Data-Driven Tools for Cyber-Physical Resiliency of the Electric Grid

A. Srivastava, Washington State University

Associate Professor, Washington State University
Director, Smart Grid Demonstration and Research Investigation Lab
Technical Lead, UI-ASSIST, https://uiassist.org
Senior Scientist, Pacific Northwest National Lab (PNNL)
anurag.k.srivastava@wsu.edu

April 2nd, 2020

RESEARCH INTERESTS

- **Data-Driven System Operation and Control Algorithms to enable resiliency, voltage stability and security (Transmission Systems with Active Distribution and Microgrids/ DERs)**

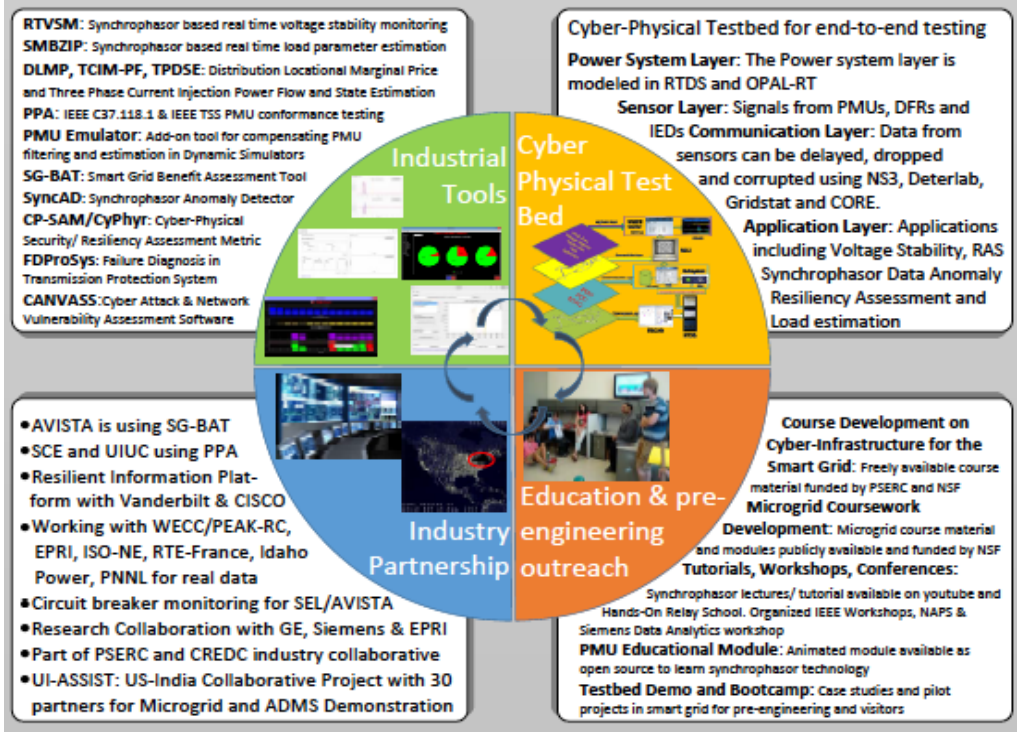
Keywords: Resiliency, PMUs, Data-driven, Cyber-Power, Voltage Control

RESEARCH SPONSORS

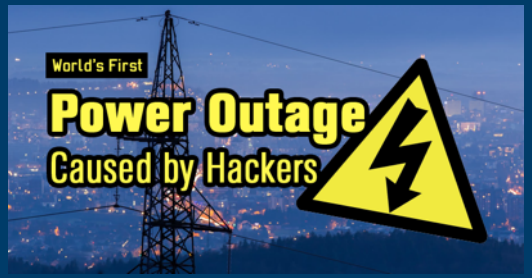
https://sgdril.eecs.wsu.edu

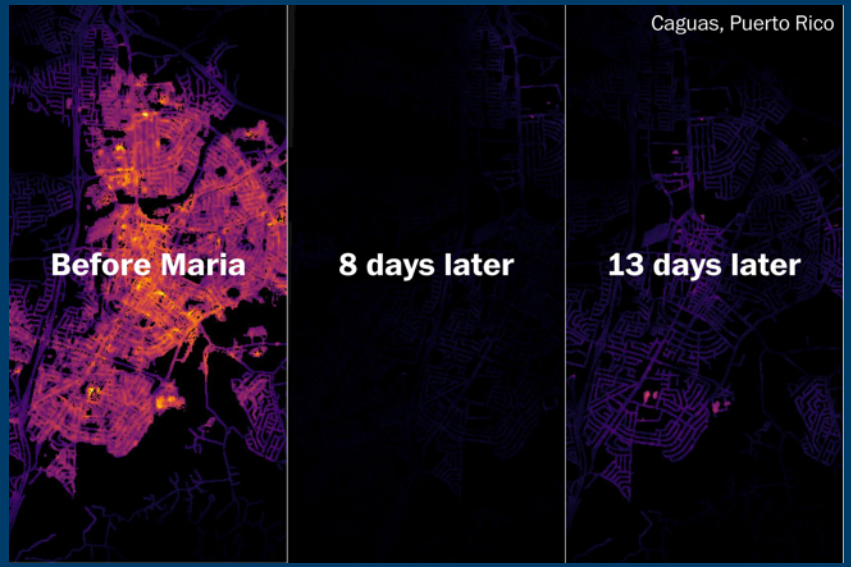
ACADEMIC/INDUSTRY EXPERIENCE

- Director, Smart Grid Demonstration and Research Investigation Lab; 2010--
- MIT, PEAC, Aachen University, RTE-France, GE, PNNL, INL, PJM, SEL; 2016-2018
- Mississippi State University; 2005-2010, IIT Kanpur; 1999-2001
- Ph.D. 2005 Illinois Institute of Technology, (IIT), Chicago



Power Grid: Reliable but Not Resilient



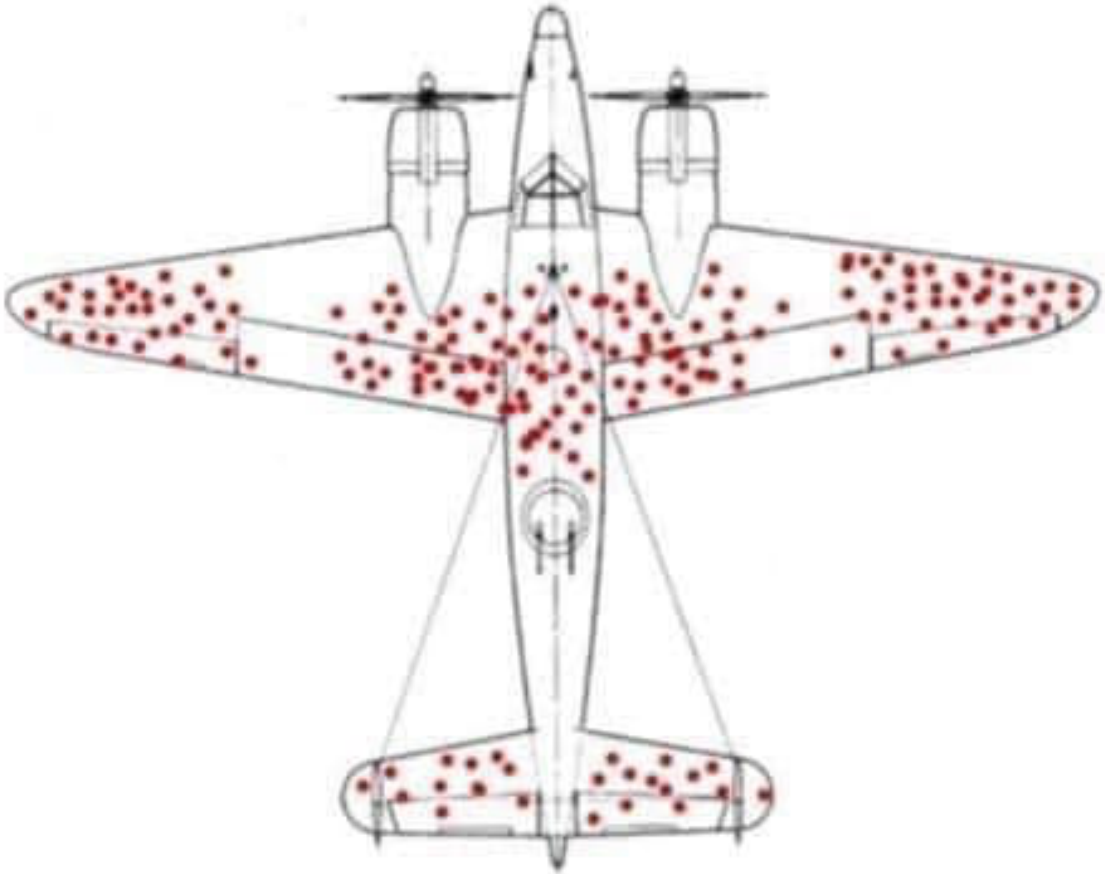


What can we do about it?

- Secure, but not resilient
- Reliable, but not resilient

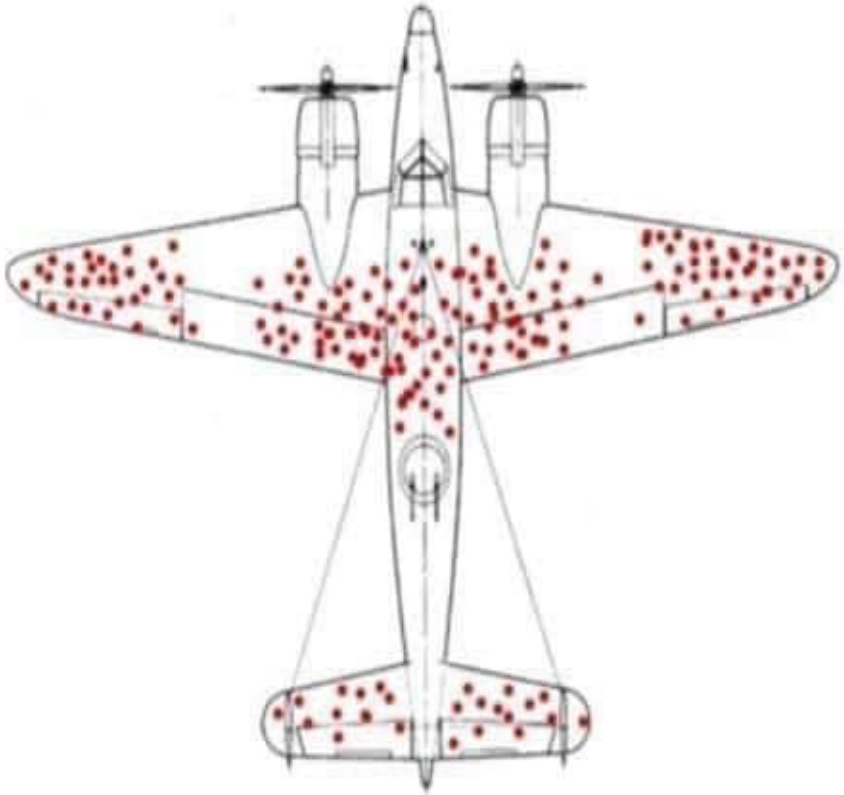
- Define and measure cyber-physical resiliency
- Change the existing practice for cyber-physical security and resiliency
- Use tools for resiliency monitoring and decision support

WW2, 1939-1945



This is a picture tracking bullet holes

WW2, 1939-1945



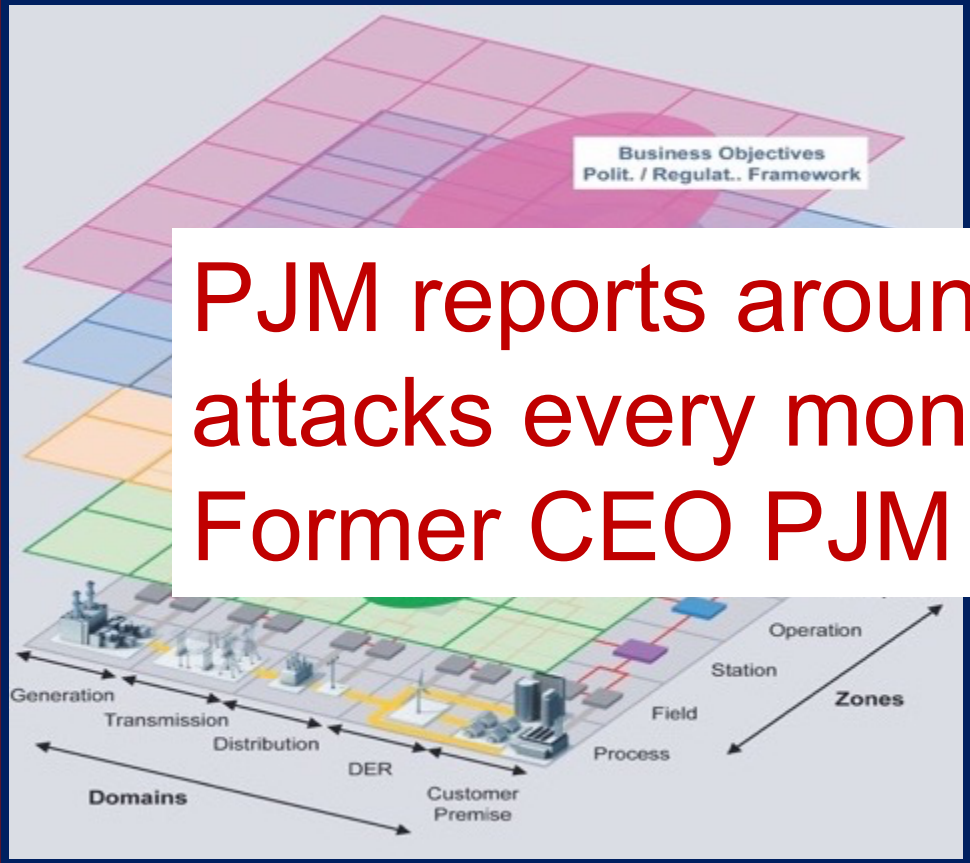
At first, the military wanted to reinforce those areas, because obviously that's where the ground crews observed the most damage on returning planes. Until

Abraham Wald pointed out that this was the damage on the planes that *made it*

where there are no dots at all, because those are the places where the planes won't survive when hit. This phenomenon is called

bias towards known vulnerability instead of system survivability.

