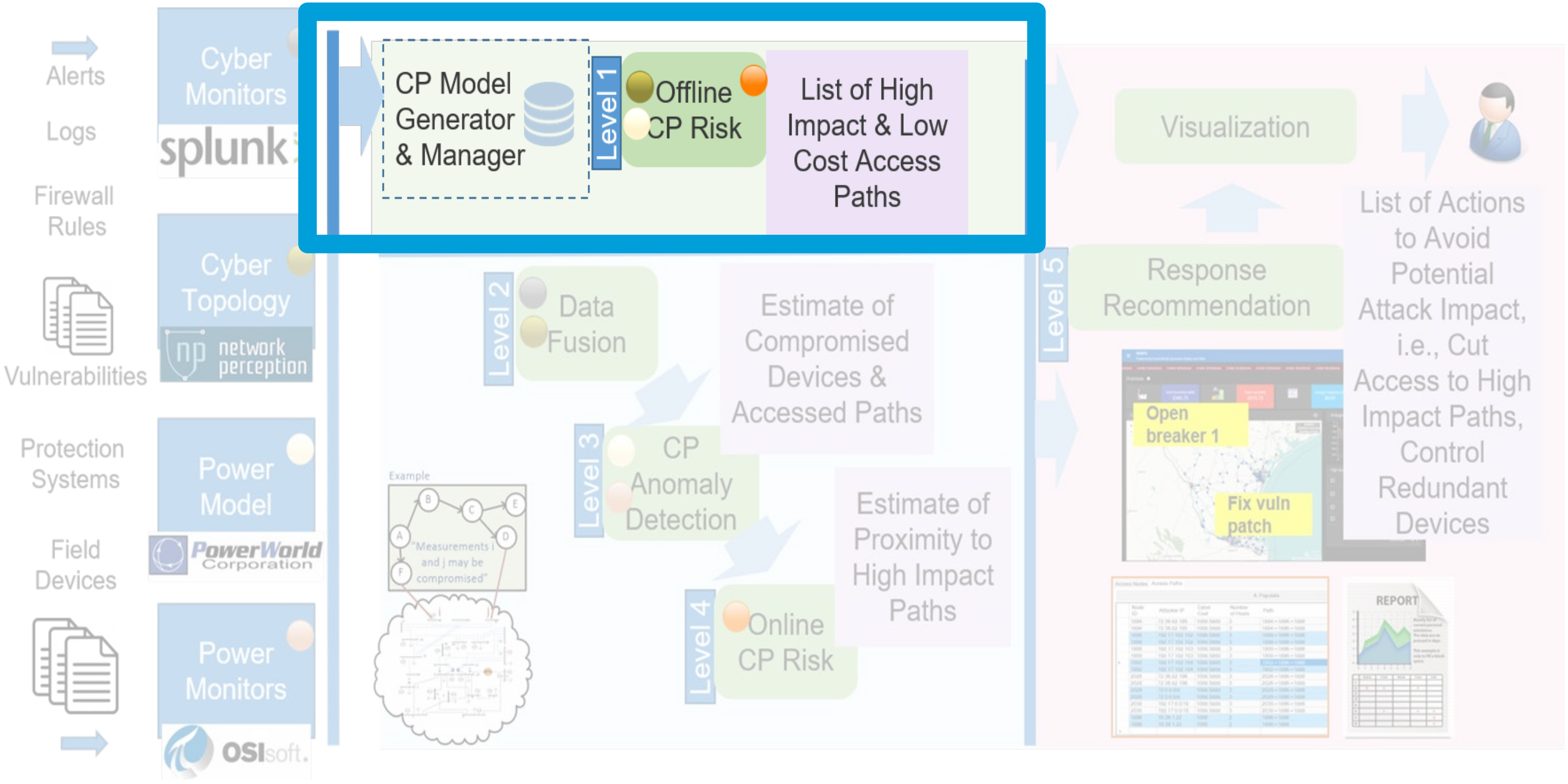
* https://cypres.engr.tamu.edu/



1. K. Davis, “An Energy Management System Approach for Power System Cyber-Physical Resilience,” invited position paper for Virtual Workshop on Cyber Experimentation and Science of Security (CESoS), Nov. 2021.
2. A. Sahu, et al, “A Framework for Cyber-Physical Model Creation and Evaluation,” IEEE ISAP, Dec. 2019.
3. P. Wlazlo, et al, “A Cyber Topology Model for the Texas 2000 Synthetic Electric Power Grid,” IPTComm, 2019.
4. N. Gaudet, et al, “Firewall Configuration and Path Analysis for Smart Grid Networks,” IEEE CQR, May 2020.
5. A. Sahu, et. al., “Design and Evaluation of a Cyber-Physical Resilient Power System Testbed,” IET Cyber-Physical Systems, June 2021.
6. A. Sahu, H. Huang, K. Davis, S. Zonouz, “SCORE: A Security-Oriented Cyber-Physical Optimal Response Engine,” IEEE SmartGridComm, Oct. 2019.
7. H. Huang, et. al “Fast Generation Redispatch Techniques for Automated Remedial Action Schemes,” IEEE 20th ISAP, Dec. 2019.
8. S. Hossain-McKenzie, et al, “Strategy for distributed controller defence: Leveraging controller roles and control support groups to maintain or regain control in cyber-adversarial power systems,” IET Cyber-Physical Systems, April 2021. (IET 2021 Premium Award for Best Paper)
9. A. Sahu, Z. Mao, K. Davis, and A. Goulart, “Data Processing and Model Selection for Machine Learning-based Network Intrusion Detection,” IEEE CQR 2020, May 2020.
10. H. Huang, C. M. Davis, and K. Davis, “Real-time power system simulation with hardware devices through dnp3 in cyber-physical testbed,” 2021 TPEC, Feb. 2021.
