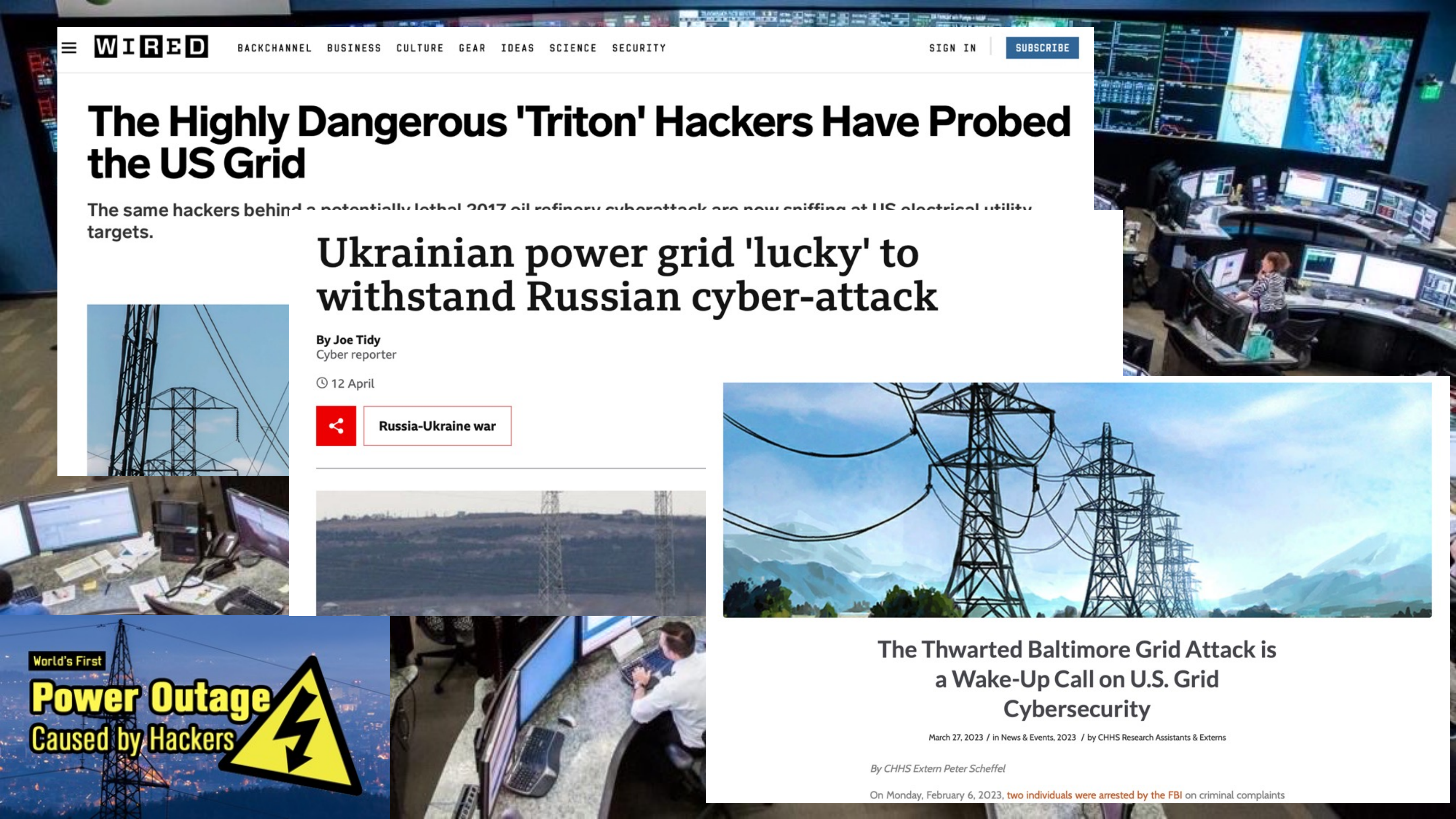
Enabling Cyber-Power Grid Security and Resiliency

Prof. Anurag K Srivastava
Raymond J. Lane Professor and Chairperson,
Lane Department of Computer Science and Electrical Engineering
Director, Smart Grid REsiliency and Analytics Lab (SG-REAL)
West Virginia University, Morgantown, WV, USA

Adjunct professor, Washington State University

Senior Scientist, Pacific Northwest National Lab, Richland, WA

CIGRE Next Generation Network Webinar, August 17, 2023


WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY
SIGN IN
SUBSCRIBE
The Highly Dangerous 'Triton' Hackers Have Probed the US Grid
The same hackers behind a potentially lethal 2017 oil refinery cyberattack are now sniffing at US electrical utility targets.
Ukrainian power grid 'lucky' to withstand Russian cyber-attack
By Joe Tidy
Cyber reporter
12 April
Russia-Ukraine war
The Thwarted Baltimore Grid Attack is a Wake-Up Call on U.S. Grid Cybersecurity
March 27, 2023 / in News & Events, 2023 / by CHHS Research Assistants & Externs
By CHHS Extern Peter Scheffel
On Monday, February 6, 2023, two individuals were arrested by the FBI on criminal complaints
World's First
Power Outage
Caused by Hackers

What can we do about it?

Understand the Problem

1

Cyber Vulnerability and Threat

Cyber Threats, exposure, risk, analysis and Mitigation

Tools

2

Data- Driven Tools for Cybersecurity and Resiliency with IoT

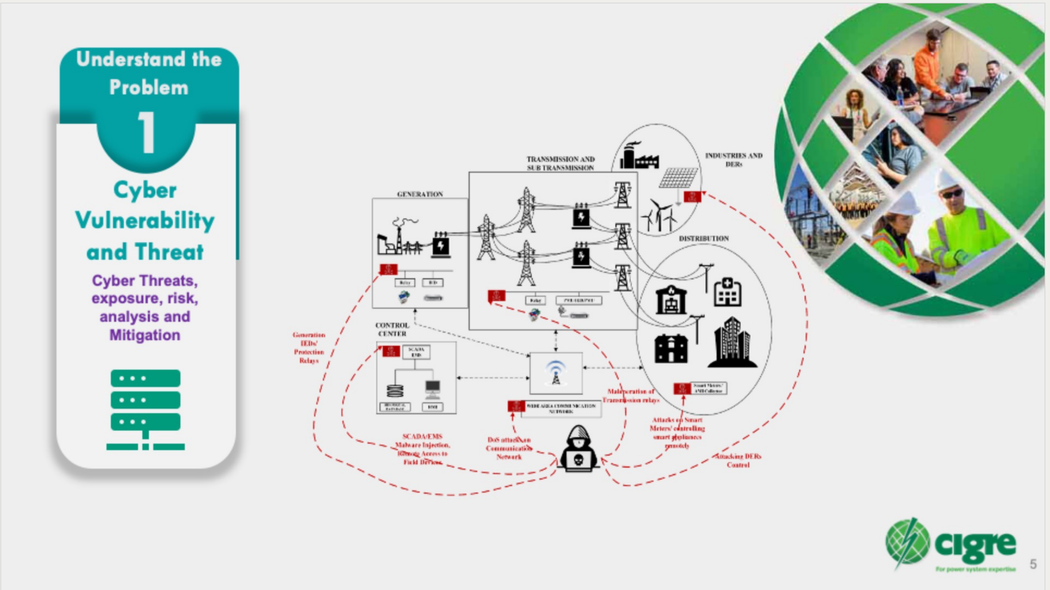
Metrics and algorithms for cyber anomaly detection, classification, localization, root cause analytics and resiliency analysis

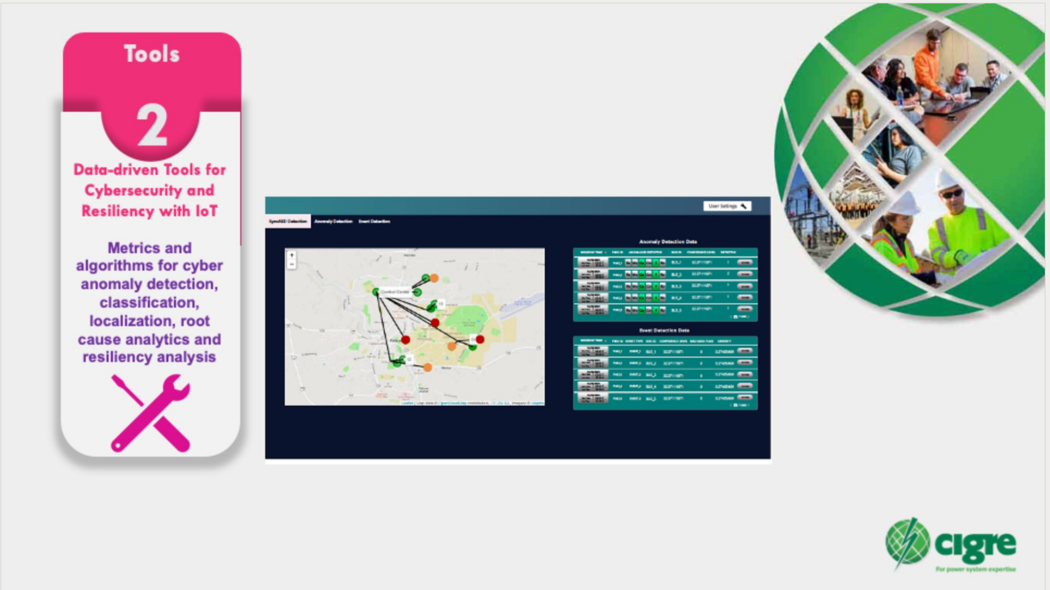
Testbed

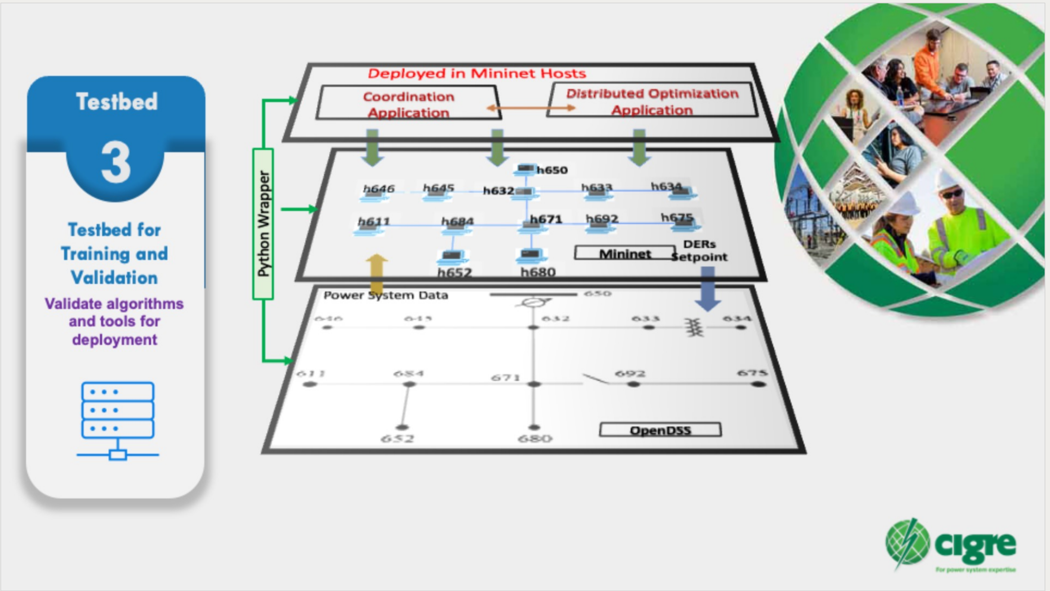
3

Testbed for Training and Validation

Validate algorithms and tools for deployment


Understand the Problem
1
Cyber Vulnerability and Threat
Cyber Threats, exposure, risk, analysis and Mitigation
GENERATION
TRANSMISSION AND SUB TRANSMISSION
INDUSTRIES AND DERs
DISTRIBUTION
CONTROL CENTER
cigre
5