6-7 Decades Later: Cyber-Power Electric Grid



At first, find vulnerabilities and attack surface, patch it and fix it and call it secure.

PJM reports around 4,000+ cyber attacks every month - T. Boston, Former CEO PJM

ıat
h

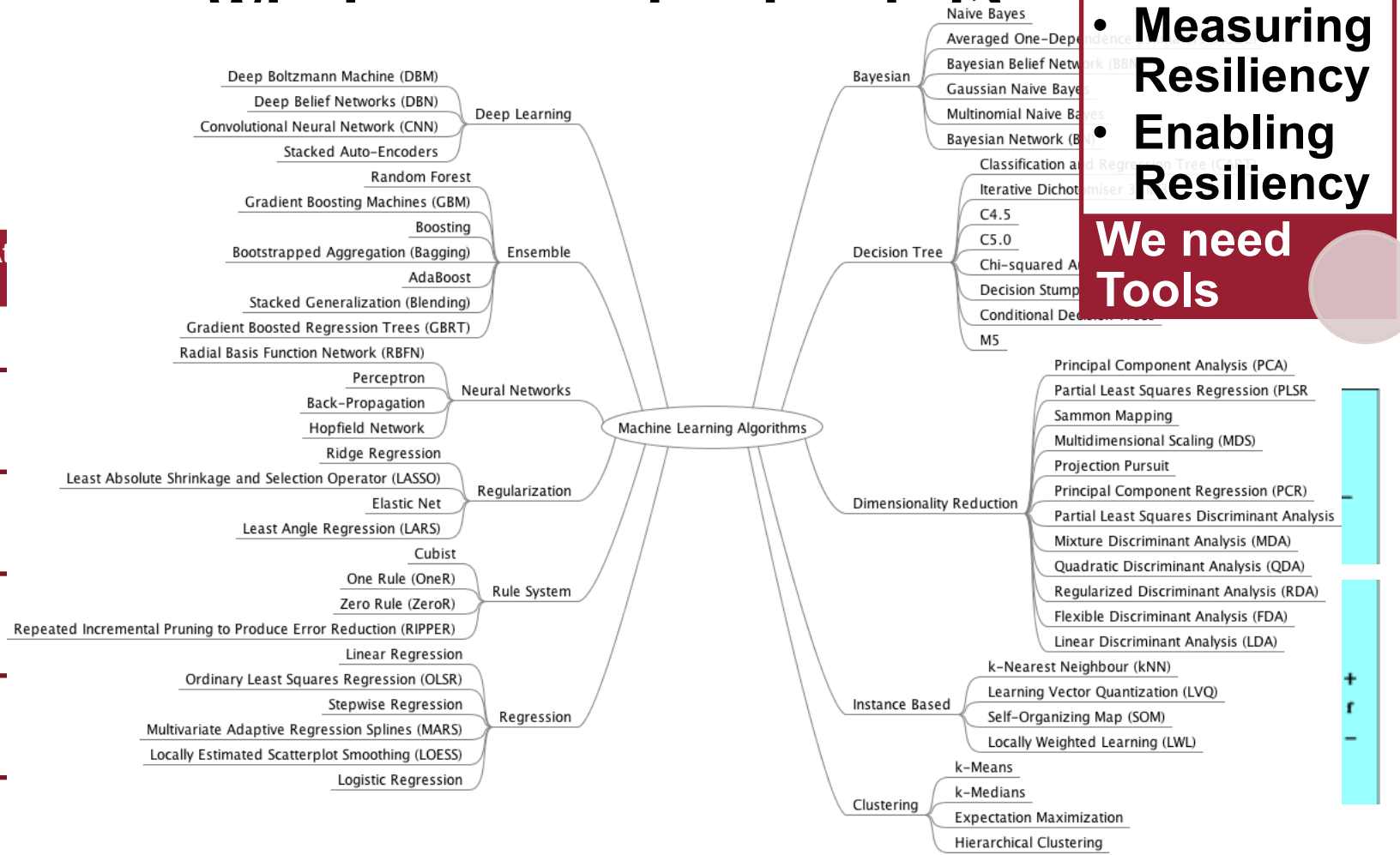
pact on
ınt for
s is

known as

bias towards known vulnerability instead of system survivability or resiliency.

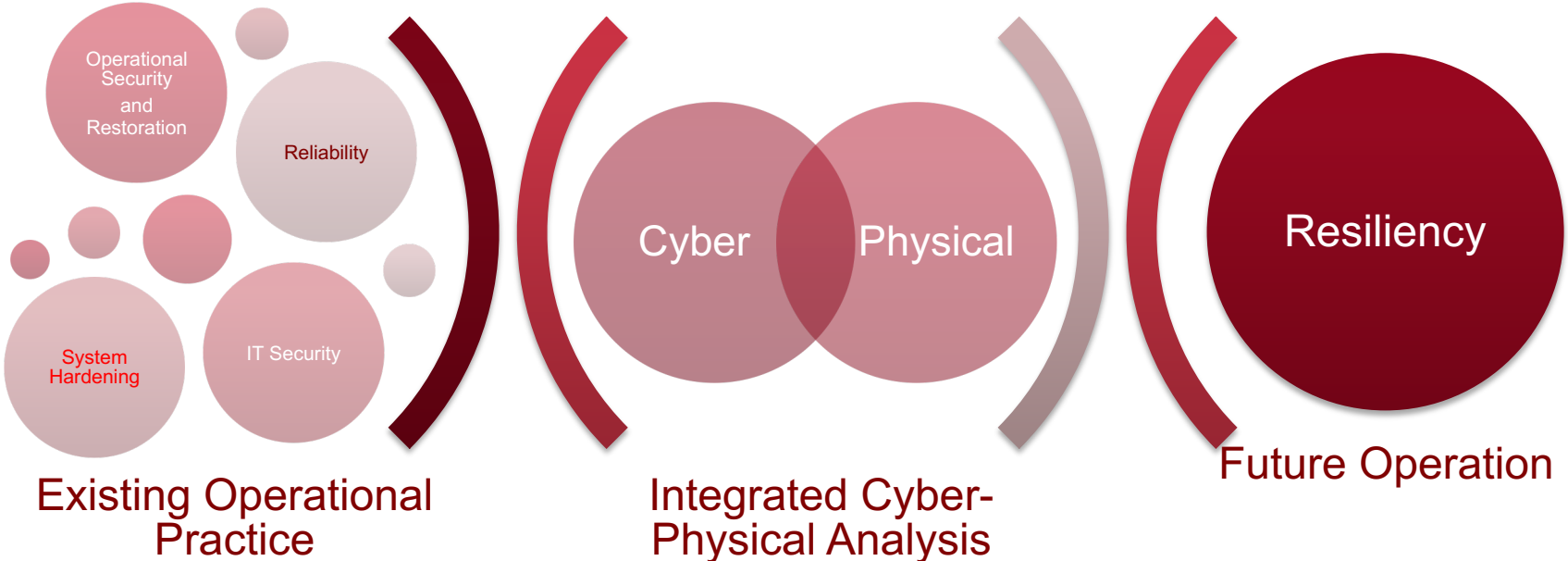
- Measuring Resiliency
- Enabling Resiliency

We need Tools



Electric Grid Resiliency

Resilience: The ability to supply its critical load through (and in spite of) limited extreme contingencies



W

Withstand any sudden inclement weather or human attack on the infrastructure.

R

Respond quickly, to restore balance in the community as quickly as possible, after an inevitable attack.

A

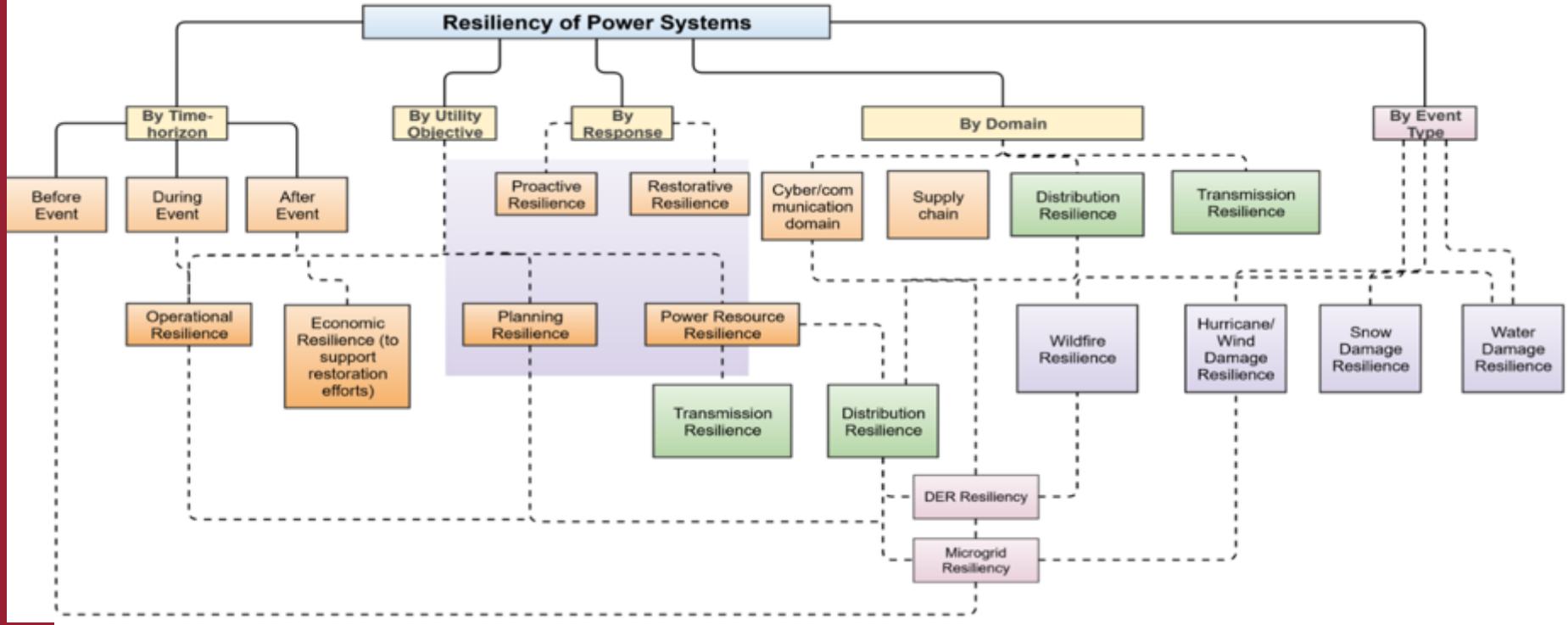
Adapt to abrupt and new operating conditions, while maintaining smooth functionality, both locally and globally.

P

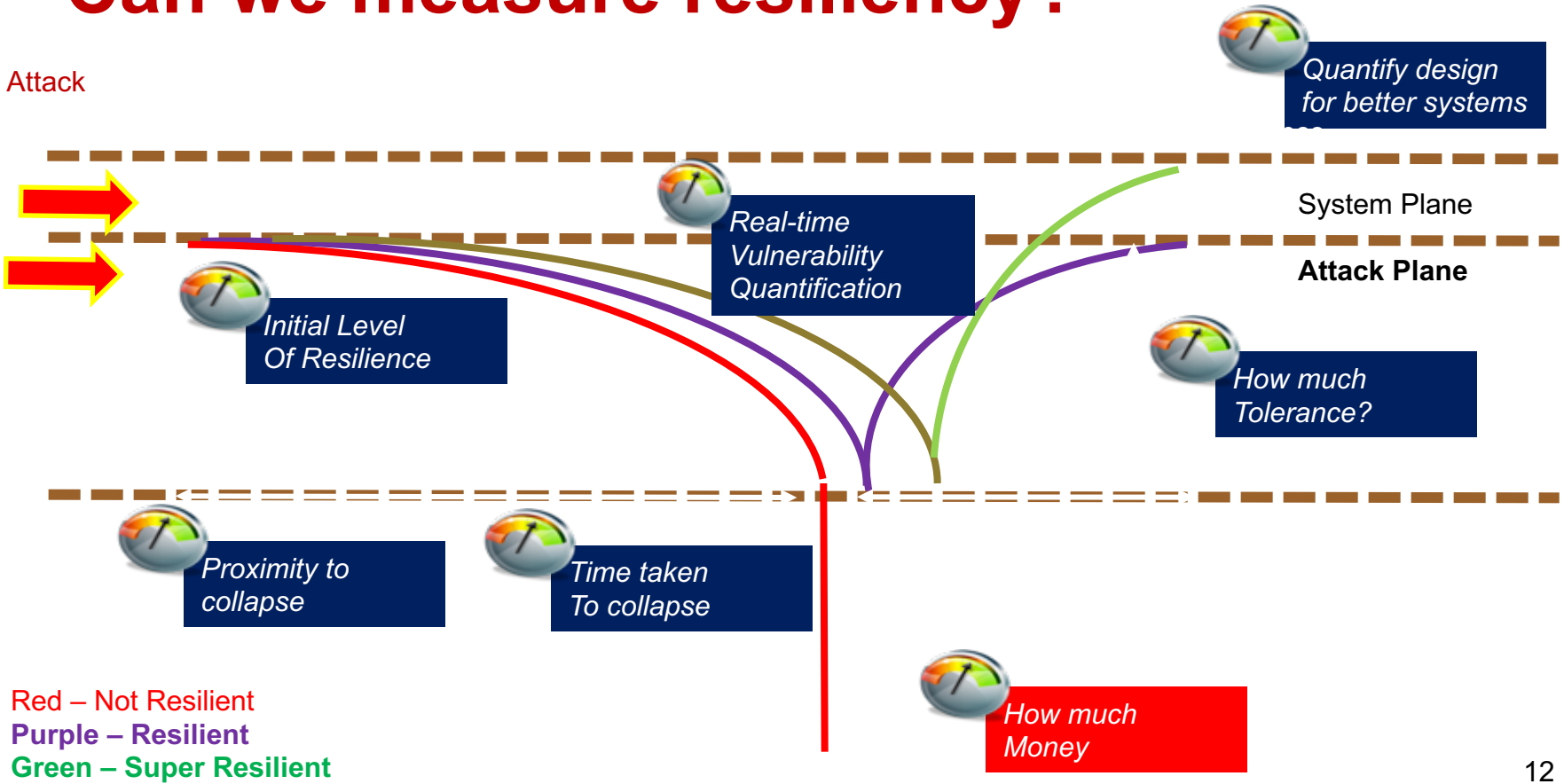
Predict or **Prevent** future attacks based on patterns of past experiences, or reliable forecasts.