11. A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, S. Zonouz “Multi-Source Data Fusion for Cyberattack Detection in Power Systems” IEEE Access, 2021.
12. P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, S. Zonouz, “Man-in-The-Middle Attacks and Defense in a Power System Cyber-Physical Testbed,” IET Cyber-Physical Systems, June 2021.
13. Z. Mao, A. Sahu, P. Wlazlo, Y. Liu, A. Goulart, K. Davis, and T. Overbye, “Mitigating TCP Congestion: A Coordinated Cyber and Physical Approach,” NAPS, Nov. 2021.
14. K. Knesek, et al, “Detecting Attacks on Synchrophasor Protocol Using Machine Learning Algorithms,” SmartGridComm, Oct. 2021.
15. Huang, et al., “Toward efficient wide-area identification of multiple element contingencies in power systems,” 2021 IEEE ISGT.
16. M. Narimani, H. Huang, A. Umunnakwe, Z. Mao, A. Sahu, S. Zonouz, and K. Davis, “Generalized Contingency Analysis Based on Graph Theory and Line Outage Distribution Factor,” IEEE Systems Journal, 2021.
17. H. Huang, D. Gray, J. Mendoza, K. Davis, “Automating the Process to Quantify Cyber-Physical Risk with Contingency Analysis and User Input,” NAPS 2021.
18. Z. Mao, H. Huang, K. Davis, “W4IPS: A Web-based Interactive Power System Simulation Environment For Power System Security Analysis,” HICSS, Jan. 2020.
19. B. L. Thayer, Z. Mao, Y. Liu, K. Davis, T. Overbye “Easy SimAuto (ESA): A Python Package that Simplifies Interacting with PowerWorld Simulator,” Journal of Open Source Software, 5 (50), 2289