Tools
2
Data-driven Tools for Cybersecurity and Resiliency with IoT
Metrics and algorithms for cyber anomaly detection, classification, localization, root cause analytics and resiliency analysis
cigre


Testbed
3
Testbed for Training and Validation
Validate algorithms and tools for deployment
Deployed in Mininet Hosts
Coordination Application
Distributed Optimization Application
Python Wrapper
h650
h646
h645
h632
h633
h634
h611
h684
h671
h692
h675
Mininet
DERs Setpoint
h652
h680
Power System Data
OpenDSS
cigre

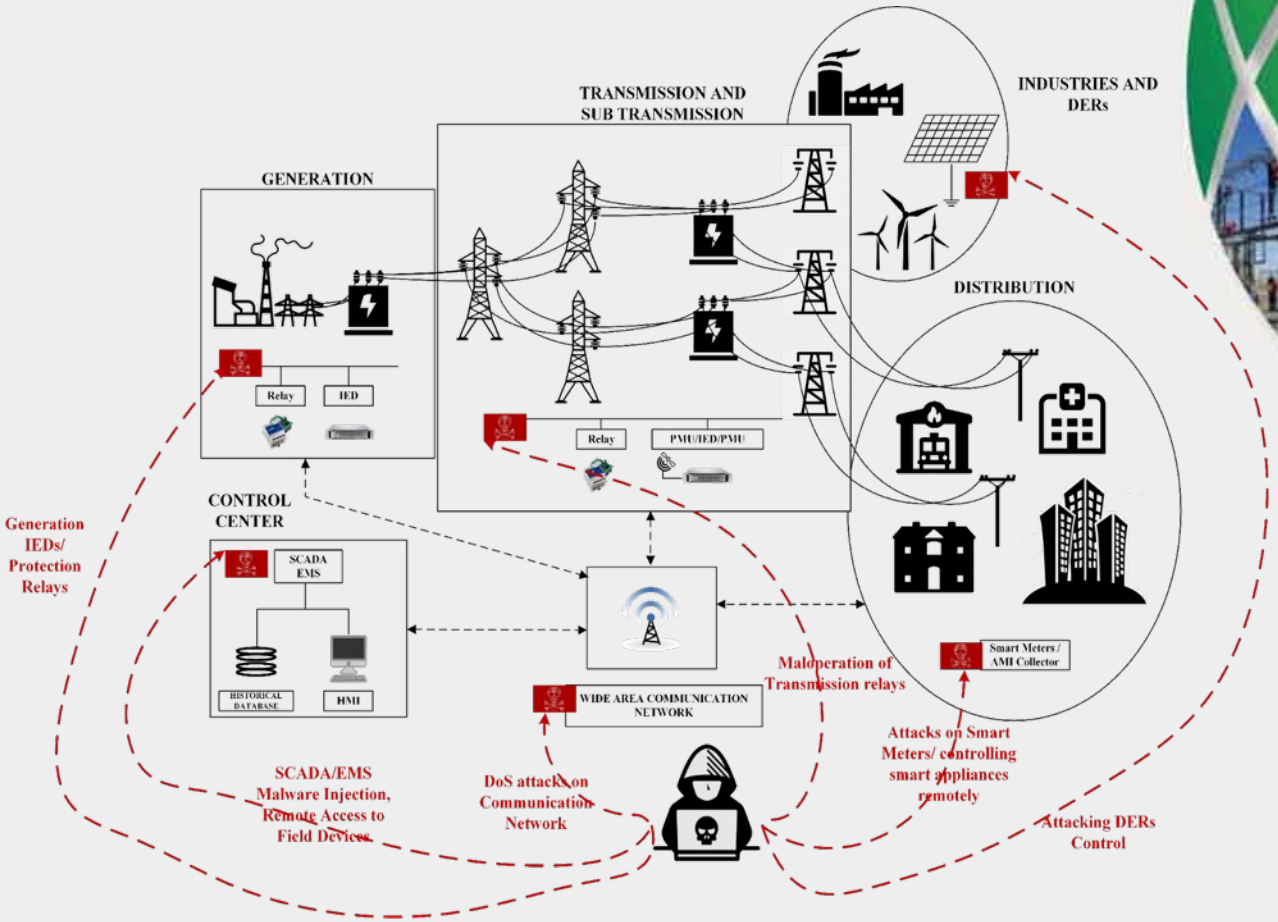

Summary
cigre

Understand the Problem

1

Cyber Vulnerability and Threat

Cyber Threats, exposure, risk, analysis and Mitigation



For power system expertise

Risk, Threats, and Vulnerabilities

- Threat – circumstance or event with the potential to adversely impact organizational operations
- Vulnerability – a weakness in an information system, system security procedures, internal controls, or an implementation that could be exploited by a threat source

Risk = Threat × Vulnerability × Impact

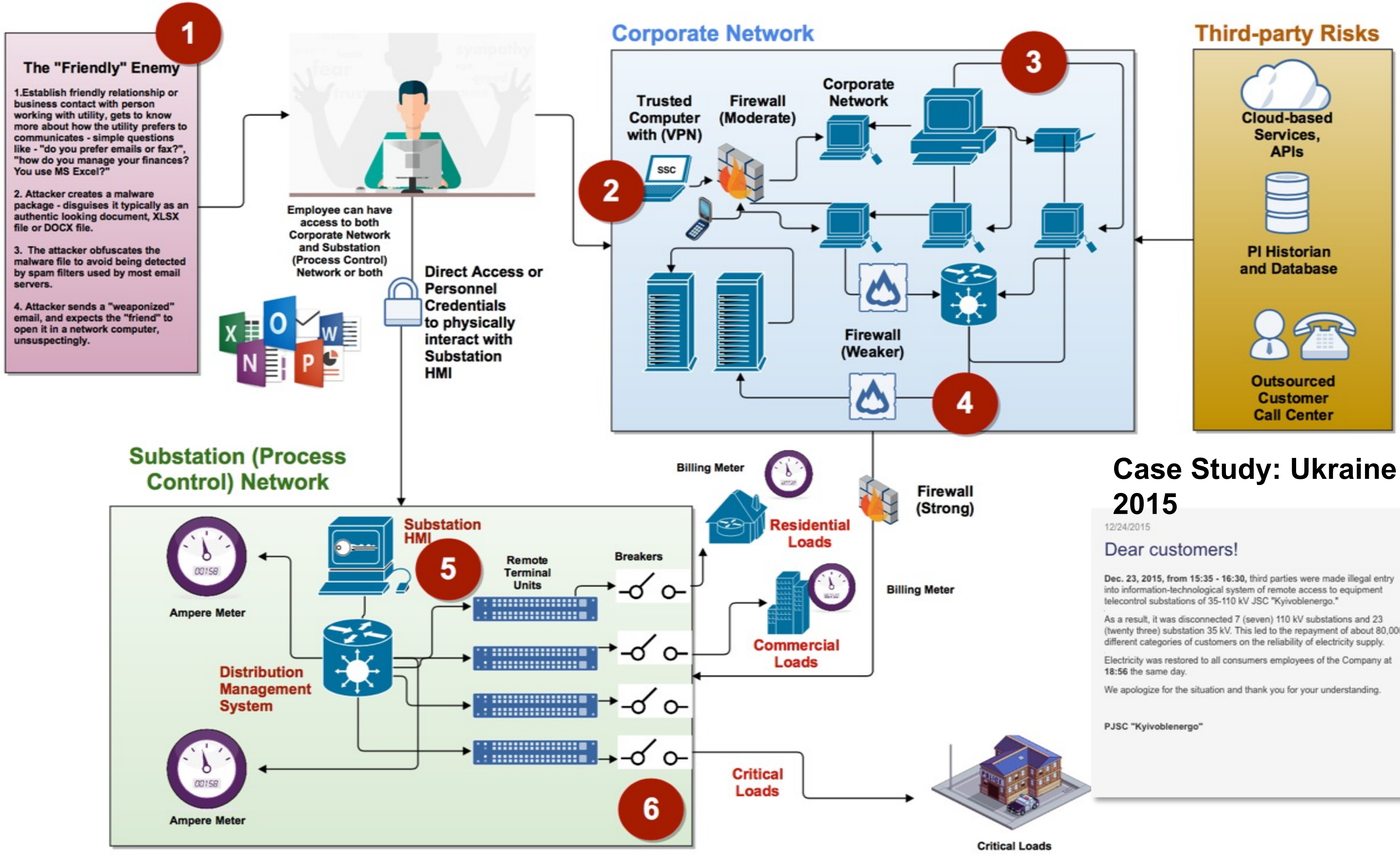
What's New??

Risk (2005) = ↓ Threat × ↑ Vulnerability × ↓ Impact

Risk (Today) = ↑ Threat × ↓ Vulnerability × ↑ Impact

Source: NIST SP 800-30, rev1. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Anatomy of a Cyber Attack



Case Study: Ukraine Cyber Attack 2015

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

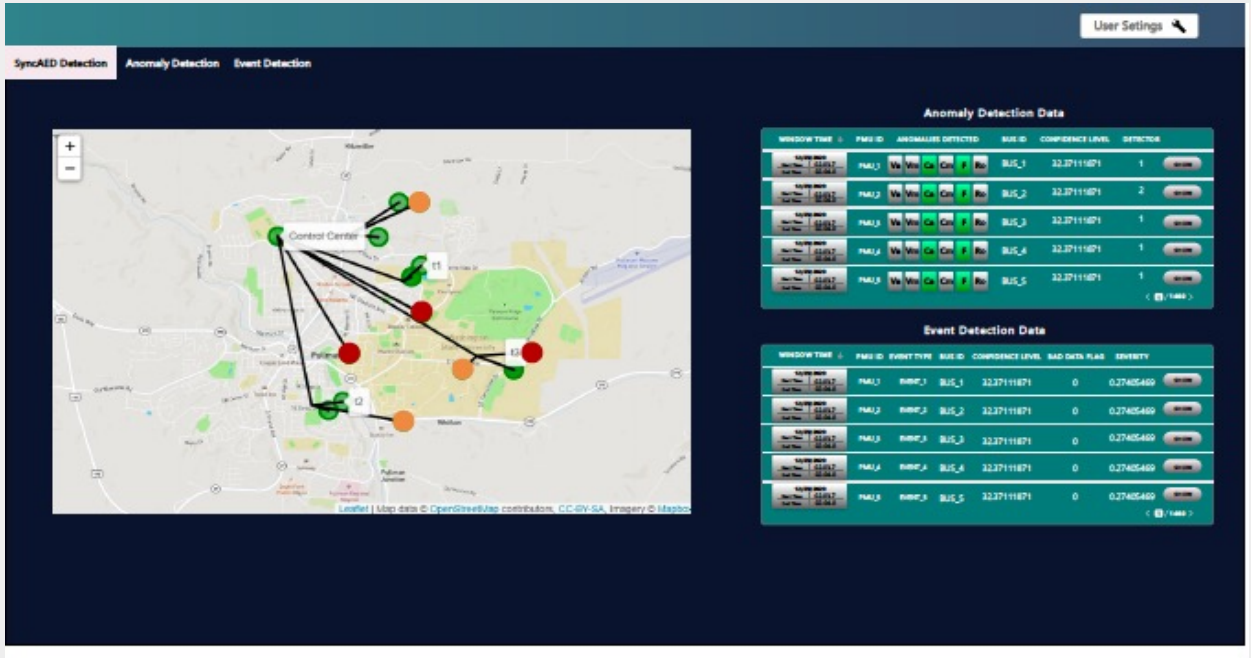
How do attackers

Tools

2

Data-driven Tools for Cybersecurity and Resiliency with IoT

Metrics and algorithms for cyber anomaly detection, classification, localization, root cause analytics and resiliency analysis



For power system expertise

Why Resiliency with IoTs?