https://science.house.gov/legislation/hearings/full-committee-hearing-resiliency-electric-grid-s-only-hope

Taxonomy of Resiliency



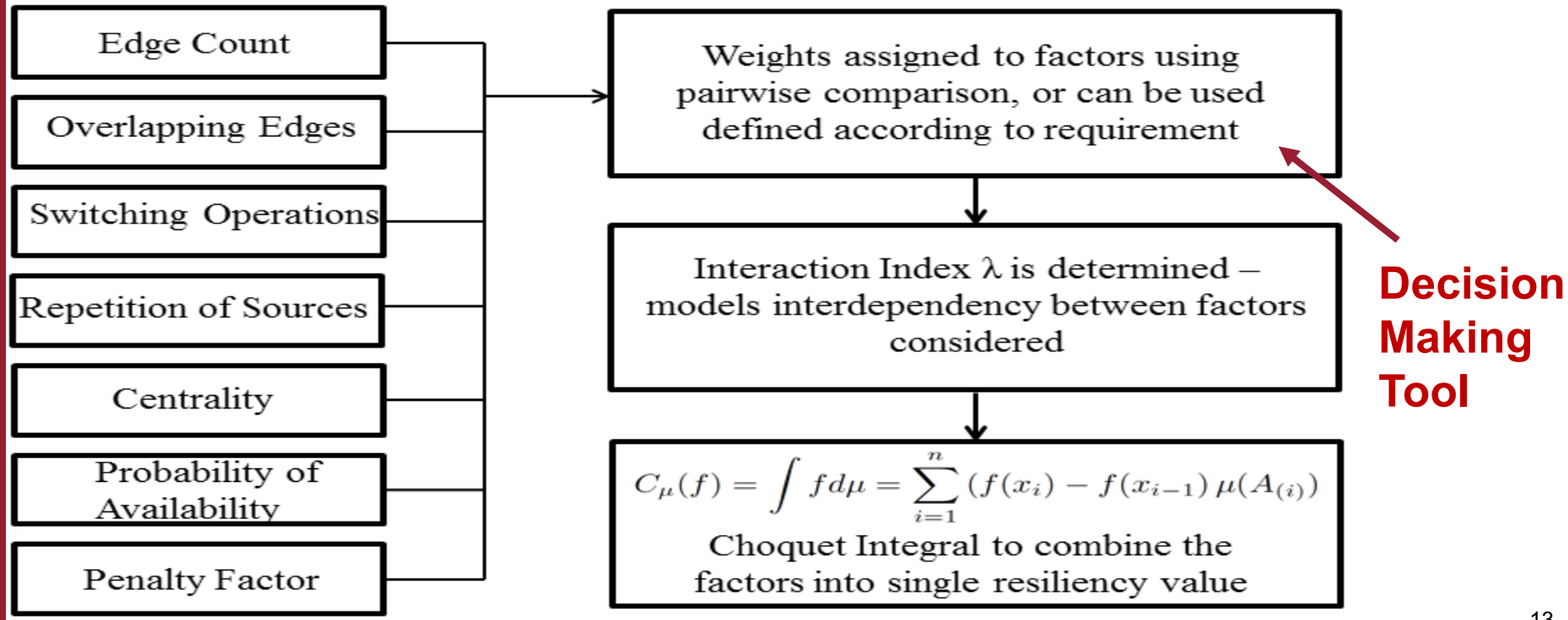
Can we measure resiliency?



Red – Not Resilient
Purple – Resilient
Green – Super Resilient

Overview of resiliency quantification process

- Network, control, generating sources and critical loads



Measuring Resiliency

Information provided by Graph Theory

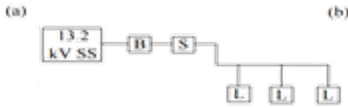
Usual Graph Theory Representation

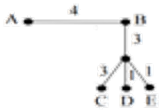
CANVASS: Cyber-Attacks and Network Vulnerability Analytics Software for Smart Distribution Grids

CyPhyR: Cyber-Physical Resiliency in Microgrid

CP-SAM: Cyber-Physical Security Assessment Metric

CP-TRAM: Cyber-Physical Transmission Resiliency Metric





$$A(G) = \begin{array}{c} \\ A \\ B \\ C \\ D \\ E \\ F \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & D & E & F \end{array} \\ \begin{pmatrix} 0 & 4 & 0 & 0 & 0 & 0 \\ 4 & 0 & 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 3 & 1 & 1 \\ 0 & 3 & 0 & 3 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Characteristic Path Length

$$\rho(i,j)' = \frac{\rho(i,j) - \min_{i=1}^{\eta}(\rho(i,j))}{\max_{i=1}^{\eta}(\rho(i,j)) - \min_{i=1}^{\eta}(\rho(i,j))}$$

- Weather Parameters
- Infrastructure Parameter

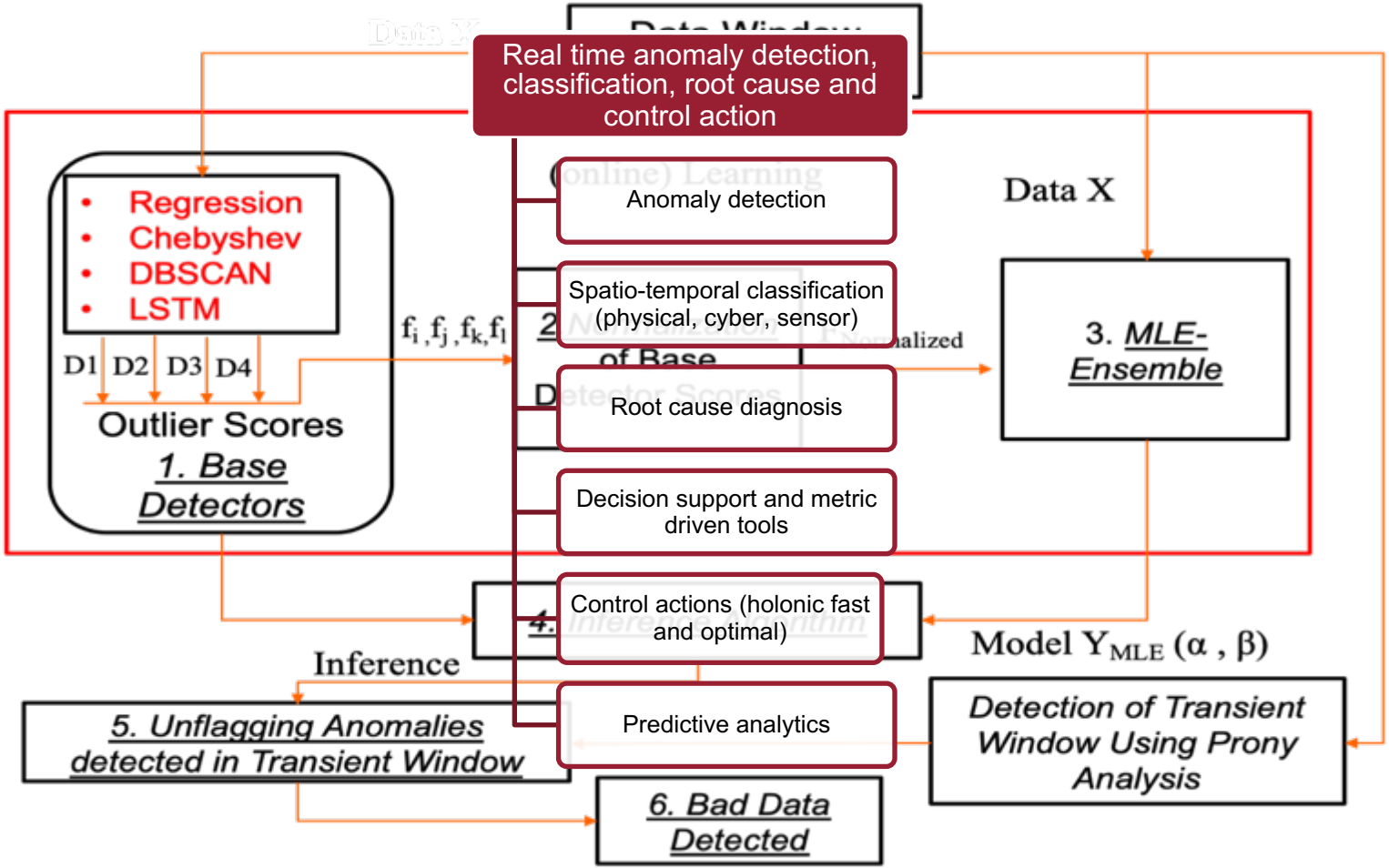
$$V = [A_{f_c}\ B_D\ C_{C_B}\ D_{l_G}\ E_{C_n}\ F_{\Delta\lambda}\ G_{\lambda_2}]^T$$

$$\Re_\tau = \sum_{j=1}^{\eta} V_j \rho(i,j)'$$


Multiple Players
Competing Goals
Dynamic Settings
Time Stress
High Task Loading
Uncertainty
Organizational Factors
High Stakes


Grid Analysis & Management
Detailed Logs
Super Mon
Anomaly D
Competi
Goa
Time
Stress
Situation Awareness & Decision Support
on
tion
nty
ntrol
amazon
GRID MANAGEMENT AND DECISION MAKING DASHBOARD

Ensemble Approach for Anomaly/ Event Detection



Results for SyncAED

Tests on the RTDS simulated PMU data (1.5 hours)

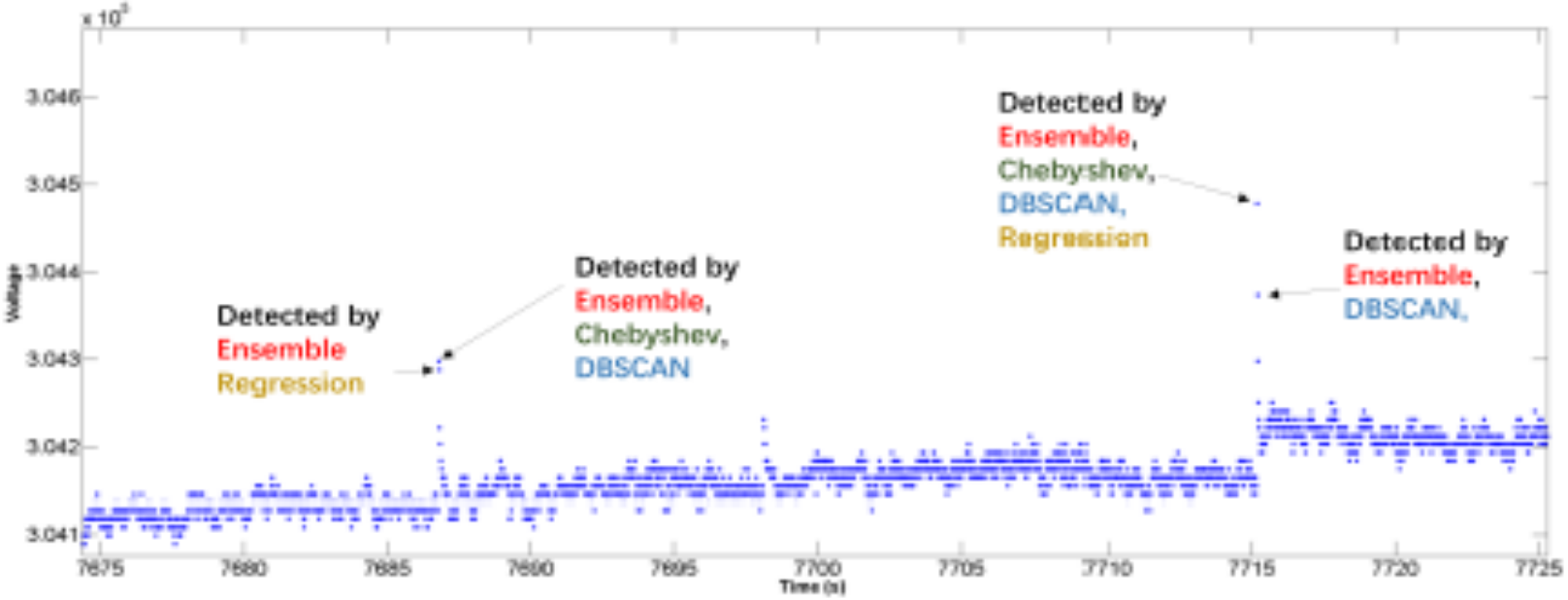
	Recall	Precision	False positive
Linear Regression	0.9021	0.8565	0.1435
DBSCAN	0.8821	0.8821	0.1179
Chebyshev	0.9154	0.8754	0.1246
LSTM	0.9298	0.8554	0.1446
MLE ensemble	**0.9351**	**0.8913**	**0.1087**

Tests on the RTDS simulated PMU data (1.5 hours, 5% bad data points, 5%-10% range)

	Recall	Precision	False positive
Linear Regression	0.7854	0.7655	0.2345
DBSCAN	0.7216	0.7015	0.2985
Chebyshev	0.8125	0.7542	0.2458
LSTM	0.8298	0.7754	0.2246
MLE ensemble	**0.8912**	**0.9021**	**0.0979**

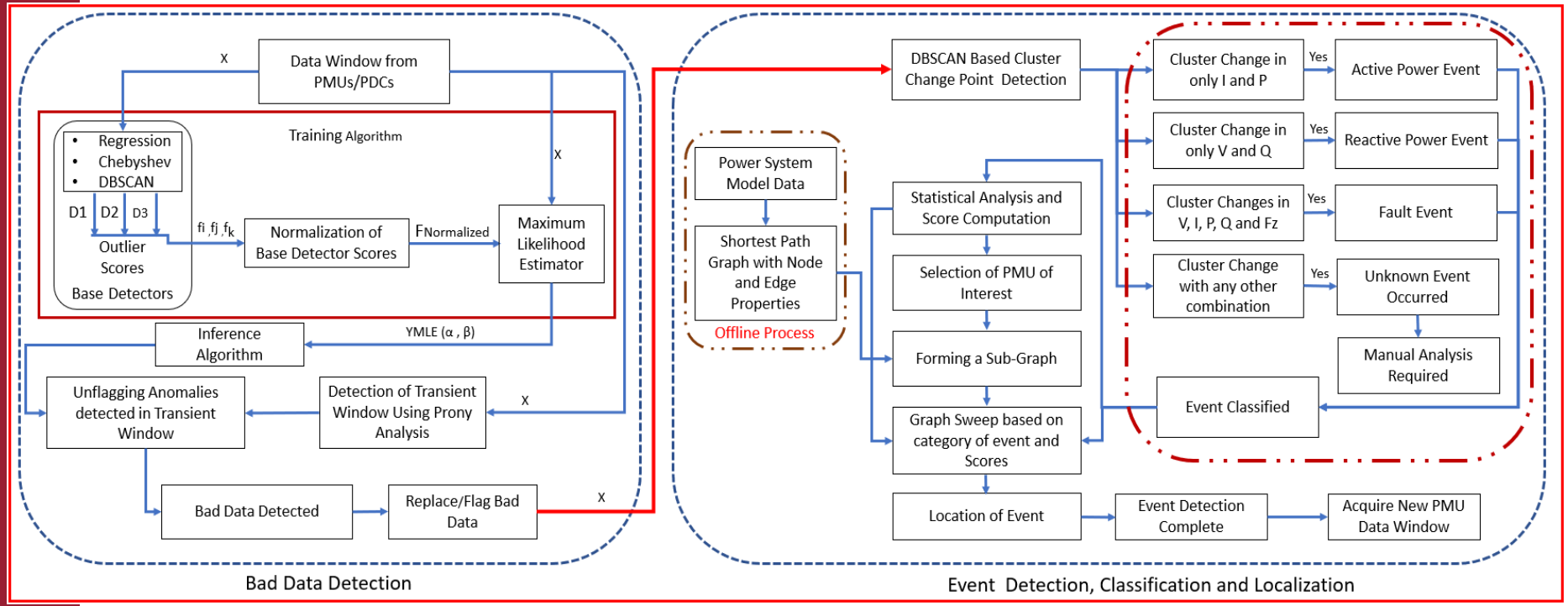
Tests on the RTDS simulated PMU data (1.5 hours, 10% bad data points, 10%-20% range)

Results with SyncAED using Real PMU Data



Thanks to PNNL/ EPRI for data

Synchrophaosr Anomaly Detection, Event Detection, Classification and Localization



- Being extended with concept drift, Graph based deep learning, microPMU
- PMU based model validation, state estimation, emergency control

SyncAED Tool

USER SETTINGS

SynchroPhasor Anomaly And Event Detection

Anomaly Detection Event Detection

Anomaly Detection data

id	diagnosis	radius_mean	smoothness_mean
842302	M	17.99	0.1184
842517	M	20.57	0.08474
84300903	M	19.69	0.1096
84348301	M	11.42	0.1425
84358402	M	20.29	0.1003
843786	M	12.45	0.1278

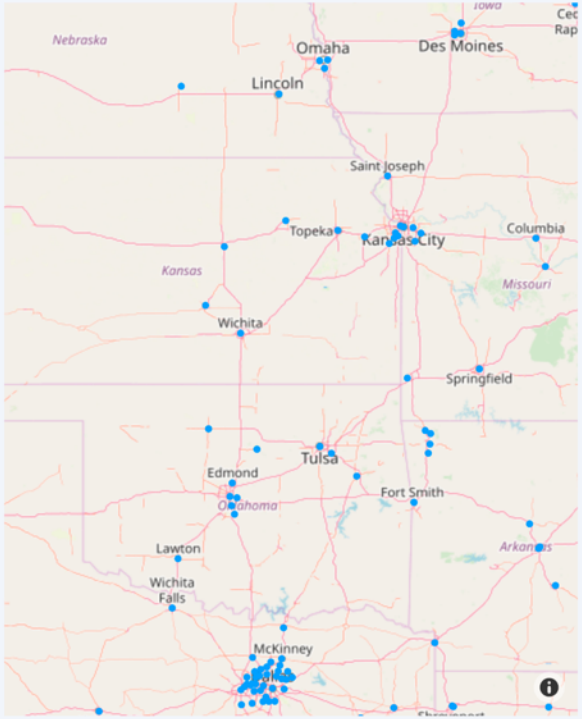
« ‹ 1 / 95 › »

Event Detection data

id	diagnosis	radius_mean	smoothness_mean
842302	M	17.99	0.1184
842517	M	20.57	0.08474
84300903	M	19.69	0.1096
84348301	M	11.42	0.1425
84358402	M	20.29	0.1003
843786	M	12.45	0.1278

« ‹ 1 / 95 › »

Network Graph of PMU Data



Event Details - Case 1

Sno.	Time (s)	Bus	Event	Voltage
1	109	9	Cap bank Closed	Up
2	119	10	3 Phase fault	Down
3	132	9	Cap bank Removed	Down
4	147	8	P load decreased	Up
5	157	9	Cap bank Closed	Up
6	168	10	3 Phase fault	Down
7	178	9	Cap bank Removed	Down
8	188	8	P load increased	Down
9	198	8	Q load increased	Down
10	209	8	P load increased	Down
11	219	8	Q load decreased	Up
12	229	2	GenDrop	Down

Results - Case 1

S No.	Time (s)	Actual Event	Actual Location	Detection Bus		Classified Event	Normalized Score	
				PMU 1	PMU 2		PMU 1	PMU 2
1	109	Cap Bank Closed	Bus 9	9	10	Reactive Power Event	0.22	0.14
2	119	Three Phase fault	Bus 10	10	9	Fault Event	37.25	23.54
3	132	Cap Bank Opened	Bus 9	9	10	Reactive Power Event	0.23	0.13
4	148	P load decreased	Bus 8	8	-	Active Power Event	2.11	-
5	158	Cap Bank Closed	Bus 9	9	10	Reactive Power Event	0.20	0.12
6	168	Three Phase fault	Bus 10	10	9	Fault Event	48.06	26.86
8	179	Cap bank Opened	Bus 9	9	10	Reactive Power Event	0.24	0.16
8	188	P load increased	Bus 8	-	-	No Detection	-	-
9	198	Q load increased	Bus 8	8	9	Reactive Power Event	0.90	0.36
10	209	P load decreased	Bus 8	8	9	Active Power Event	2.07	0.72
11	219	Q load decreased	Bus 8	8	9	Reactive Power Event	1.15	0.62
12	229	Gen Drop	Bus 2	2	-	Active Power Event	2.73	-

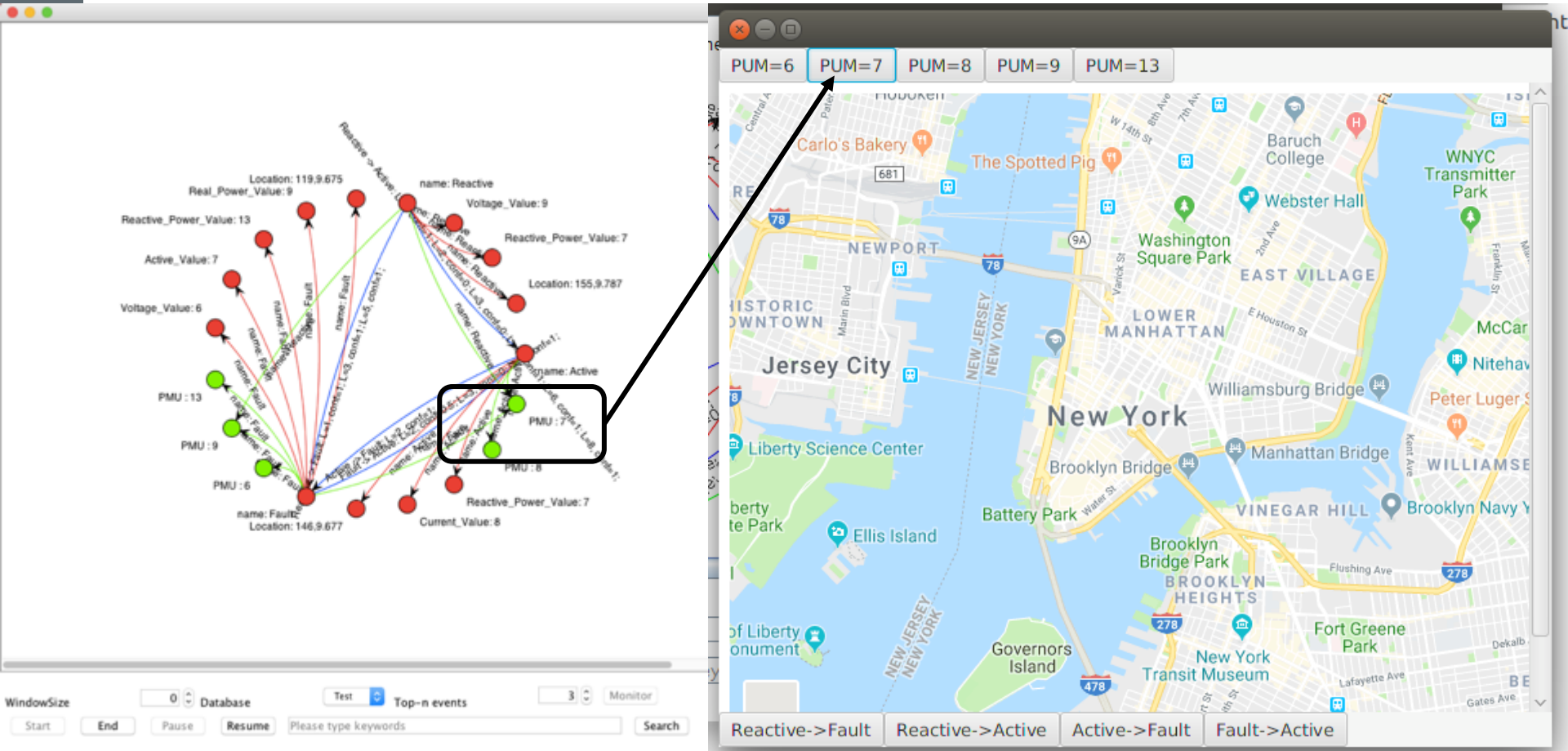
Events Details – Case 2

Sno.	Time (s)	Bus	Events	Voltage
1	109	9	Cap bank Closed	Up
2	119	13	3 Phase fault	Down
3	132	9	Cap bank Removed	Down
4	148	8	P load decreased	Up
5	158	9	Cap bank Closed	Up
6	168	13	3 Phase fault	Down
7	178	9	Cap bank Removed	Down
8	188	8	P load increased	Down
9	198	8	Q load increased	Down
10	209	8	P load increased	Down
11	219	8	Q load decreased	Up
12	229	6	Tap Down	Down
13	240	13	3 Phase fault	Down
14	240	3	Cap Bank closed	Up
15	253	6	Tap Up	Up
16	263	2	GenDrop	Down

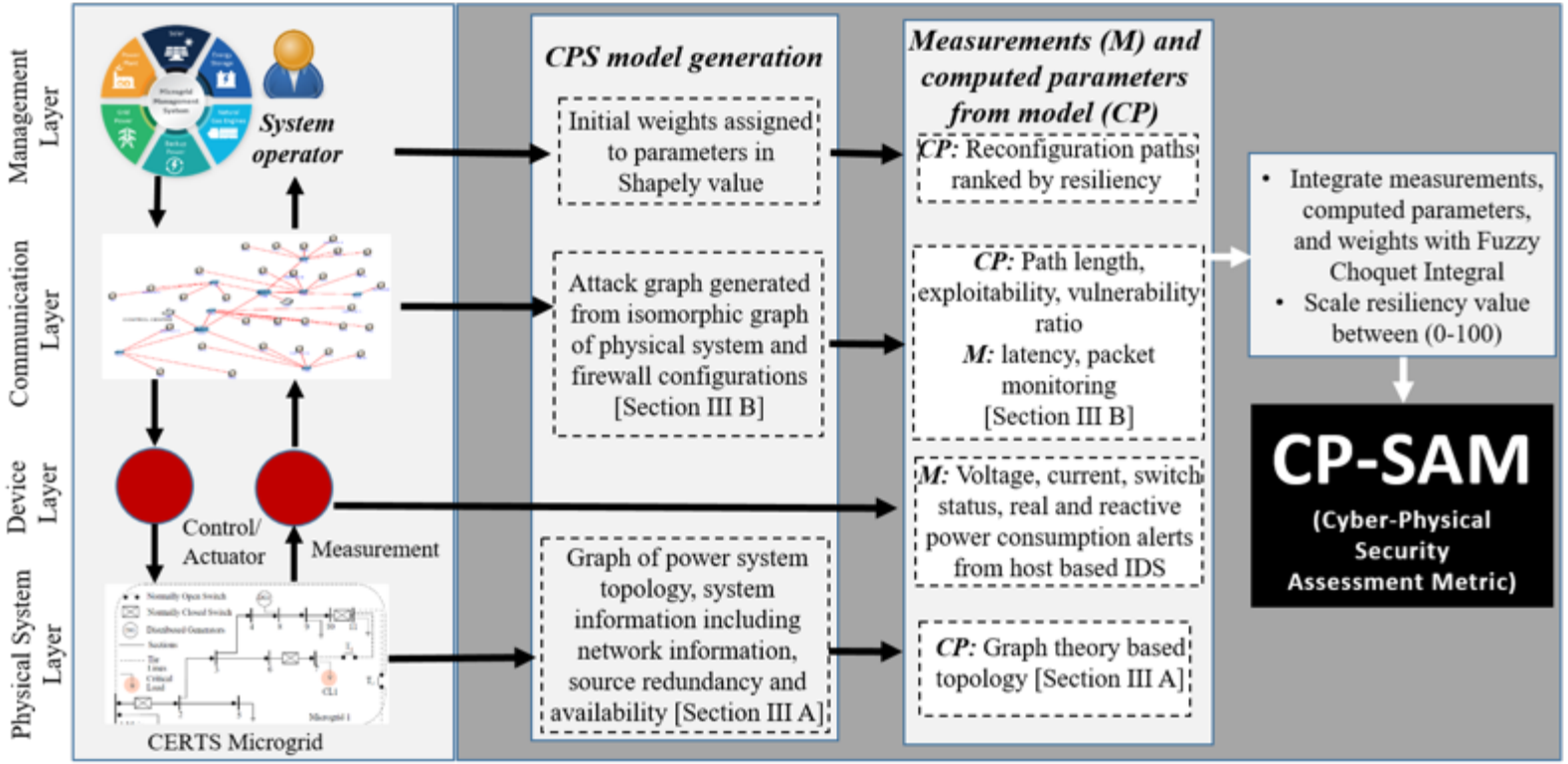
Results- Case 2

S No.	Time (s)	Actual Event	Actual Location	Detection Bus		Classified Event	Normalized Score	
				PMU 1	PMU 2		PMU 1	PMU 2
1	109	Cap Bank Closed	Bus 9	9	7	Reactive Power Event	2.15	2.11
2	119	Three Phase fault	Bus 13	13	9	Fault Event	26.56	11.09
3	132	Cap Bank Opened	Bus 9	9	7	Reactive Power Event	1.89	1.84
4	148	P load decreased	Bus 8	7	-	Active Power Event	2.61	-
5	158	Cap Bank Closed	Bus 9	9	7	Reactive Power Event	2.26	2.25
6	168	Three Phase fault	Bus 13	13	9	Fault Event	40.32	12.92
8	179	Cap bank Opened	Bus 9	9	7	Reactive Power Event	1.58	1.57
8	188	P load increased	Bus 8	-	-	No Detection	-	-
9	198	Q load increased	Bus 8	7	9	Reactive Power Event	0.74	0.67
10	209	P load decreased	Bus 8	7	9	Active Power Event	2.71	0.68
11	219	Q load decreased	Bus 8	7	9	Reactive Power Event	0.85	0.79
12	229	Tap Down	Bus 6	6	-	Reactive Power Event	0.62	-
13	240	Three Phase Fault	Bus 13	13	9	Fault Event	20.72	15.37
14	240	Cap bank closed	Bus 3	-	-	No Detection	-	-
15	253	Tap Up	Bus 6	6	13	Reactive Power Event	0.68	0.51
16	263	Gen Drop	Bus 2	2	-	Active Power Event	2.06	-

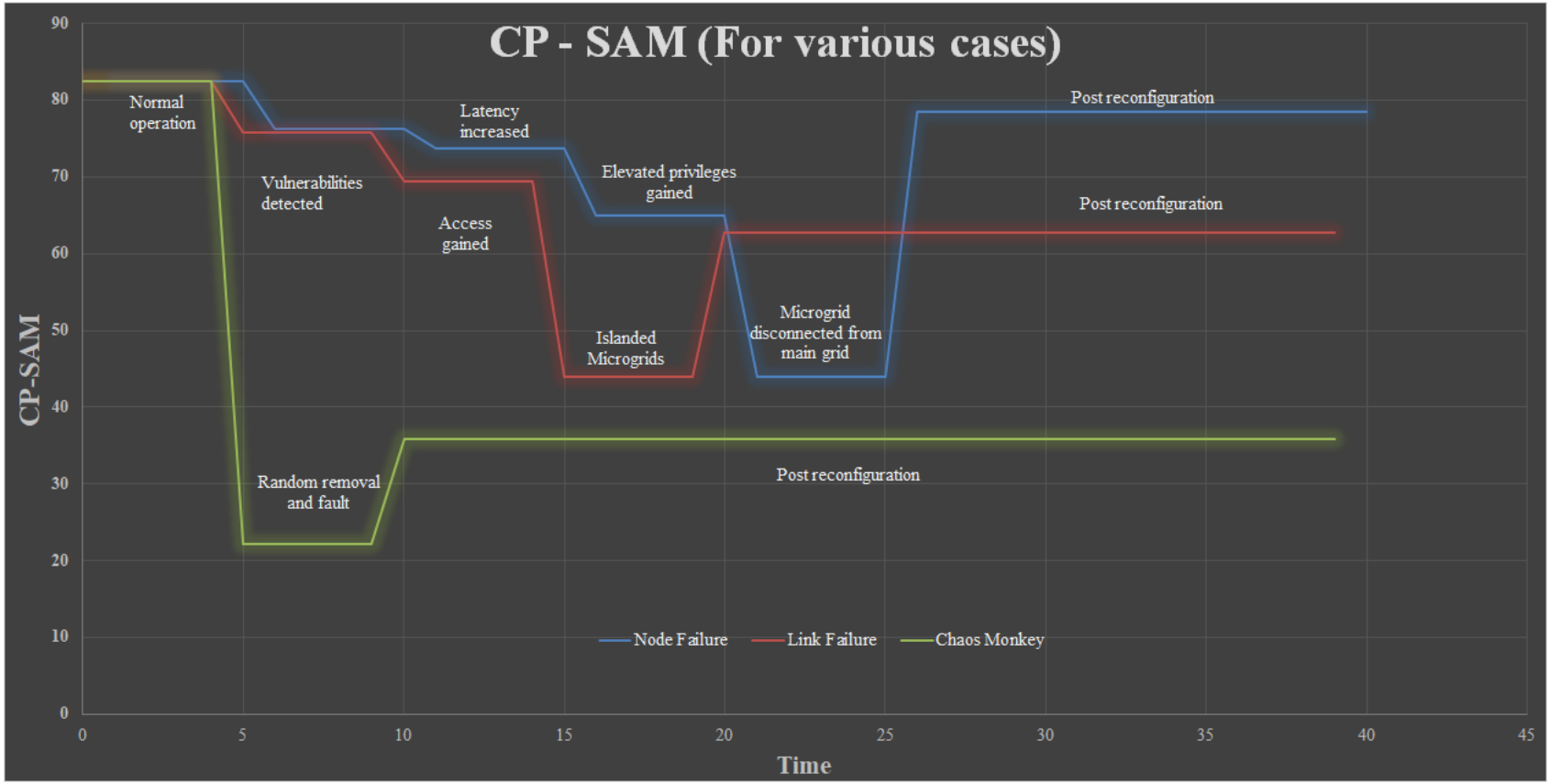
Map and Graph Interaction (google map)



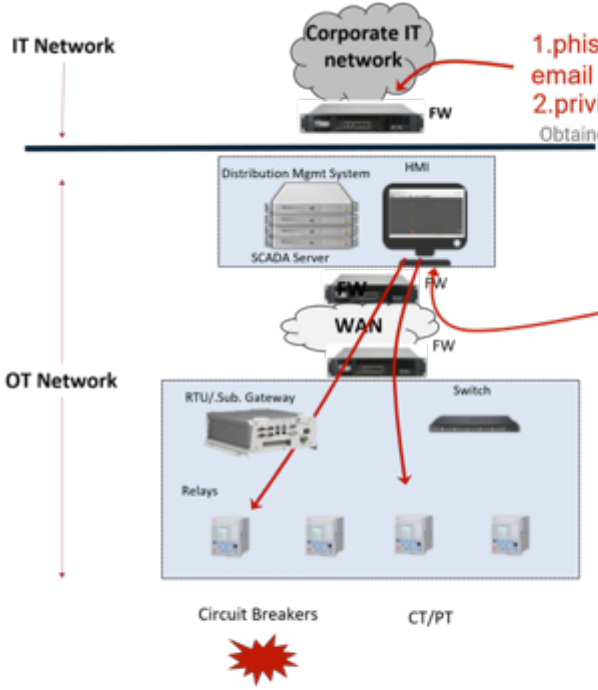
Cyber-Physical Security Assessment Metric (CP-SAM)



CP-SAM for Chaos Monkey (Netflix) and Other Events



Cyber-physical Analytics for Ukraine Attack



225,000 customers without power

IT

1.phishing email to IT network

2.privilege escalation

Obtained admin on DC

OT Pre-Impact

3.ot vpn login

Stolen credential from DC used to remotely login to vpn

4.install malware

BlackEnergy malware installed on control systems

5.remote hmi session

Created remote operators session to SCADA server

6.trip breakers

Operate key circuit breakers, 225,000 customers offline

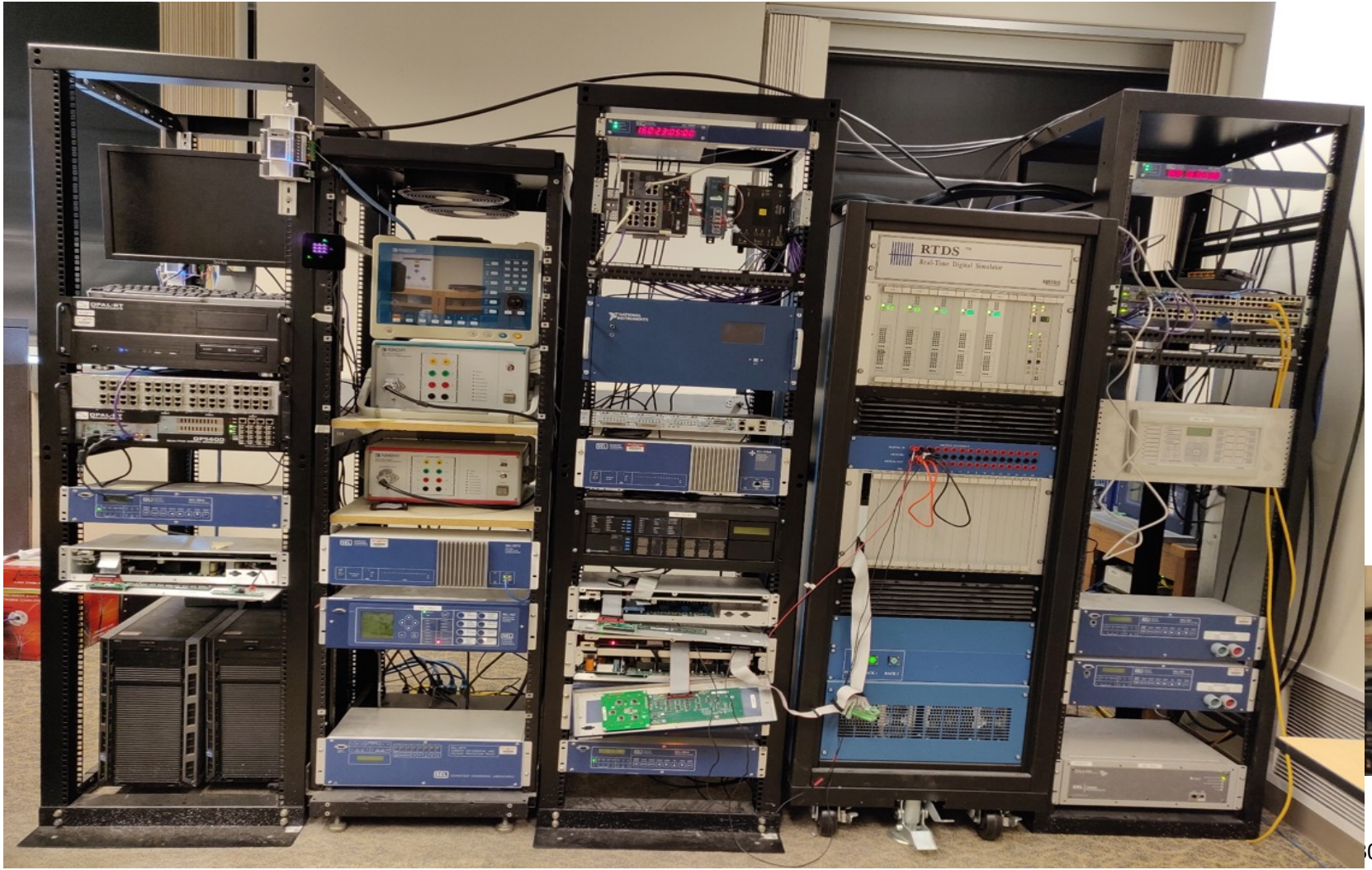
OT Post-Impact

7.disable systems

Wipe SCADA servers, brick serial-ethernet converts and control center ups

8.telephone ddos

Telephone DDoS prevents communication about grid state


RTDS
Real-Time Digital Simulator

Testbed

Power System

- Real-Time emulation tools including RTDS and OPAL-RT

Communication System

- Emulation tools such as CORE, DeterLab

Security Tools

- Device and host level attack implementation and analysis

TCP/IP, Remote Encapsulation, Hardware

TCP/IP, libpcap, attack libraries

- Offline simulation tools

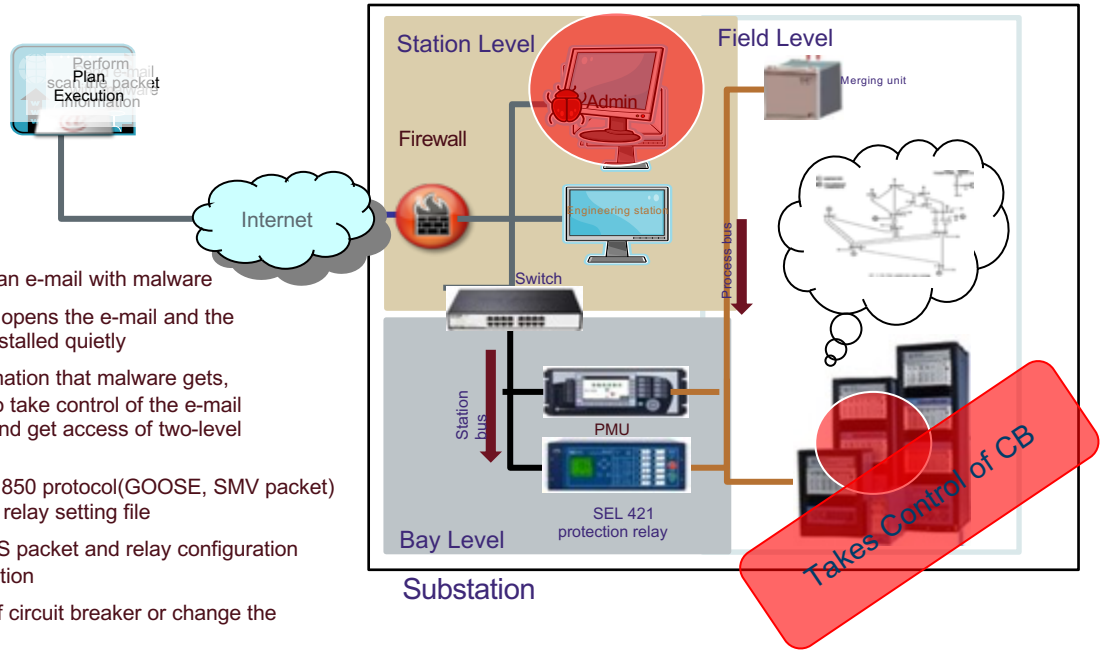
- Simulation tools such as NS-3, Mininet