CYPRES Modeling & Workflow

Offline CPS Risk

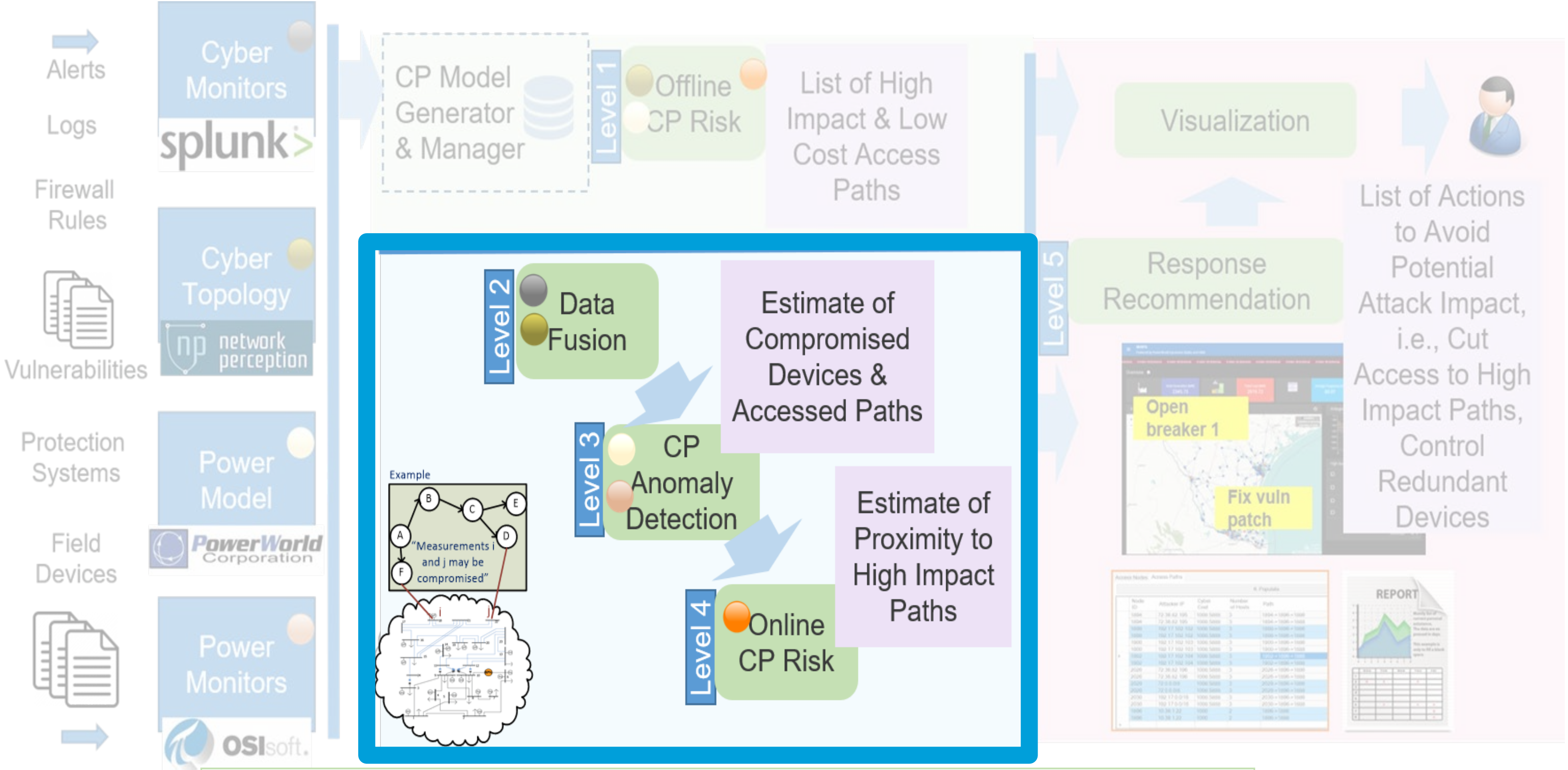


Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

CYPRES MODELING & WORKFLOW

Online CPS Risk

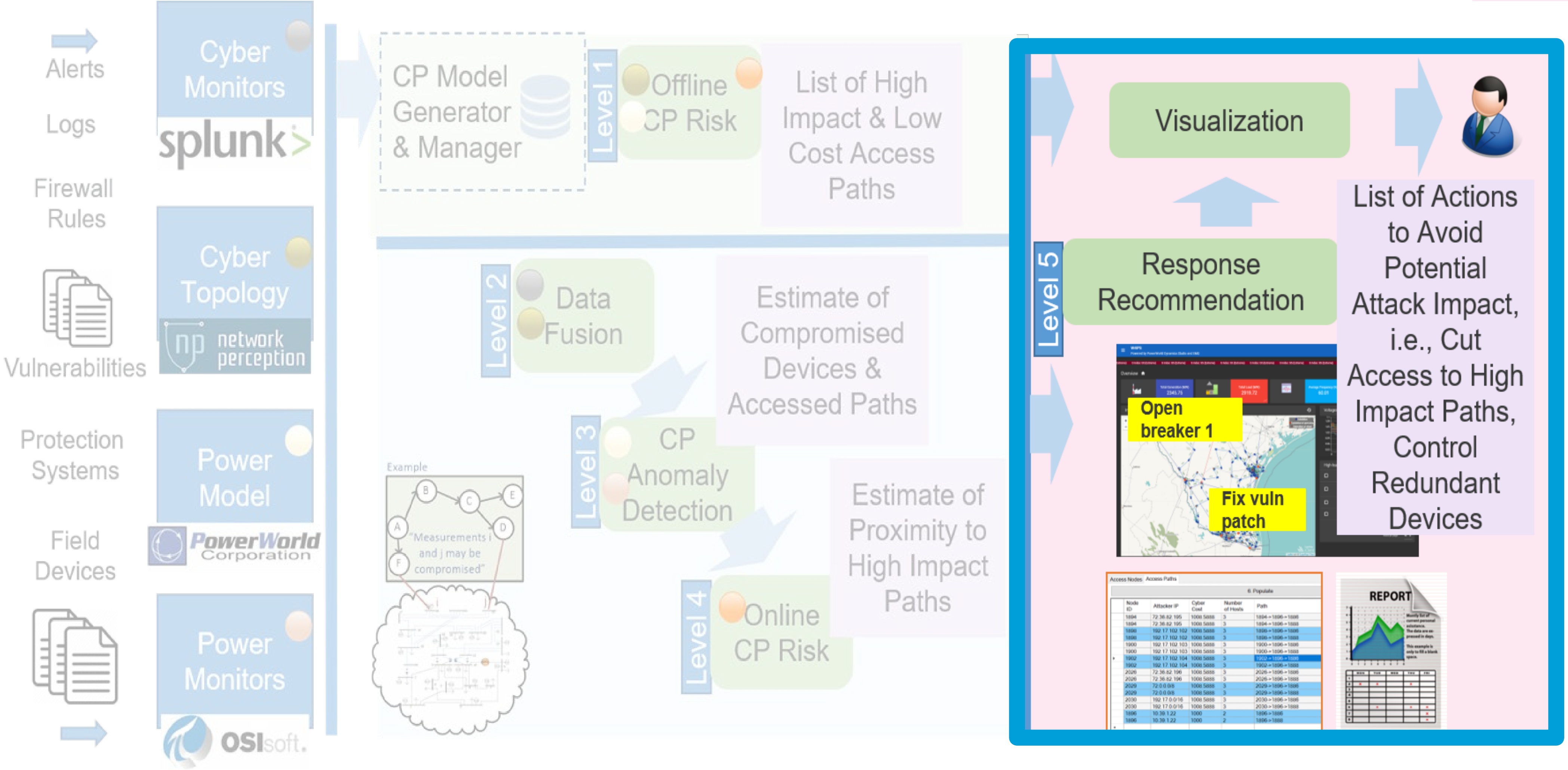


Cyber-Physical Resilient Energy Systems (CYPRES)
https://cypres.engr.tamu.edu/

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

CYPRES Modeling & Workflow

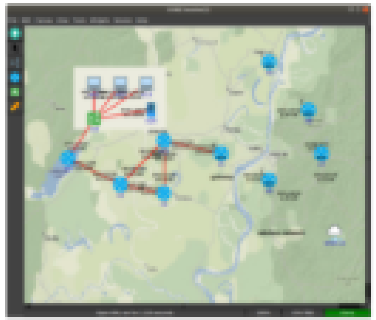
Visualization & Response



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

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Mapping Real System Architectures and Technologies to the Emulated Environment



Network Data → NPView → Export to JSON and CSV Data → NPViewToCore Python Script → CORE-pygui

Network Data

- IP Tables Rules
- Network Device Configurations

NPView

- Parses the Firewall rules and Device Config
- Graphical View of the Network
- Analysis of Firewall Network Rules

Export to JSON and CSV Data

- Graph is Split into Region and Nodes