Resiliency

- Being a critical infrastructure, the power grid has been embracing cyberattacks of gradual increasing complexity and intricacy.
- Considering that these risks cannot be eliminated, resiliency becomes vital to enable the essential infrastructure to continue to perform when faced with such threats.
- National Academy of Sciences, Engineering, and Medicine (NASEM) released a report titled ”Enhancing the Resiliency of the Nation’s Electricity System,” details the need for defining resilience metrics that can drive planning and operational decisions.
- **Resiliency :** System’s ability to keep providing energy to the critical load even with adverse events.

IoTs

- Electric Grid transformation by advanced communication infrastructure and digital devices.
- IoTs record one of the fastest growth rates in computing technologies.
- Smart devices and appliances based on IoTs are replacing traditional distribution system loads and resources.

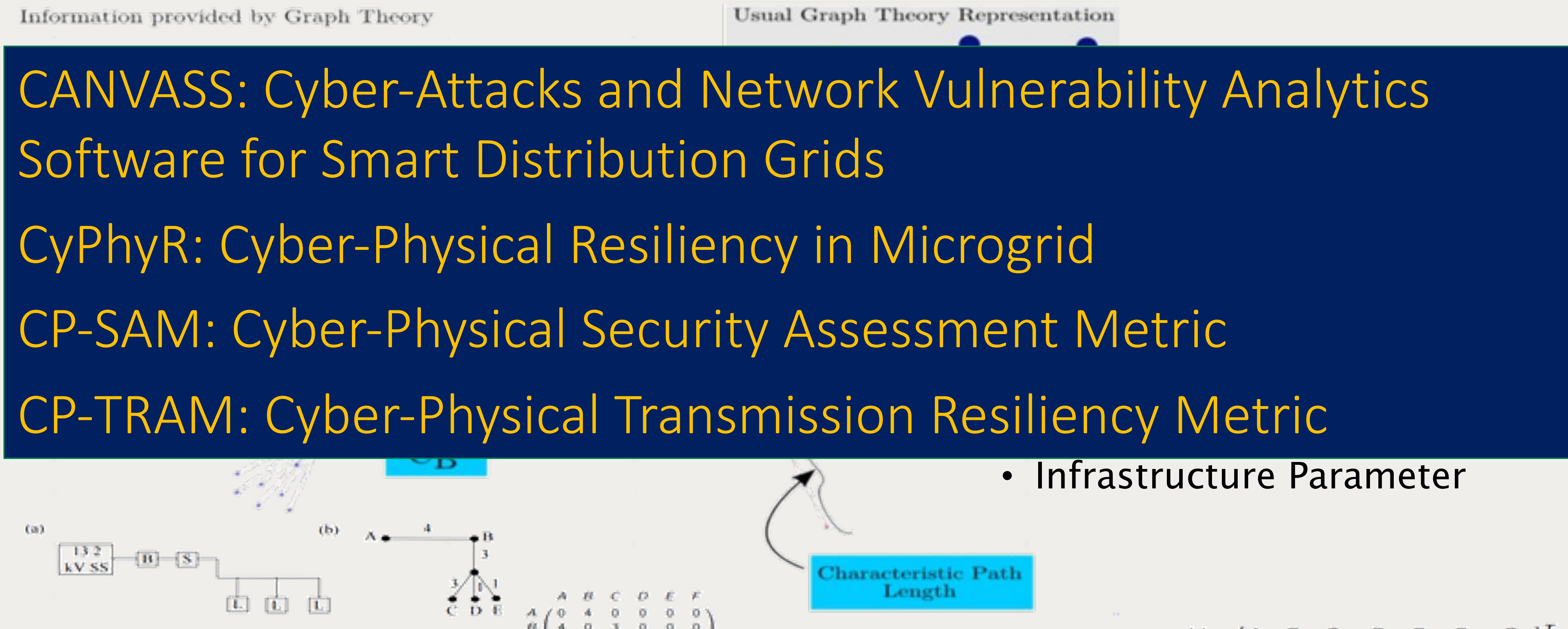
Measuring and Enabling Cyber Resiliency

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



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

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

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

Power System IoTs

According to the IEEE IoT Initiative: The definition often depends on the particular vision of the proponent entity with respect to the assets of IoT that are deemed more relevant.

Devices with the following attributes are considered as IoTs-

- Connected to others and can exchange information.
- Has unique identifier like IP address.
- Connected to control devices, or a power source or load.
- Has computing capability.
- Has some autonomous activity.
- Plug & Play

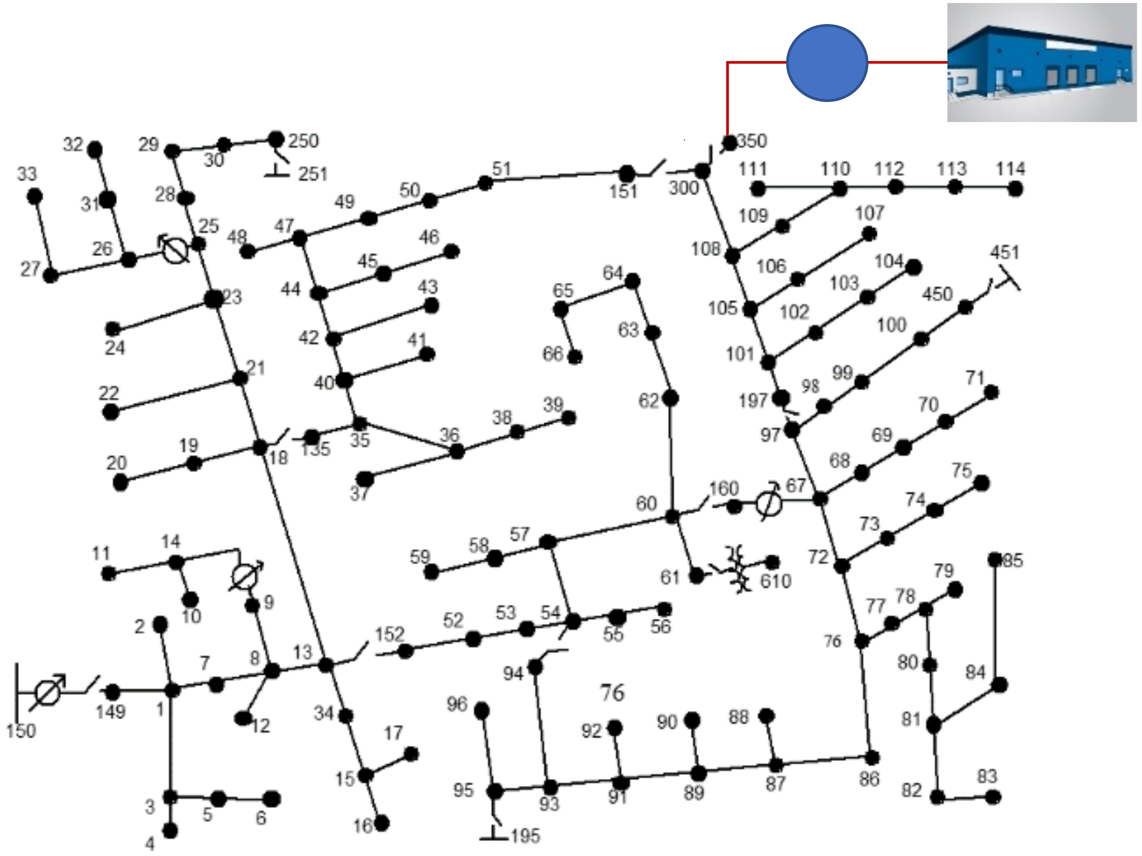
Power System IoTs of Interest: Heating, Ventilation, Air Conditioning (HVAC) system; Solar PV; Battery Storage; and Electric Vehicle (EV)

Challenges with IoTs:

IoTs attributes need to be **quantized** for **Resiliency Metric** Formulation

- IoTs data encapsulates very sensitive user information.
- Utilities or Microgrid operators do not have direct access to all the IoTs data.
- Limitation of available IoTs data.
- Data integrity and data privacy are big concerns when it comes to use of IoTs data

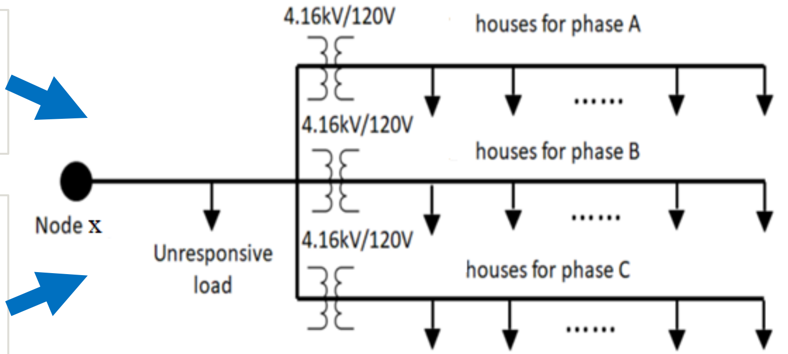
Modeling and Analysis of Distribution system with IoTs

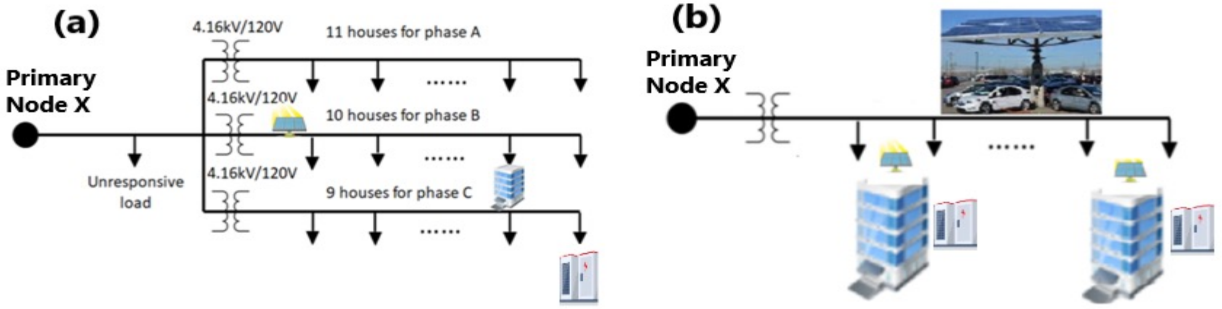


IoT – EV/HVAC/Critical loads

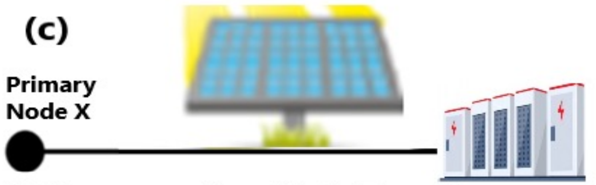
Physical Primary Node: Primary Node with no digital component in the secondary level down stream.

Cyber-Physical Primary Node without IoT: Primary Node with no IoT devices in the secondary level down stream. Digital relays, CB, SW and any other non-IoT digital device





Cyber-Physical Primary node with IoTs in the secondary level



Cyber-Physical Primary node with IoTs and no secondary level

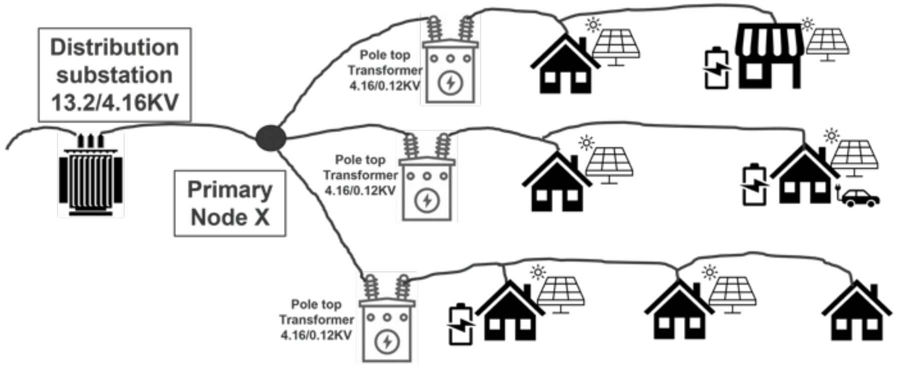
Primary feeder IEEE 123 test feeder system

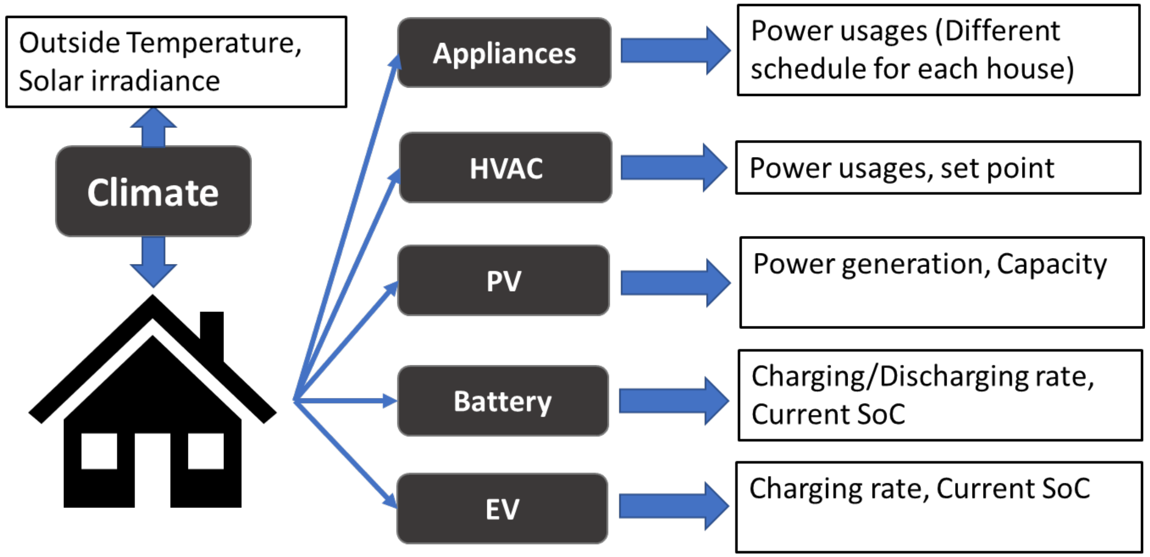
Secondary feeder mapped to each node with houses, PV, and battery

IoT level – 2 devices per house, can be expanded

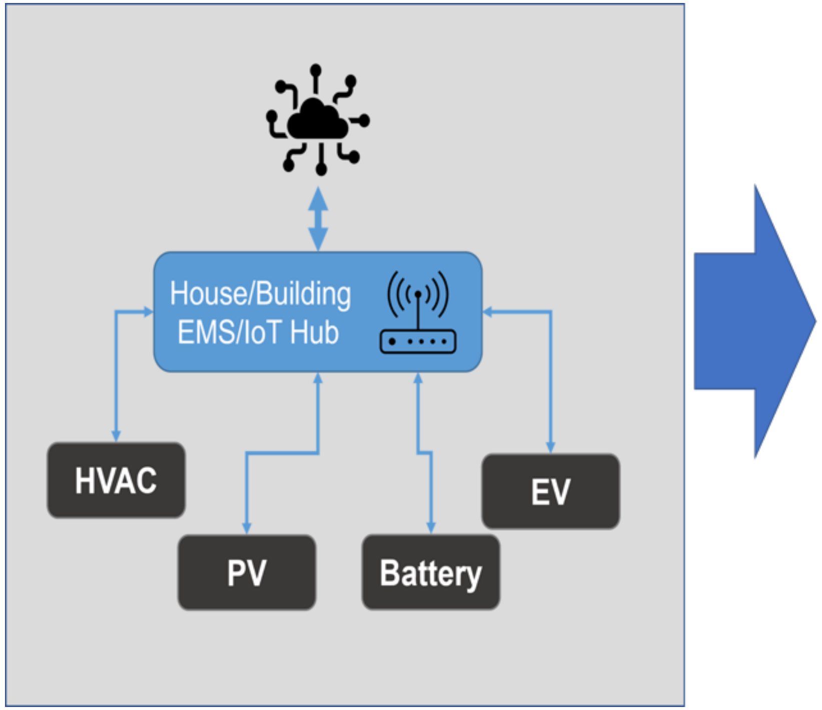
Emulation of Power System IoTs

Gridlab-D Model For Secondary Level





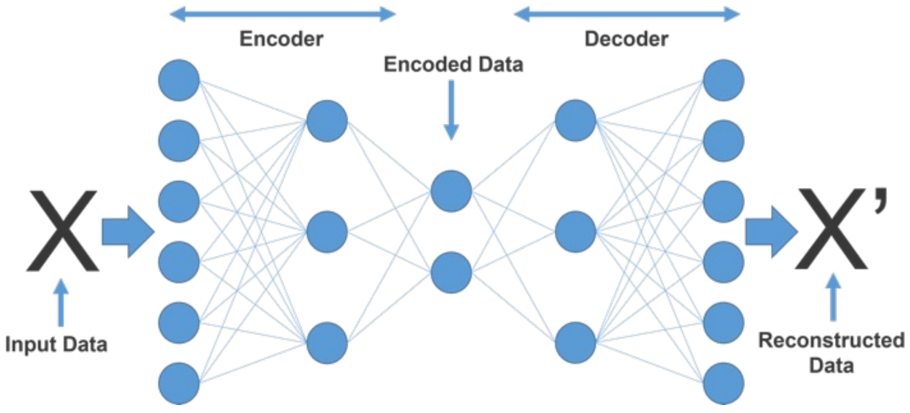
Cyber Model of in-House IoT Network in Mininet



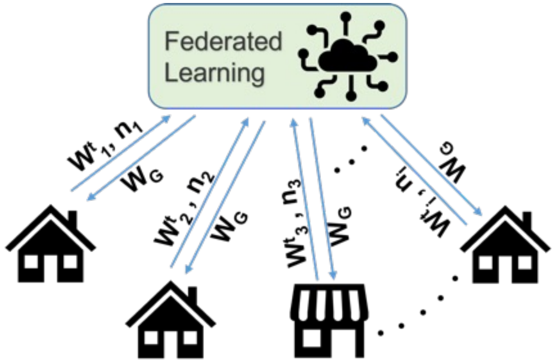
- IP Information (sr., dst.)
- Port Information (sr., dst.)
- Packet Length
- Intra communication packet delay
- ARP Table

IoT TRUSTABILITY SCORE (ITS)

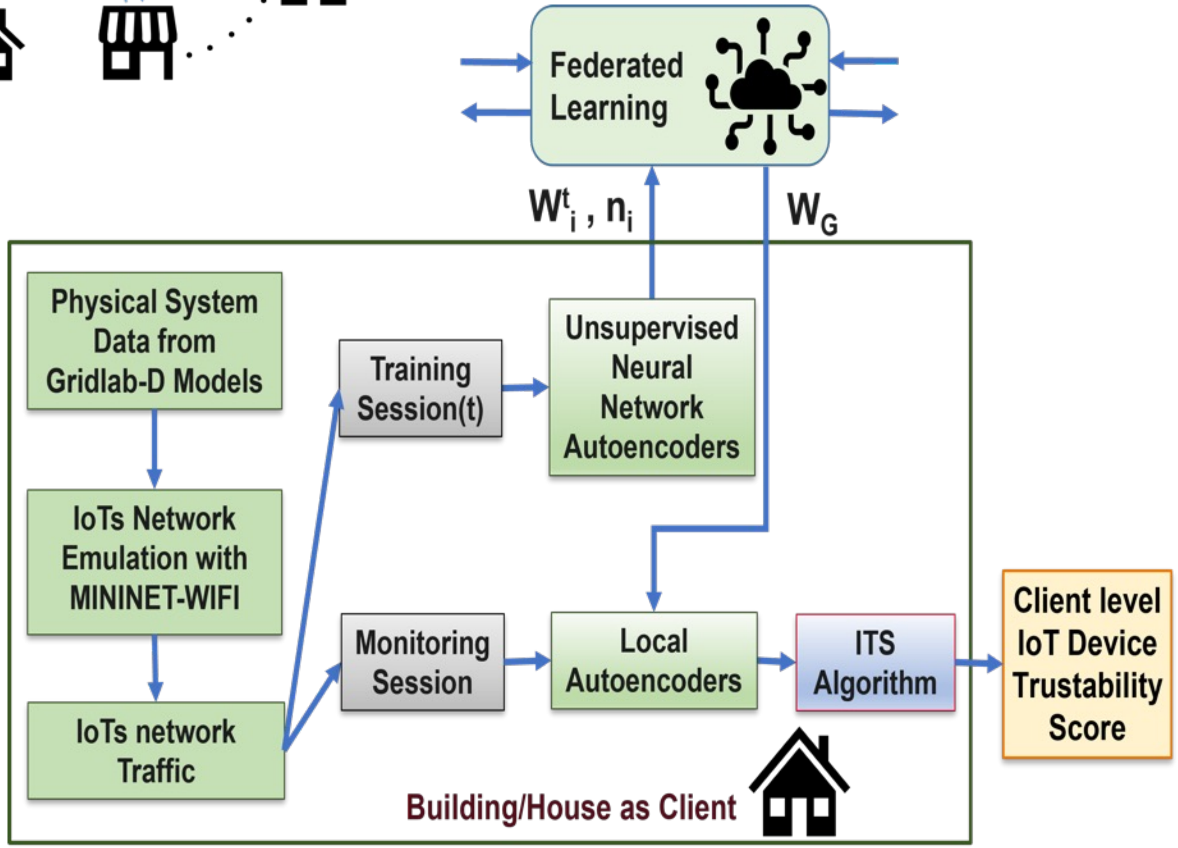
Data Source	Features
IoTs network packet	Source/Destination IP, Source/Destination port, Packet length, Protocols, Intra-packet arrival time
HVAC	Timestamp, Load, Indoor temperature, outdoor temperature, Temperature setpoint, Indoor area, Building thermal insulation
PV	Timestamp, Power generation, Rating, Solar irradiance
Battery	Timestamp, Charging/Discharging rate, SoC, KW capacity
EV	Timestamp, Charging rate, SoC



$$L(x, x') \approx \|x - x'\|$$



$$W_G = \sum_{i=1}^{M} \frac{n_i}{n} W_i^t$$



❑ P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022

IoT Trustability Score Algorithm

- Tolerance Value $\mathbf{T}_{err}$ for RE

- If RE> $\mathbf{T}_{err}$

Anomalous Data Point (ADP)= Data Point (DP)

- Non-Anomaly Ratio (NAR)

$$NAR = 1 - \frac{\text{Total ADP number over } \Delta t}{\text{Total DP number over } \Delta t}$$

- Cumulative Non-Anomaly Ratio (CNAR)

$$CNAR_t = \sum_{j=1}^{\frac{T}{\Delta t}} \frac{T}{j\Delta t} NAR_{t-j\Delta t}$$

$$ITS_t = w_t \times NAR_t + w_{t-} \times \frac{CNAR_t}{CNAR_{max}}$$

where,

$$w_t \geq w_{t-} \quad \& \quad w_t + w_{t-} = 1$$

$$ITS = \frac{\sum_{i=1}^{M} ITS_{t,i}}{M}$$

- P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022

Primary Level Node Resiliency Metric Formulation

FACTORS CONSIDERED FOR RESILIENCY CALCULATION OF EACH TYPE OF CONFIGURATION.

Primary node configuration	Factors
Physical Primary Node	Available generation Amount of critical load Connectivity redundancy
Cyber-Physical Primary Node without IoT	Available generation Amount of critical load Connectivity redundancy Device and communication vulnerabilities
Cyber-Physical Primary Node with IoT (Type-A, B, C)	Available generation Amount of critical load Connectivity redundancy Device and communication vulnerabilities IoT Device Trustability Score

Concerns related to Weight Assignment:

- No definite methods to evaluate the impact of different factors in the resiliency of cyber-physical power systems.
- Requires expertise decisions from different domains such as power systems, cyber-physical systems, and cyber system experts.
- Handle ambiguities and uncertainties in the existing information.

Fuzzy Analytic Hierarchy Process (Fuzzy AHP):

- Fuzzy AHP comes from fuzzy multiple-criteria decision-making (MCDM).
- Can incorporate the impreciseness of human judgment raised due to the subjective or qualitative nature of the criteria that can not be represented by exact numbers.
- Can controls the uncertainty and vagueness in the decision makers' opinions through fuzzy set theory.

❑ **P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022**

Primary Level Node Resiliency Metric Formulation

Fuzzification of factors' comparison:

LINGUISTIC PREFERENCES WITH SCALE FOR PAIRWISE COMPARISON [18], [20]

Linguistic preferences	Saaty's Scale	Saaty's Reciprocal Scale	Triangular Fuzzy Scale	Triangular Fuzzy Reciprocal Scale
Equally strong	1	1	(1, 1, 1)	(1, 1, 1)
Moderately strong	3	1/3	(2, 3, 4)	(1/4, 1/3, 1/2)
Strong	5	1/5	(4, 5, 6)	(1/6, 1/5, 1/4)
Very strong	7	1/7	(6, 7, 8)	(1/8, 1/7, 1/6)
Extremely strong	9	1/9	(9, 9, 9)	(1/9, 1/9, 1/9)
Intermediate values	2, 4, 6, 8	1/2, 1/4, 1/6, 1/8	(1, 2, 3), (3, 4, 5), (5, 6, 7), (7, 8, 9)	(1/3, 1/2, 1), (1/5, 1/4, 1/3), (1/7, 1/6, 1/5), (1/9, 1/8, 1/7)

Introduction of Multiple Experts/Operators:

Let there be K number of experts → $R_k = (l_k, m_k, u_k), k = 1, 2, ..., K$

Aggregated fuzzy ratings → $R = (l, m, u)$

$$l = \min_k l_k \qquad m = \frac{1}{K}\sum_{k=1}^{K} m_k \qquad u = \max_k u_k$$

For n number of factors, fuzzy pairwise comparison matrix →

$$D = \begin{bmatrix} (1,1,1) & R_{12} & \cdots & R_{1n} \\ R_{21} & (1,1,1) & \cdots & R_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ R_{n1} & R_{n2} & \cdots & (1,1,1) \end{bmatrix}$$

Fuzzy geometric mean → $r_i = (R_{i1} \times R_{i2} \times ... \times R_{in})^{\frac{1}{n}}$

Fuzzy weight → $w_i = r_i \times (r_1 + r_2 + ... + r_n)^{-1}$

Defuzzification using CoA → $w_i = \dfrac{l_i + m_i + u_i}{3}$

Final weight → $W_i = \dfrac{w_i}{\sum_{i=1}^{n} w_i}$

Primary level Node Resiliency(PNR) → $PNR = \prod_{i=1}^{n_c} (F_i)^{W_i}$

❑ P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022

Distribution System Resiliency Metric

Factors:

1) Primary Node Level Resiliency: Primary node level resiliency(PNR) considers all the attributes considering the secondary level configuration of a primary node.
2) Available power outflow: Available power outflow (APO) from primary node is the difference between the available power from different generation and storage resources, and the total amount of critical load presented in the down-stream of that primary node.
3) Primary node centrality: Primary node centrality (PNC) provides the importance of a primary level node in the whole distribution in terms of connectivity using the concept of leverage centrality. It is very effective compared to other centralities in determining the importance of any node in a network where network flow can happen in any direction rather than only along the shortest path or in a serial fashion.

$$PNC_i = \frac{d_i}{\sum_{j \in N_i} d_j}$$

4) Device and communication vulnerabilities in Primary Network: ALL the device and communication vulnerabilities presented in the Primary (DCVP) level of a distribution system is considered here.

Weight Assign and Aggregation:

- Weight distribution problem is formulized as a Data Envelopment Analysis (DEA) problem.
- The concept from "Egoist's dilemma: a DEA game" is used to determine the weights so that each node will have the best set of weights so that they can contribute to the maximum possible value.

$$\max_{w^p} \frac{\sum_{i=1}^{m} w_i^p f_{ip}}{\sum_{i=1}^{m} w_i^p \sum_{j=1}^{n} (f_{ij})}$$

$$s.t. \quad w_i^k \geq w_i^{ex}, \quad \sum_{i=1}^{m} w_i^k = 1$$

Distribution System level Resiliency:

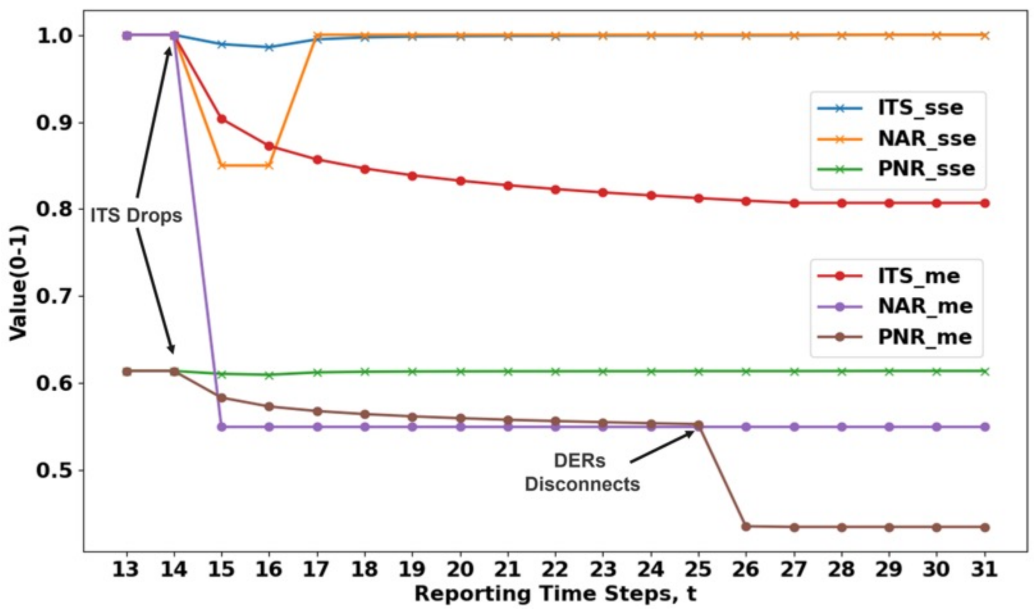
$$DSR = \sum_{j=1}^{n} \left(\prod_{i=1}^{m} (f_{ij})^{w_i^j} \right)$$

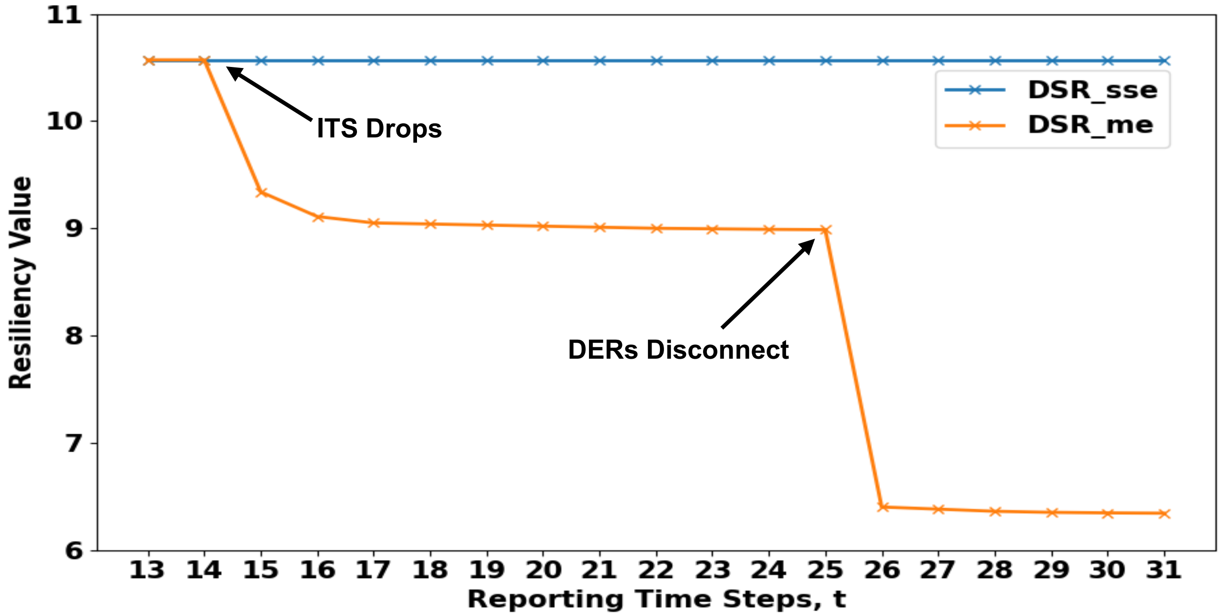
- P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022

Case Studies & Results

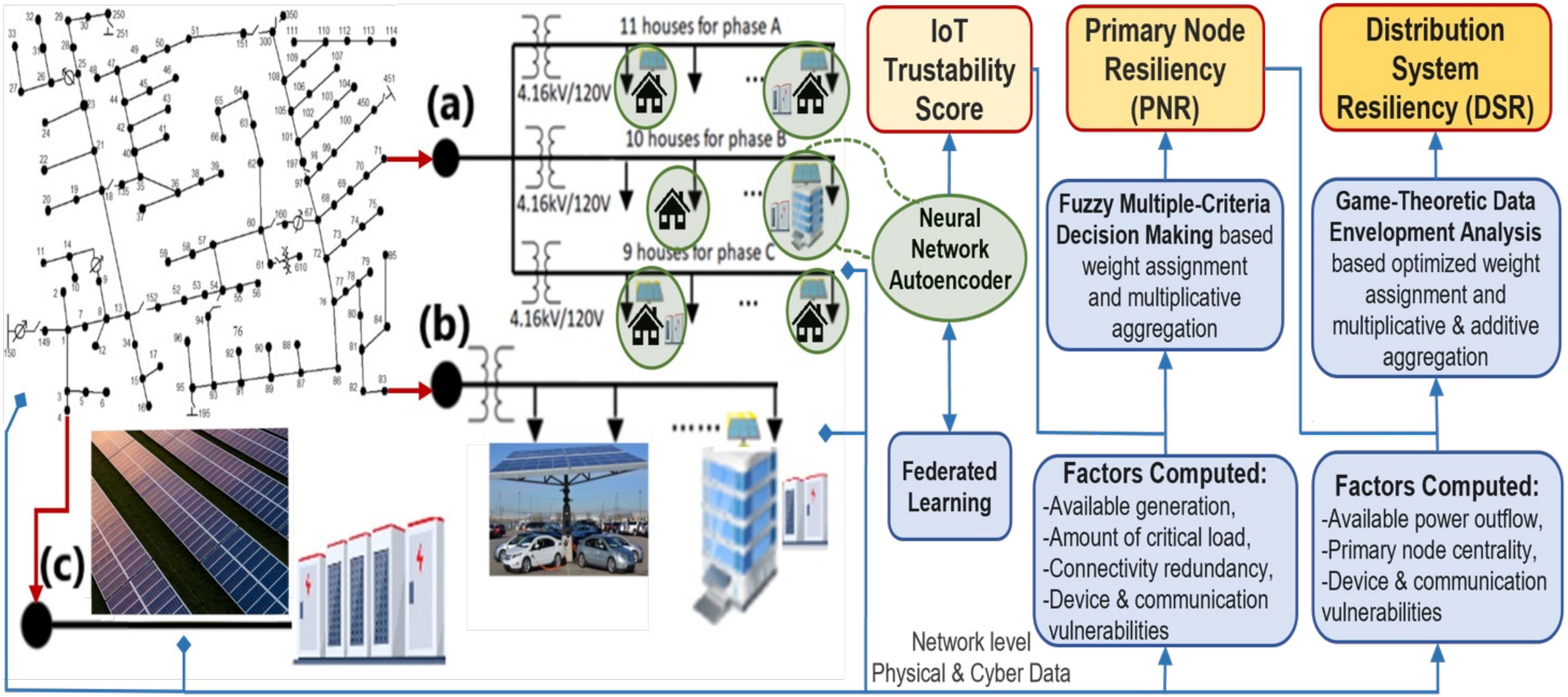
Short Suspicious Event (sse): solar PV of one house from the primary node accidentally got disconnected from its smart IoT-based inverter during maintenance of the PV panel.

Malicious Event (me): two houses and the commercial building use smart IoT-based inverters from the same manufacturer for their solar PV and battery, and attackers have discovered vulnerabilities of the inverters of that manufacturer.





Resiliency Metrics and it's Usages



Applications

Planning upgrade or modification focusing resiliency

Design resilient microgrids and compare resiliency of different microgrid designs

Perform root cause analysis of degraded operational resiliency

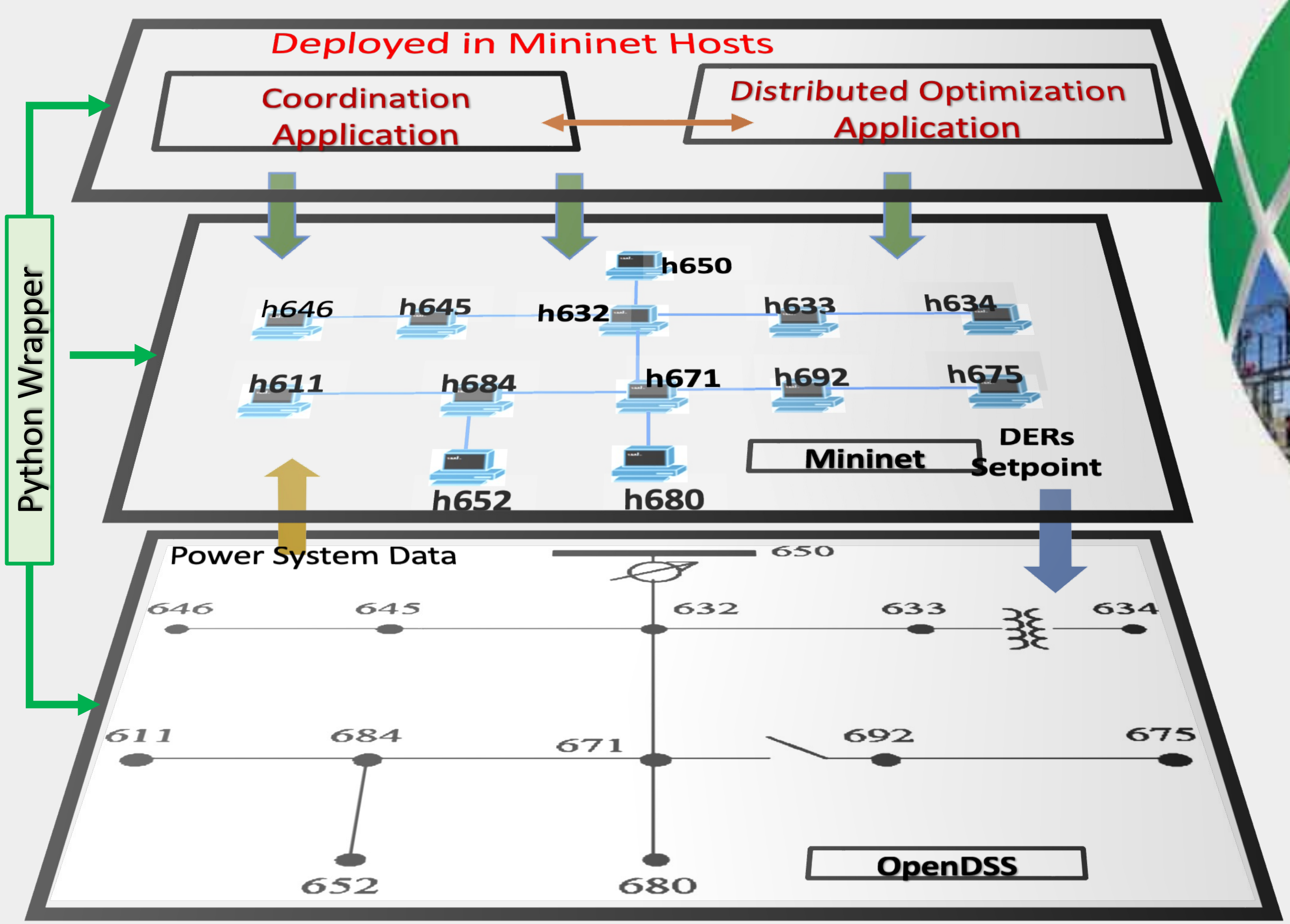
Post event resilient reconfiguration

Testbed

3

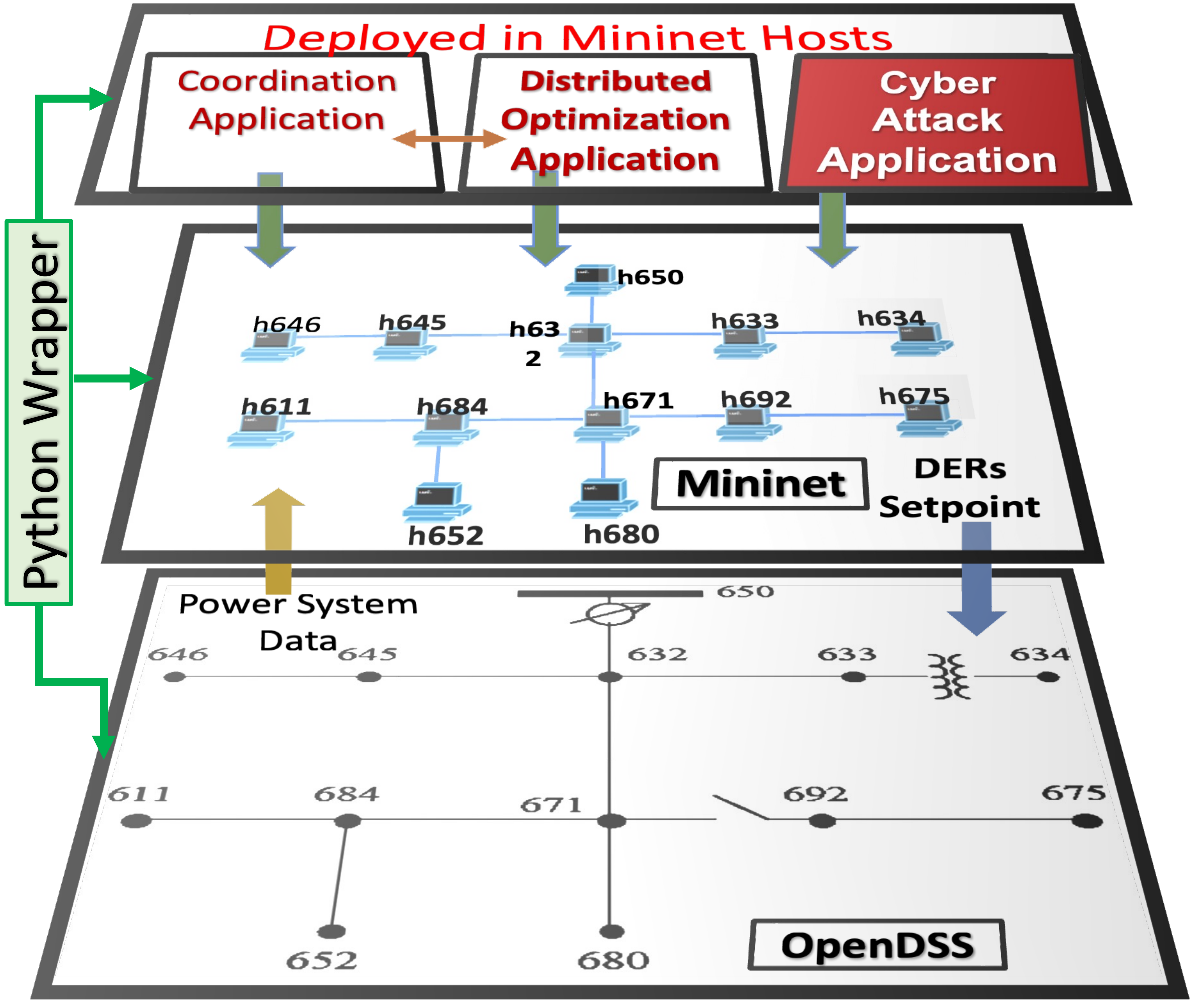
Testbed for Training and Validation

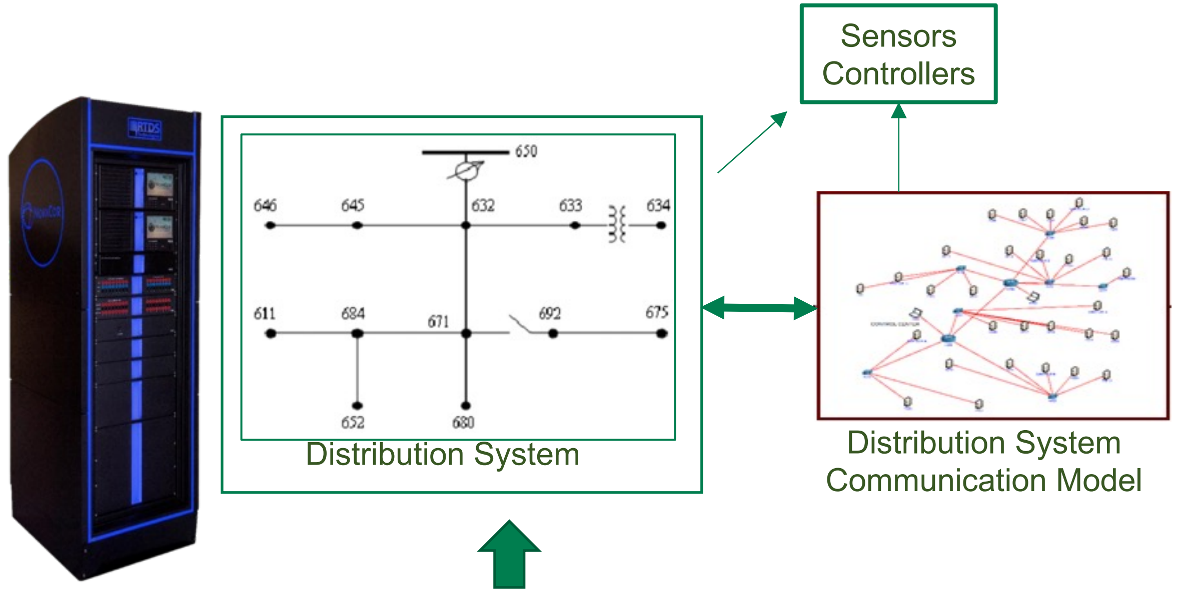
Validate algorithms and tools for deployment



cigre
For power system expertise

CYBER-POWER TESTBED





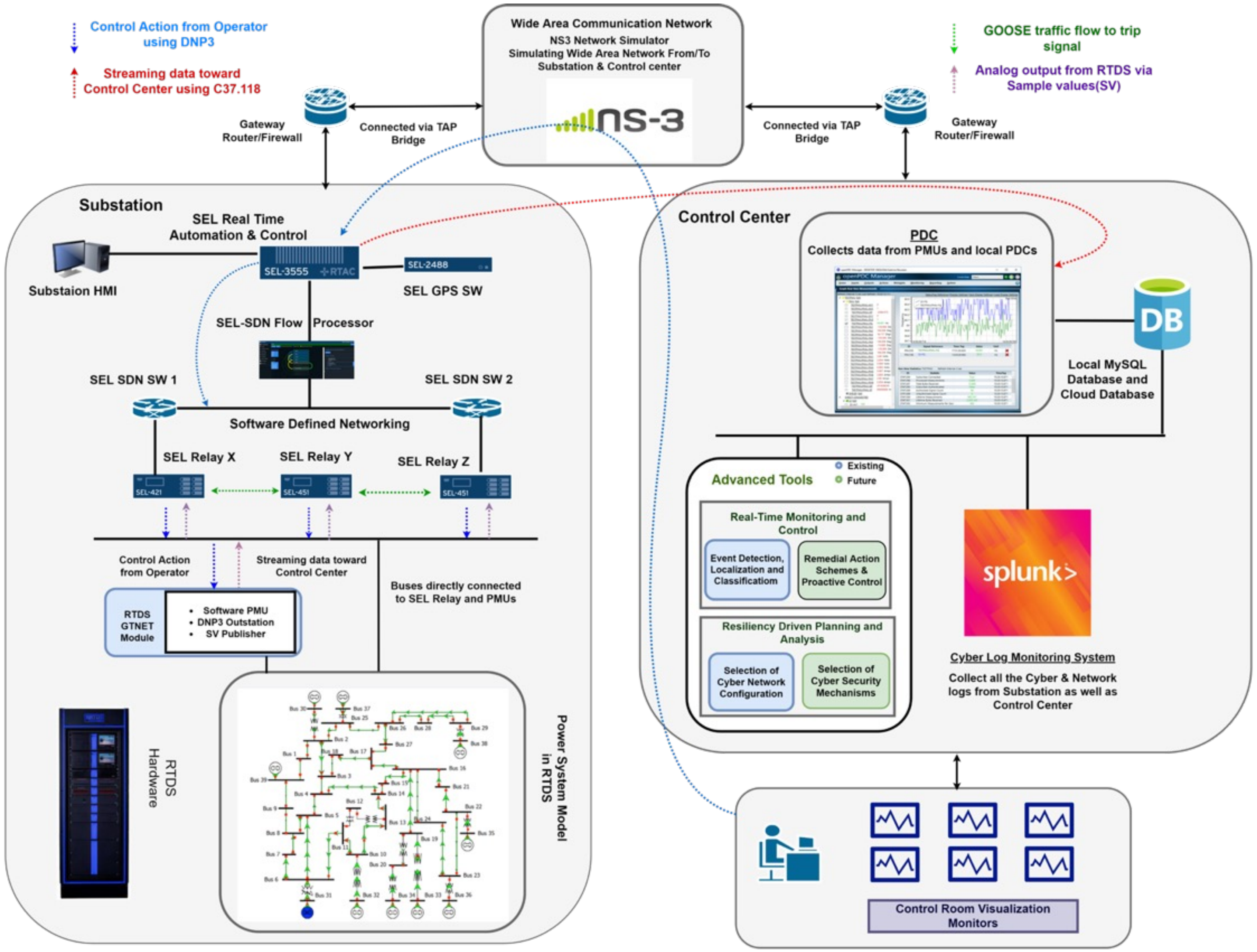
Testbed 2: Electromagnetic Real Time Simulator with HIL

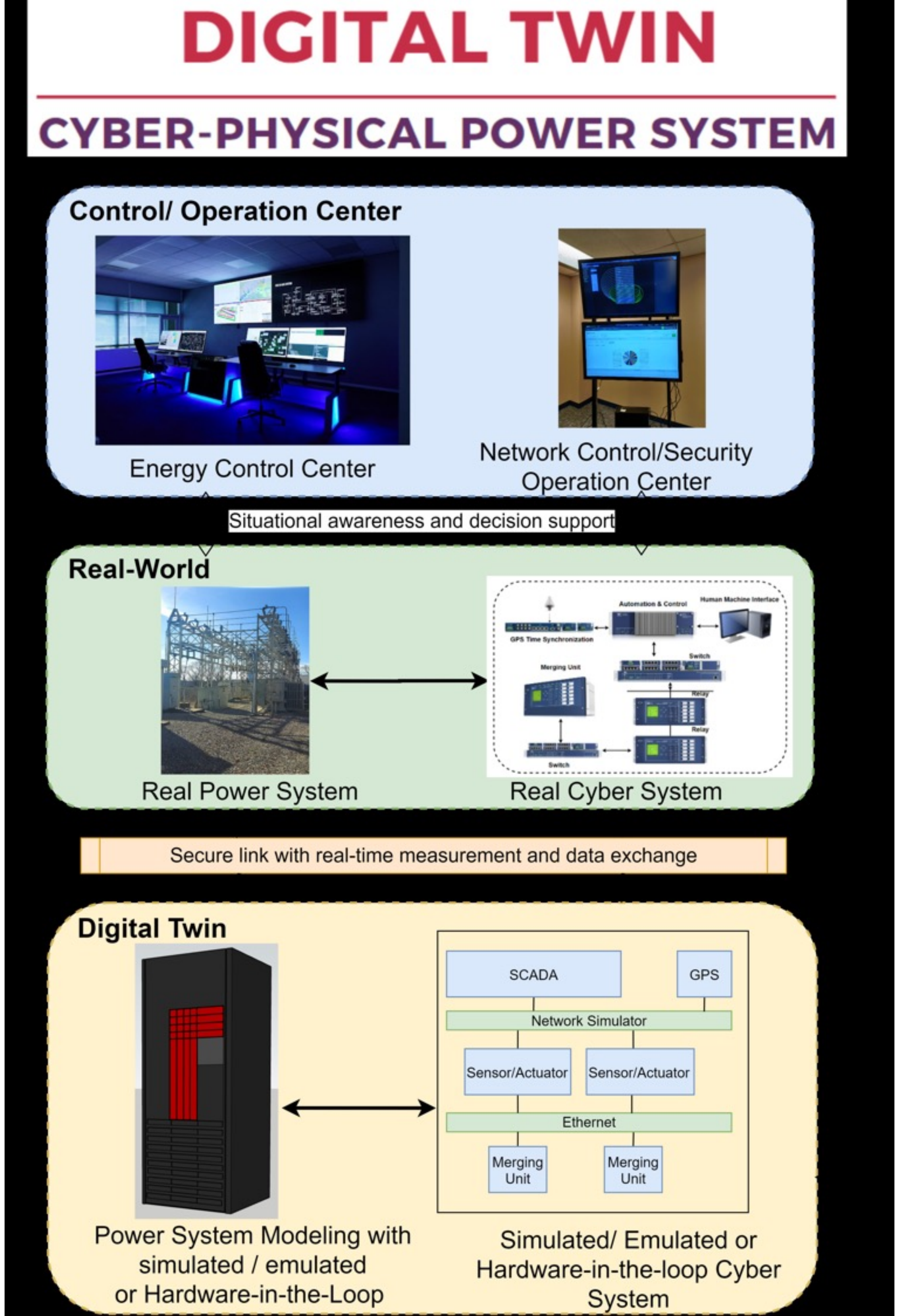
Testbed 1: Electromechanical Simulator

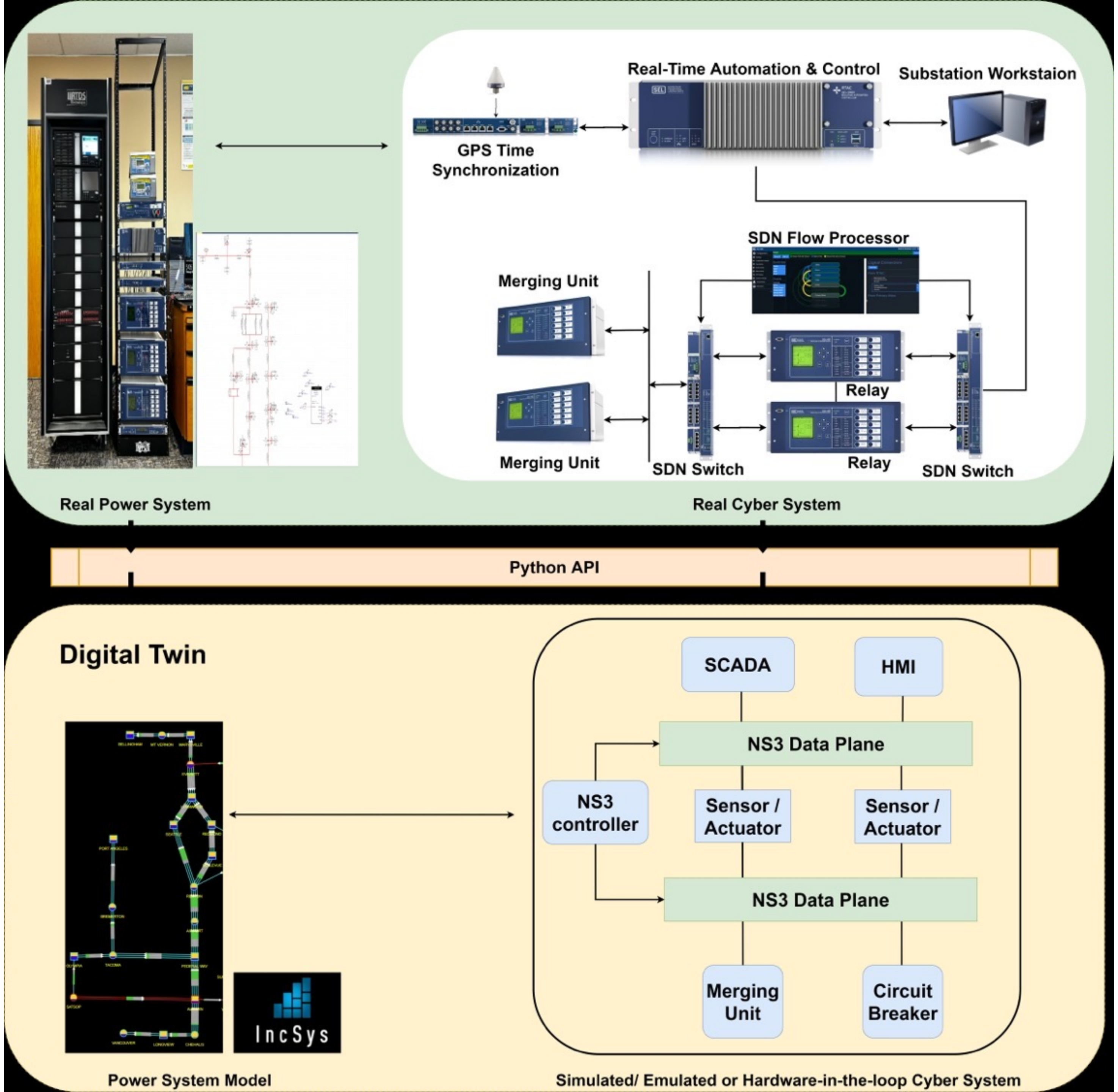
Real-Time Cyber-Power-HUMAN Testbed

Developed Real-Time Cyber-Power Testbed

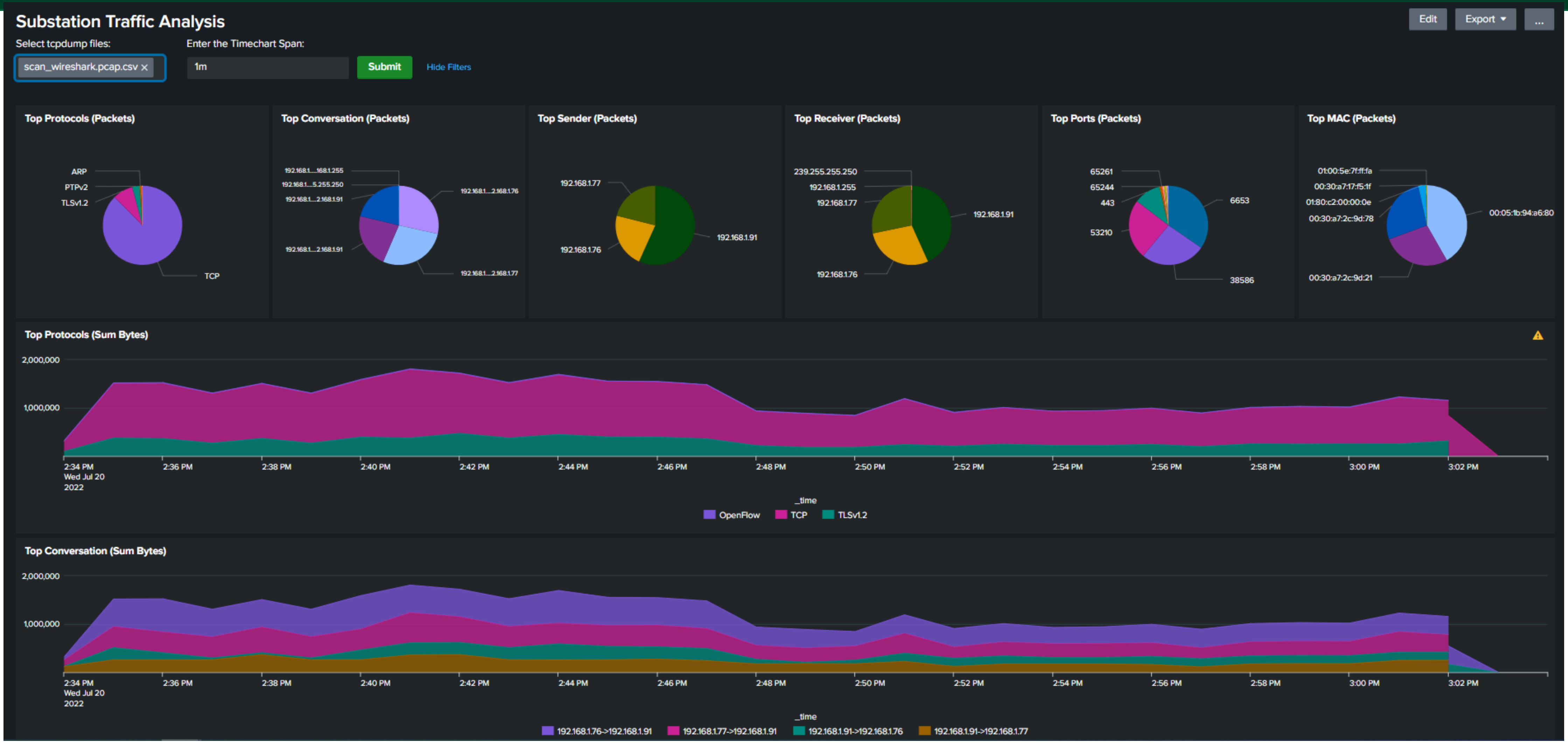
- Physical power system layer
- Substation automation and protection Layer
- Wide area communication network layer
- Control center layer
- Visualization and monitoring layer
- Human operator layer




DIGITAL TWIN
CYBER-PHYSICAL POWER SYSTEM
Control/ Operation Center
Energy Control Center
Network Control/Security Operation Center
Situational awareness and decision support
Real-World
Real Power System
Real Cyber System
Secure link with real-time measurement and data exchange
Digital Twin
SCADA
GPS
Network Simulator
Sensor/Actuator
Sensor/Actuator
Ethernet
Merging Unit
Merging Unit
Power System Modeling with simulated / emulated or Hardware-in-the-Loop
Simulated/ Emulated or Hardware-in-the-loop Cyber System


Real-Time Automation & Control
Substation Workstaion
GPS Time Synchronization
SDN Flow Processor
Merging Unit
Merging Unit
Relay
Relay
SDN Switch
SDN Switch
Real Power System
Real Cyber System
Python API
Digital Twin
SCADA
HMI
NS3 Data Plane
NS3 controller
Sensor / Actuator
Sensor / Actuator
NS3 Data Plane
Merging Unit
Circuit Breaker
IncSys
Power System Model
Simulated/ Emulated or Hardware-in-the-loop Cyber System

SG-REAL CYBER LOG MONITORING SYSTEM



Assisting operator to investigate Network anomaly using dashboard and data logging

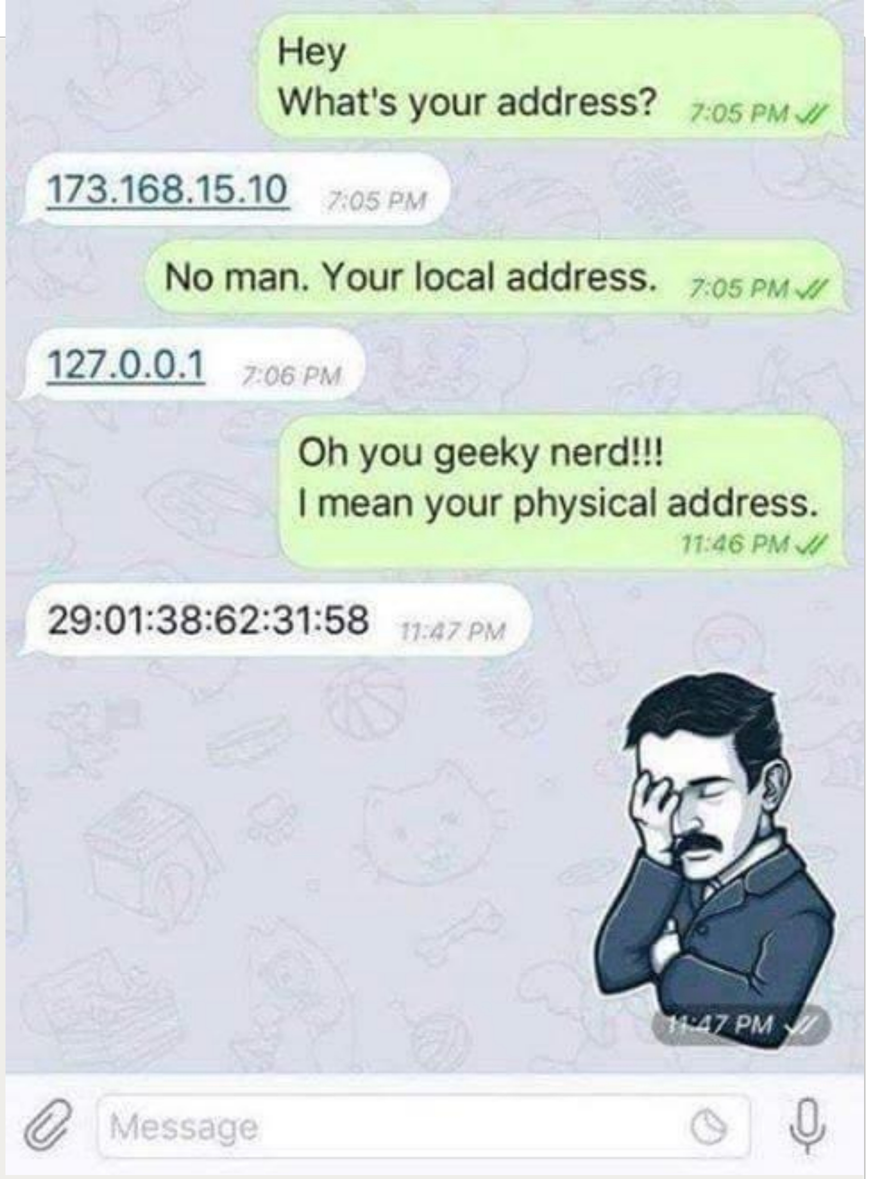
Human operator layer - Eye Glass sensors

- Gaze mapping → maps dynamic eye tracking data onto a static 'reference' image of the environment.
- Heatmaps → visualization that summarizes which objects in a scene were looked at most by a group of respondents.
- AOI editor → derive eye tracking metrics related to objects or other defined parts of the stimulus.

Summary

Takeaway

- Electric grid is cyber-physical-human network and going through major transformation
- Introduction of IoTs based DERs, loads, and other devices leads to better and efficient operation with flexibility but also brings vulnerabilities.
- Massive sensor data provides opportunity for transformative approach
- ITS, PNR and DSR metrics offer visibility to the edge of the system.
- Proposed metrics are scalable and capable to facilitate resiliency based monitoring and operation for any advanced microgrid/distribution system.
- These metrics can be used to find out weaknesses for a given microgrid configuration and improvement actions can be prioritized based on the scores.
- Testbed are important for simulated data and validating decision support



Thanks to organizers, my students, funding agencies: DOE, NSF and Industry Collaborators

Anurag K. Srivastava: anurag.srivastava@mail.wvu.edu