- Network level simulation of attacks

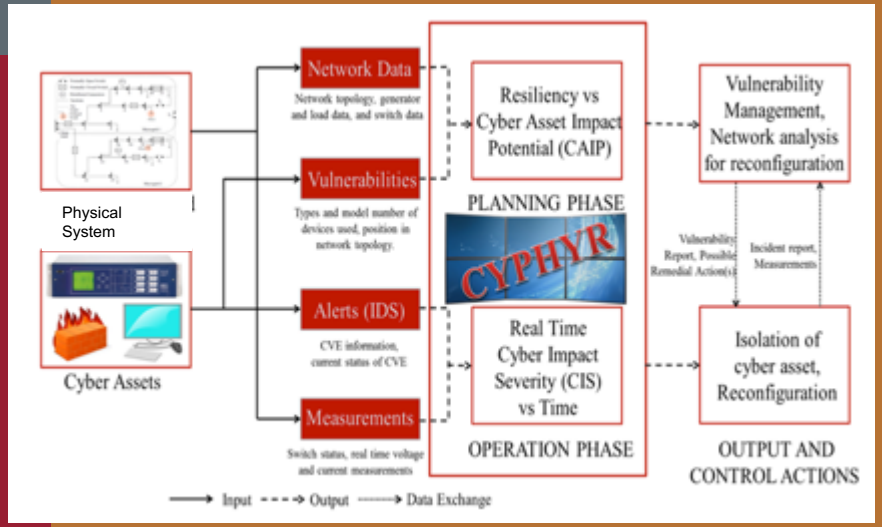
IPC, TCP/IP, Remote Encapsulation

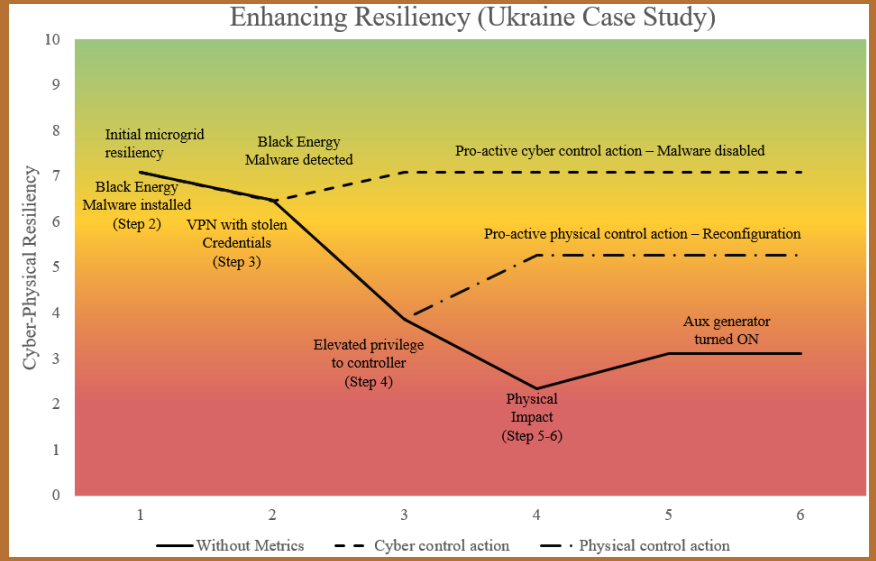
Proxy interface, attack implementations

Simulating Ukraine Attack



1. Attacker sends an e-mail with malware
2. E-mail recipient opens the e-mail and the malware gets installed quietly
3. Using the information that malware gets, hacker is able to take control of the e-mail recipient's PC and get access of two-level password
4. Analysis IEC 61850 protocol(GOOSE, SMV packet) information and relay setting file
5. Manipulate MMS packet and relay configuration session information
6. Takes control of circuit breaker or change the setting of relay



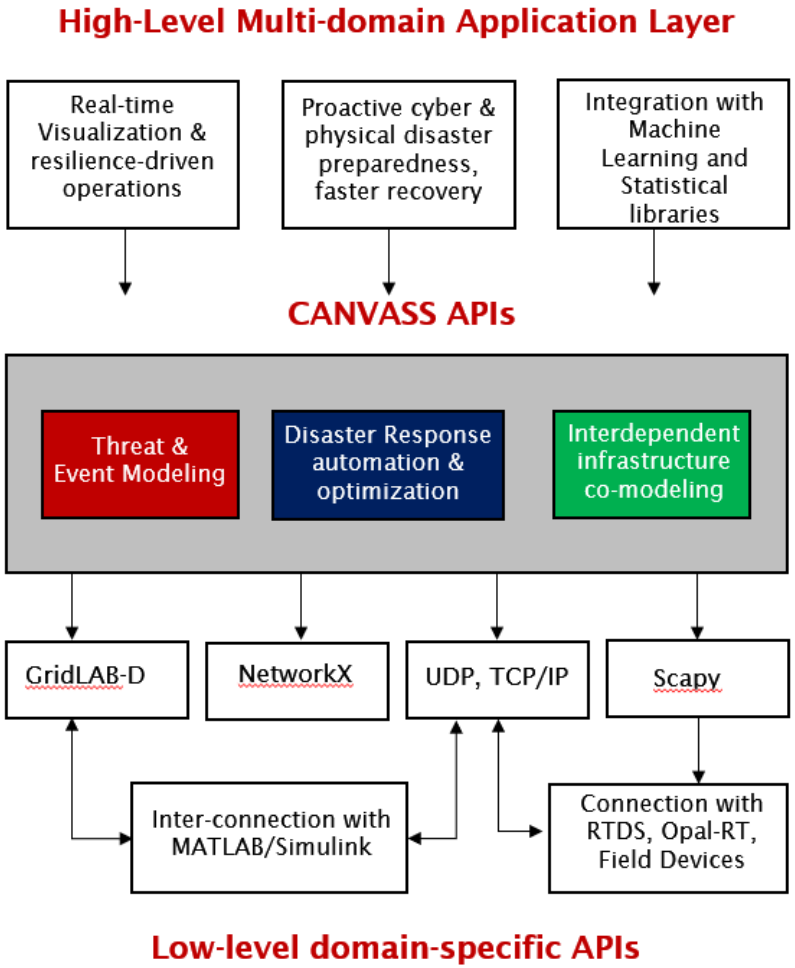


CyPhyR: Cyber-Physical Resiliency Tool

CANVASS?

- Canvass stands for Cyber-Attacks and Network Vulnerability Analytics Software for Smart Grids
- It enables unfavorable physical and cyber event simulation for power systems
- **Free, open-source, platform-independent resiliency-computation toolkit**
- It has default restoration and resiliency computation algorithms – with ability for user to define own metrics and scenarios.
- It enables easy power system modeling and inter-disciplinary resiliency engineering research by abstracting lower level (hard-to-learn) open-source:
  - power simulation software [GridLAB-D],
  - network analysis library [NetworkX],
  - OS-based socket libraries [TCP/IP]
  - Packet Manipulation library [ScaPy]

  into a single, easy-to-use Python package.
- Multiple interdependent infrastructure modeling, such as cyber-physical power grid, along with crew transport network.
- It can interface with Real-Time Simulation software through socket programming.



https://sgdril.eecs.wsu.edu/research-interests-and-grants/industrial-grade-products/pycanvass/

City of Cordova
ALASKA

NRECA
America's Electric Cooperatives

INL
Idaho National Laboratory

SIEMENS

Sandia National Laboratories

Pacific Northwest
NATIONAL LABORATORY

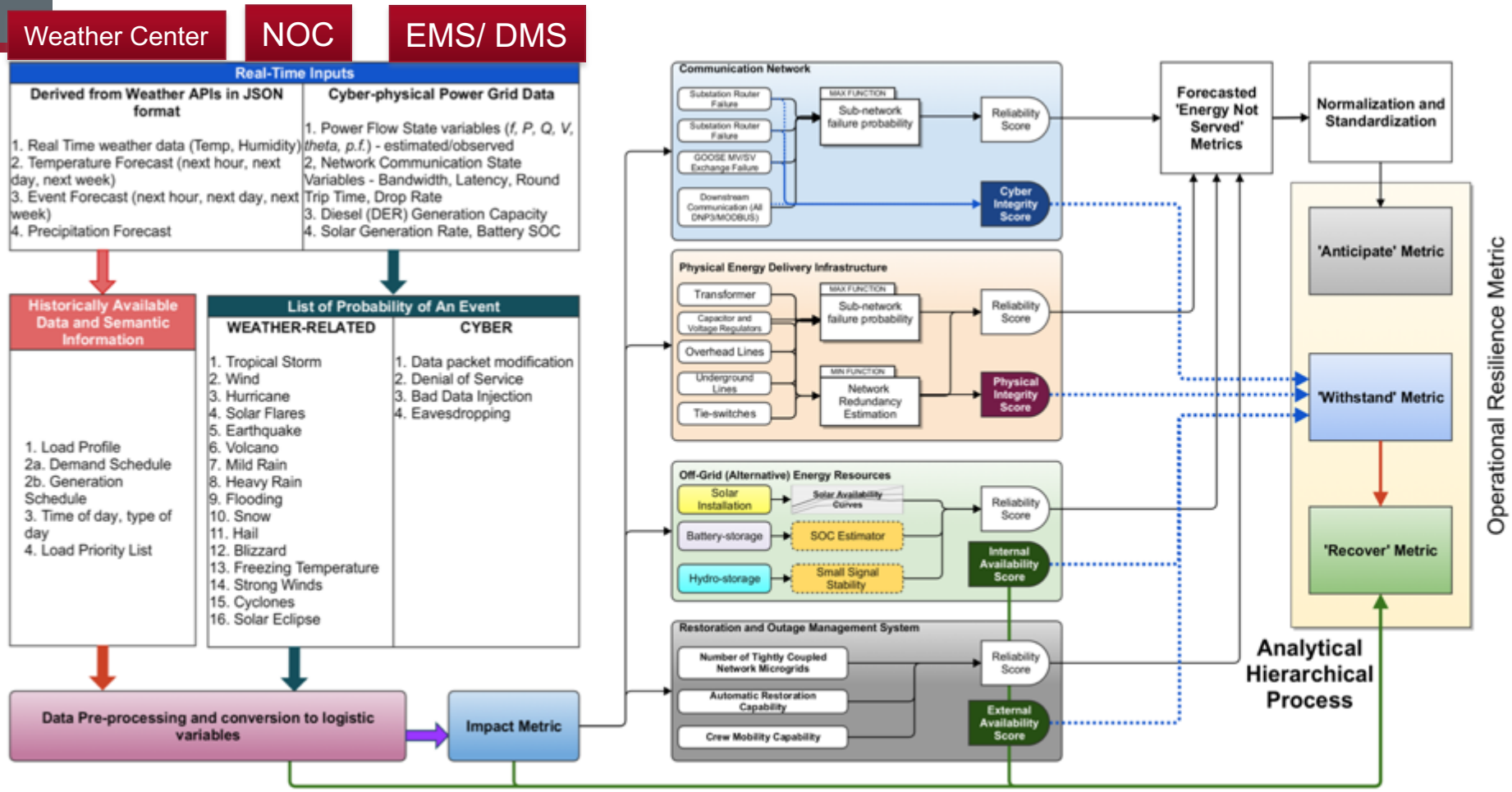
NRECA
America's Electric Cooperatives

ACEP
Alaska Center for Energy and Power

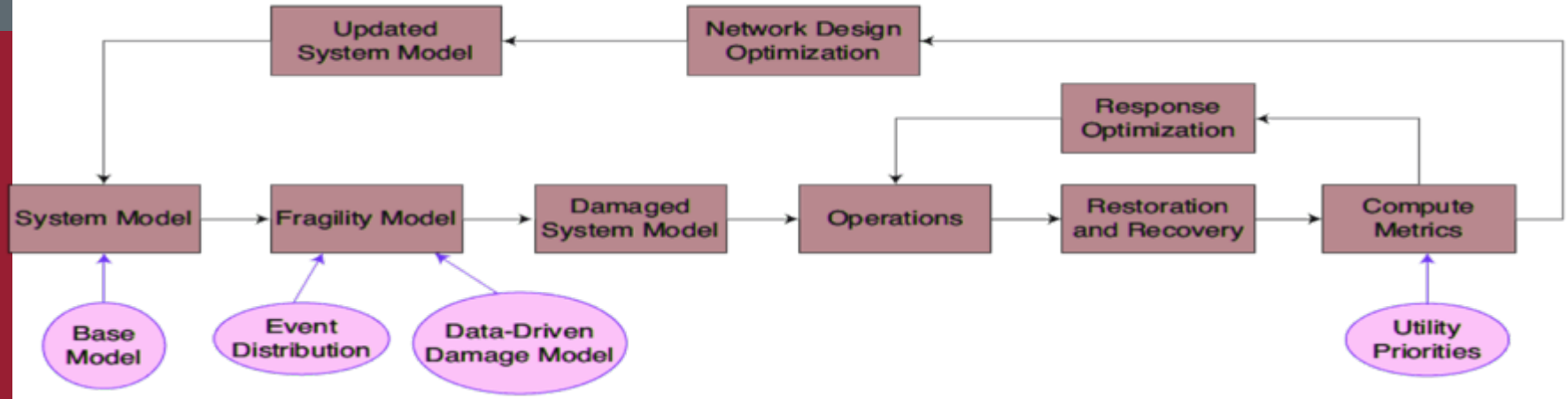
FLORIDA STATE UNIVERSITY 1851

NM STATE UNIVERSITY

Measuring Resiliency in Alaska



Enabling Resilient Smart Grid



By System Design:

- Redundancy and system approach
- Embedding resiliency concepts in operational and planning practice
- Automation, flexibility, adaptability, and physical network switching and hardening
- Resilient Communication Networking
- Providing incentive for resiliency

By Cyber Security and Weather Resistance Measure:

- Cyber-Physical Threat Detection
- Integrated Defense Plan

By Robust Computing and Data Analytics:

- Distributed coordination
- Centralized, decentralized, distributed

By Robust Mathematical Algorithm and Robust Control:

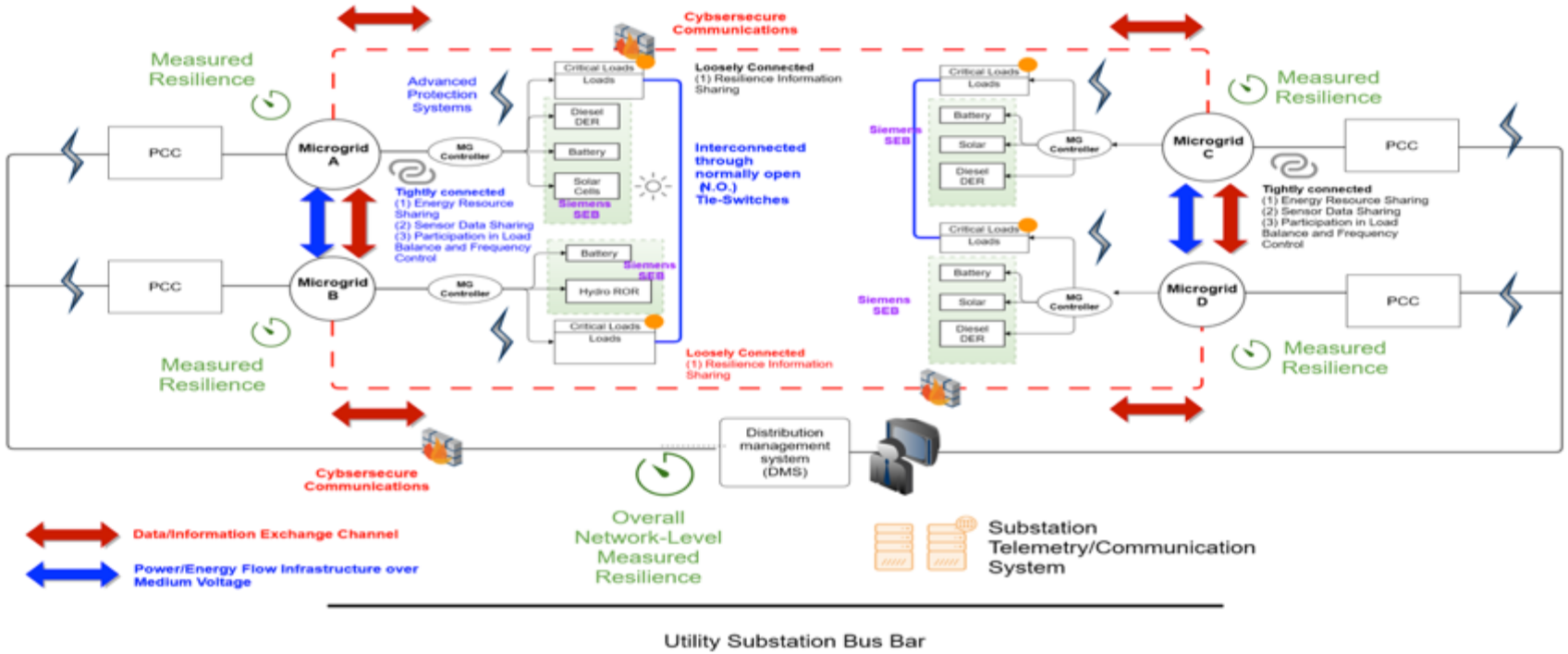
- Distributed optimization
- Robust convergence and time guarantee
- Distributed coordination for RAS

By Physical System Measure:

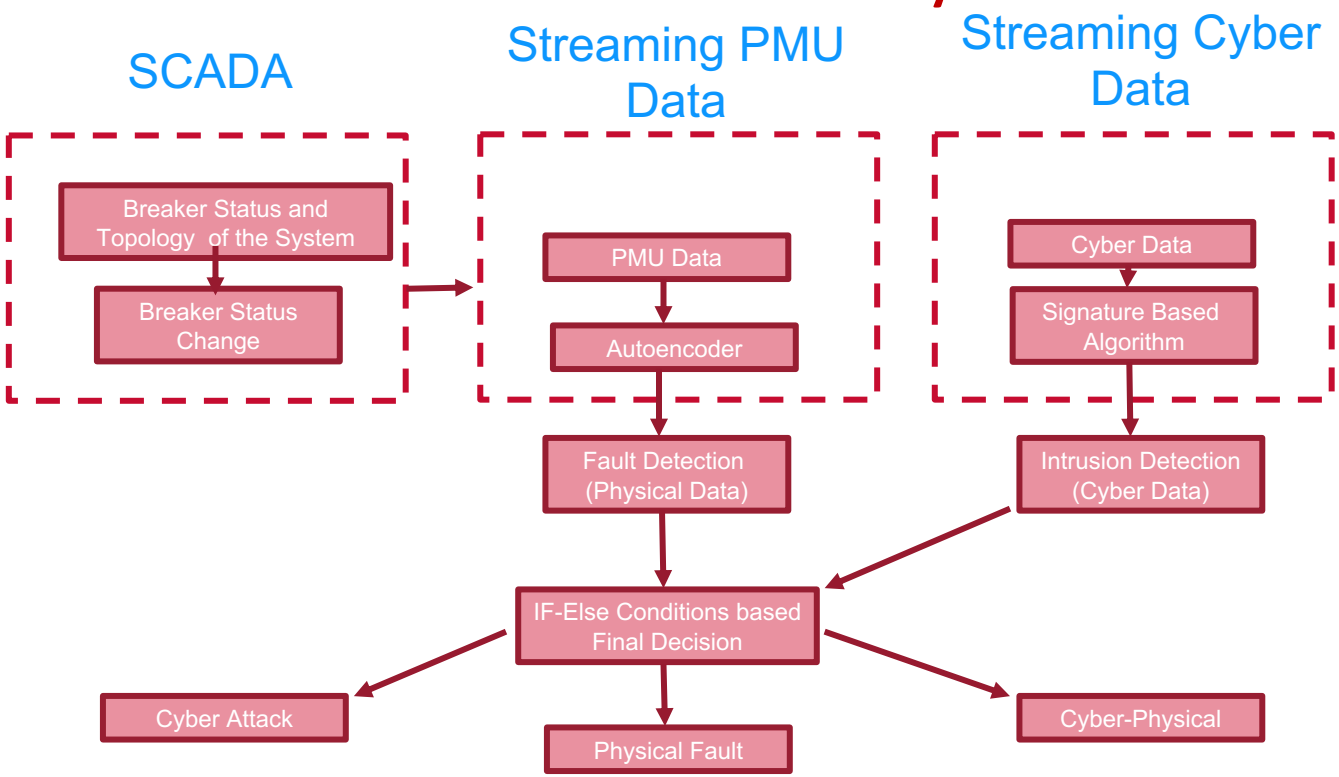
- Reconfiguration and resource allocation
- Controlled islanding

Example: Microgrid/ DERs based restoration During contingencies

- **ML based cold load pickup estimation, behind the meter DER estimation, MEMS and ADMS coordination, proactive/ corrective control, centralized/decentralized/ distributed voltage control and energy management**



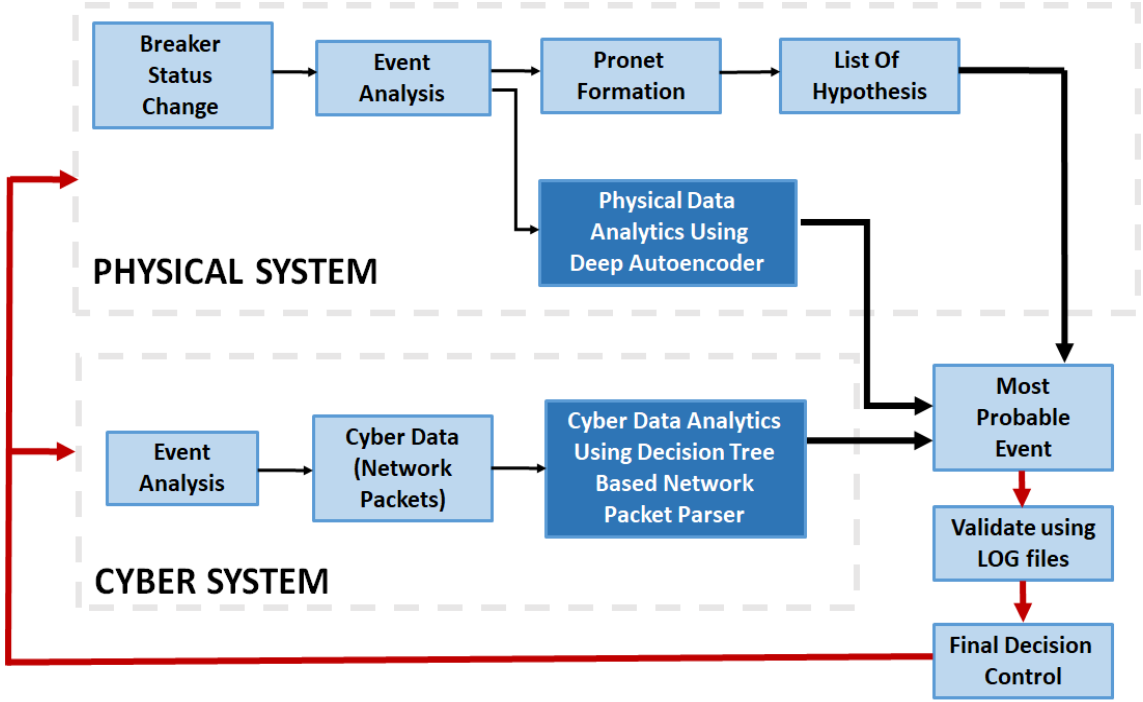
Example: Cyber-physical Data Analytics For Event Classification in Protection System



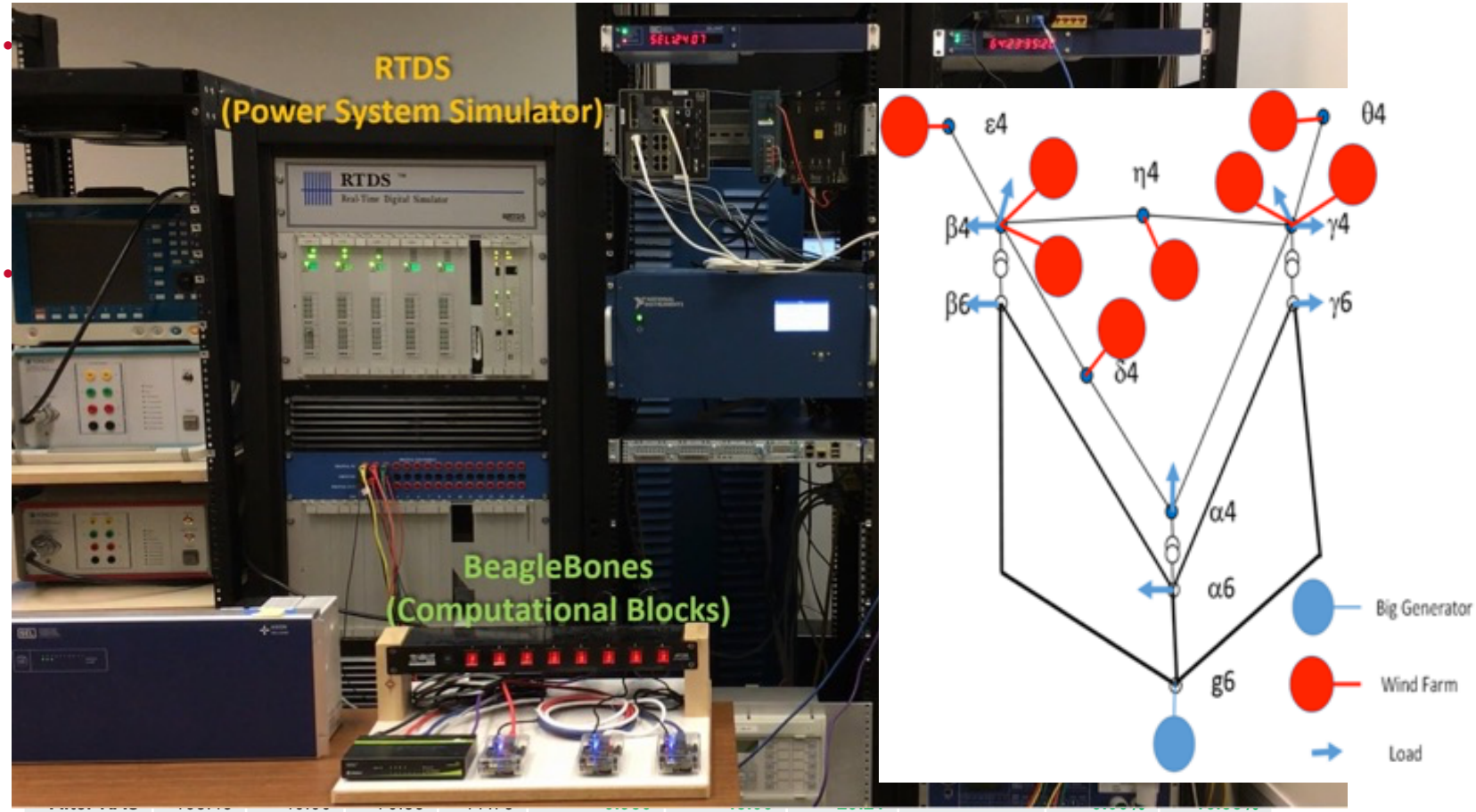
Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems

Example: Cyber-physical Data Analytics in Protection Failure

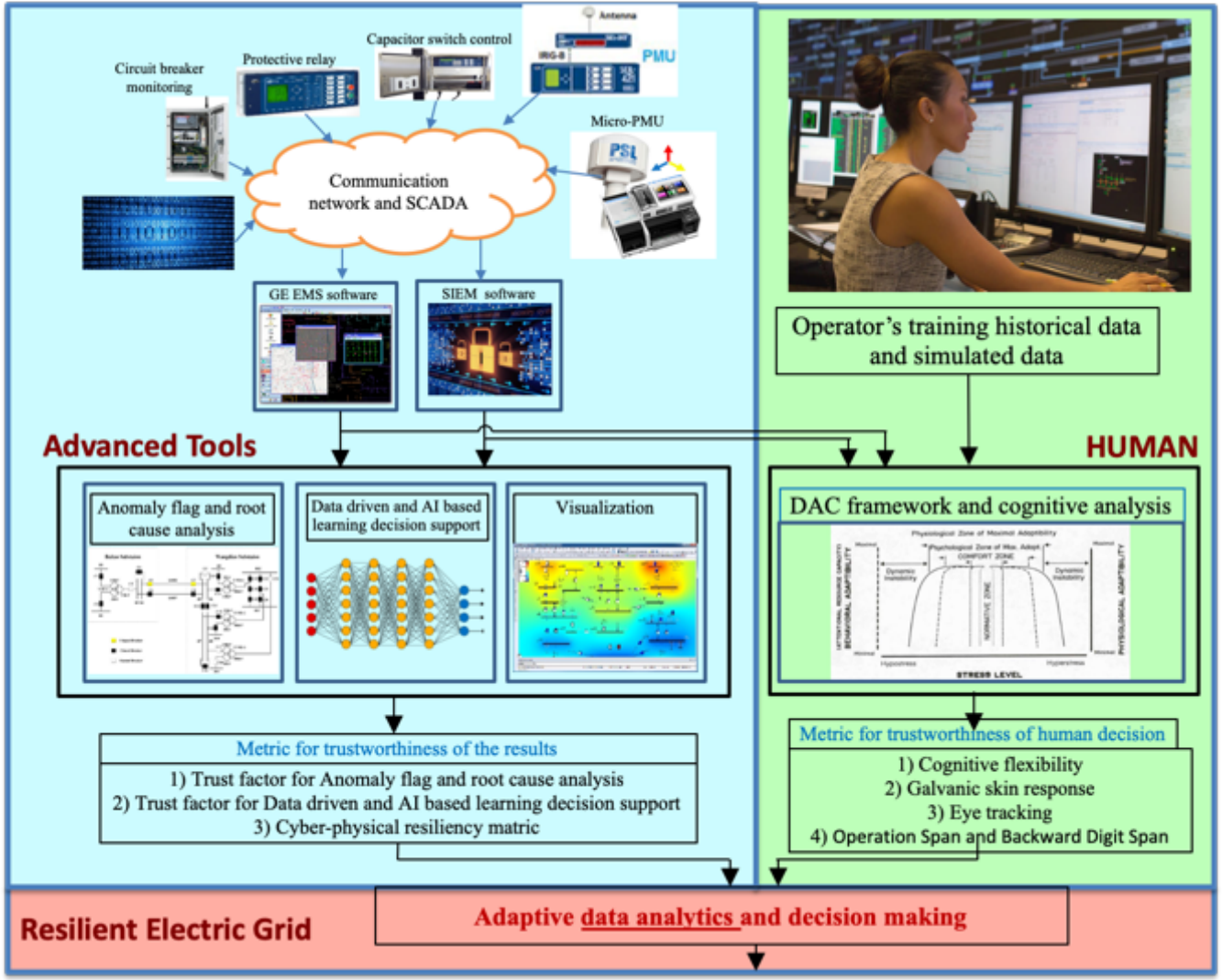
- Protection Mal-operation is #1 concern according to NERC
- Protection and associated control is becoming more digital

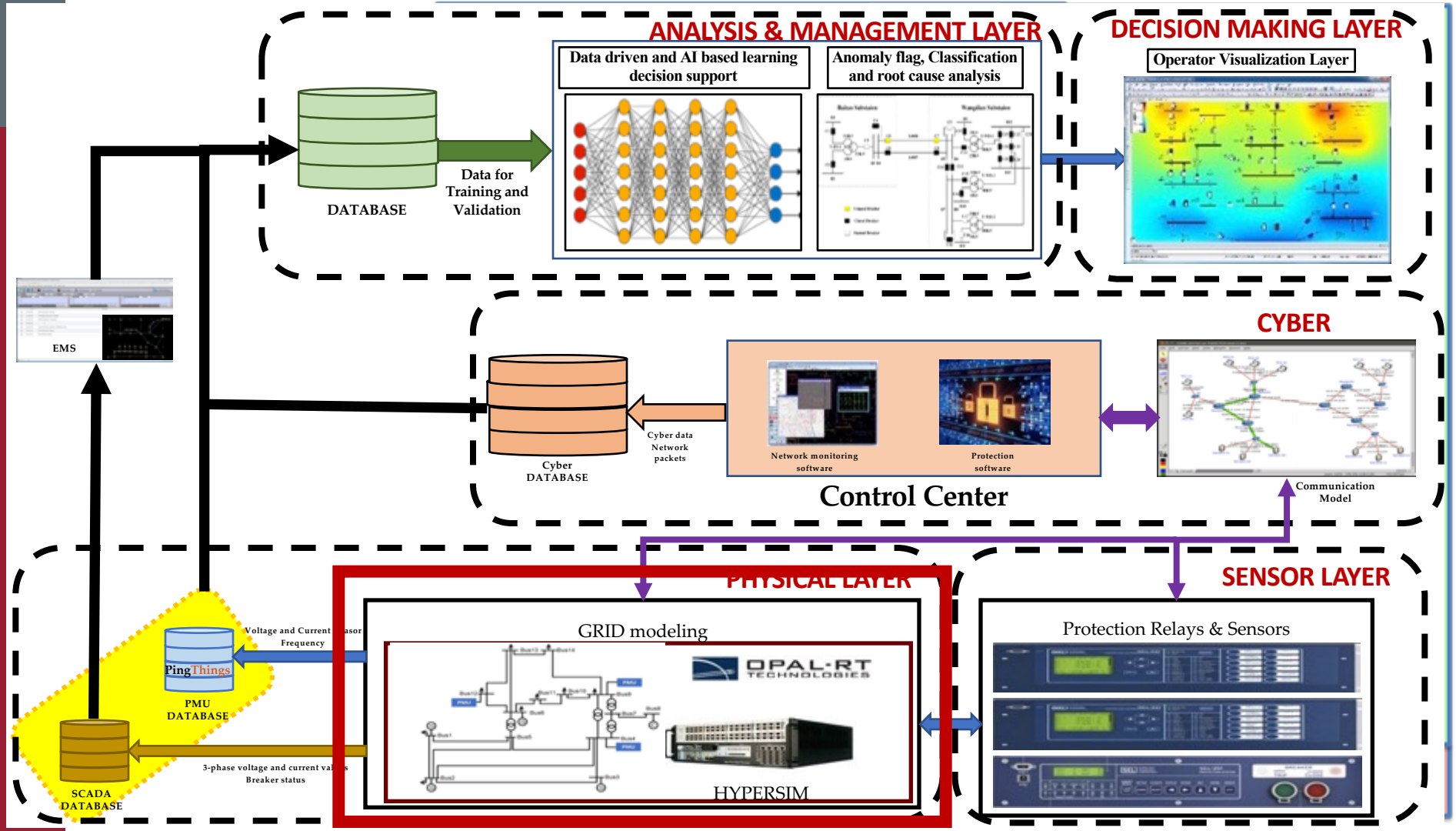


Example: RAS based Wind Curtailment



Cyber-Physical-Human Resiliency Analysis for Extreme Events (With PNNL)

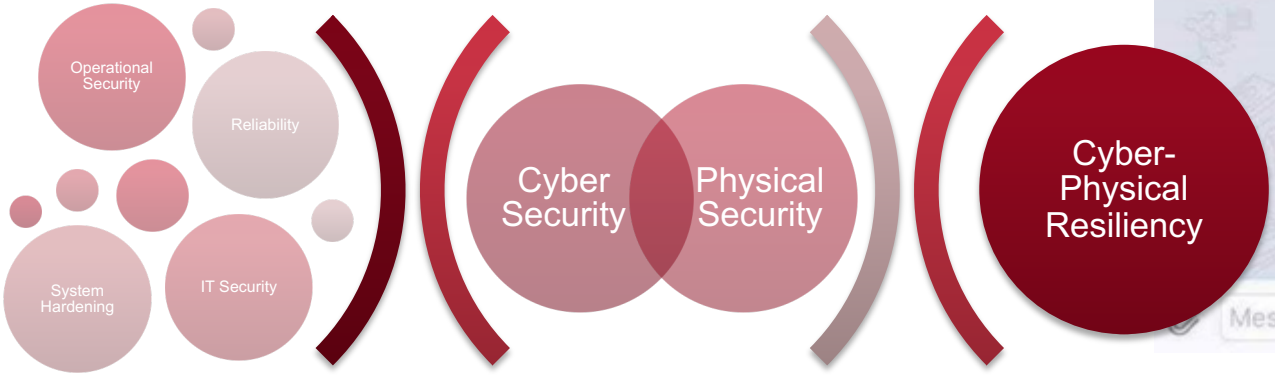



ANALYSIS & MANAGEMENT LAYER
DECISION MAKING LAYER
Operator Visualization Layer
Data driven and AI based learning decision support
Anomaly flag, Classification and root cause analysis
DATABASE
Data for Training and Validation
EMS
CYBER
Cyber DATABASE
Cyber data Network packets
Network monitoring software
Protection software
Control Center
Communication Model
PHYSICAL LAYER
SENSOR LAYER
Voltage and Current Phasor Frequency
PingThings
PMU DATABASE
SCADA DATABASE
3-phase voltage and current values Breaker status
GRID modeling
OPAL-RT TECHNOLOGIES
HYPERSIM
Protection Relays & Sensors

Research Problem #1: Shift in Grid Cyber Security Practices

- Murphy's Law of Security
  - Law 1: "Whatever that can be hacked, will be hacked."
  - Law 2: "Anything worth hacking has already been hacked (we just don't know about them yet)"

PJM reports around 4,000+ cyber attacks every month
- T. Boston, Former CEO PJM



Research Problem #2: Resiliency is a Complex Problem

Power Grid Resiliency = **Flexible Infrastructure** ⊗ **Secure Cyber Infrastructure** ⊗ **Resilient Power Control Applications**

Flexible Infrastructure

- **Multiple switch**
- **Macrogrid**
- **Minigrid**
- **Microgrid**
- **Nanogrid**
- **Graceful disintegration and interconnection**
- **Flexible management and control of resources**
- **Economic and market incentive**

Secure Cyber Infrastructure

Communication
- Authentication
- Encryption

Computation
- Access control
- Attestation
- Forensics
- Patch management
- Software Audits

System Management
- Intrusion Detection
- Event Monitoring/Analytics
- Security Assessment

Resilient Power Control Applications

Generation
- Automatic Generation Control
- Governor Control
- Automatic Voltage Regulation
- Protection

Transmission
- State Estimation
- VAR Compensation
- Protection

Distribution
- Load Shedding
- Protection
- Advanced Metering Infrastructures

- Resiliency metric is a MCDM problem
- Resiliency is characteristics of the system
- Resiliency management system need to be integrated and validated with large scale simulation

Research Problem #3: Physics-driven Data Analytics/ ML Techniques and finding suitable applications

- Data Analytics and machine learning approaches needs to be applied after analyzing the power system problem carefully. Finding match between machine learning strength and power system problem to be solved is important.
- Machine learning is only applicable in data-rich problems if no system model is available (e.g. forecasting)
- If model is available with rich data set, typically it will be two step approach: apply machine learning to narrow down your possible options and refine it with model based approach (e.g. event detection)
- Machine learning will not give a good results based on state of the art for highly complex and dynamic problems (e.g. transient stability, contingency analysis).
- Validation and metric is important for these evolving solution technologies

- Physics based model driven and existing power system operational algorithm need to be revisited with power electronics based DERs, active distribution system/ microgrids
- Existing practice of measurements based on SCADA and PMU, waveform capturing
- Not best but best possible evolving solutions

Most important threat

- The most important threat to the power grid is a force of nature - http://cybersquirrel1.com/

- Humans have to catch up…

TOTAL SUCCESSFUL CYBER WAR OPS
AS OF 2019.01.21 - 2524

Agent	Success
Squirrel	1252
Bird	639
Snake	117
Raccoon	115
Rat	53
Cat	28
Marten	25
Jellyfish	13
Monkey	12
Human	3*

Thank You

Acknowledgement: My Research Group, My collaborators, PNNL and my funding agencies.

Anurag K. Srivastava

anurag.k.srivastava@wsu.edu

https://www.youtube.com/channel/UCJvYOVqPi-vM7nmR4qSxpmQ/videos

https://sgdril.eecs.wsu.edu