- Firewall rules are complied into csv

NPViewToCore Python Script

- Import all data into dataframe
- Store host node info in NetworkX Graph
- Assign services to each node
- Save CORE session in XML format

CORE-pygui

- Visualize/Validate the CORE Network Setup
- (Re)create Cyberattacks

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

CPS Testbed Operation

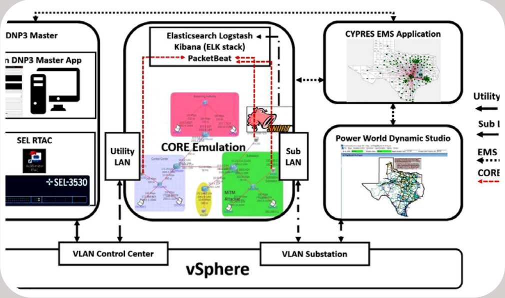
Port Scan | DoS | DDoS | MiTM

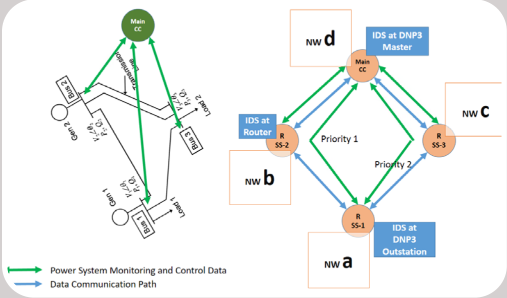
Network Monitoring | IDS Alerts | Physical Meas.

Fusion Engine

Intrusion Detection | CyPSE | CyPSA

Visualization | Decision Support / Control





Modeling

Realistic modeling and testbed emulation of the system with its threats and defenses

Situational Awareness

Vulnerability and risk analyses, monitoring, inference, detection

Response

Mitigations, defense, outreach, training

The Pillars

Dr. Kate Davis
katedavis@tamu.edu

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

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering