



PSERC WEBINAR
September 17, 2025



Cybersecurity and Resiliency for DERs and Microgrids



Manimaran Govindarasu

Dept. of Electrical and Computer Engr.

Iowa State University

gmani@iastate.edu



Murti Salapaka

Dept. of Electrical and Computer Engr.

University of Minnesota

murtis@umn.edu

Acknowledgement:

Project funded by US Department of Energy (DOE)

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

DOE Award: DE-CR0000040

<https://cyderms.iastate.edu/>



**IOWA STATE
UNIVERSITY**



UNIVERSITY OF MINNESOTA

Outline of the Talk

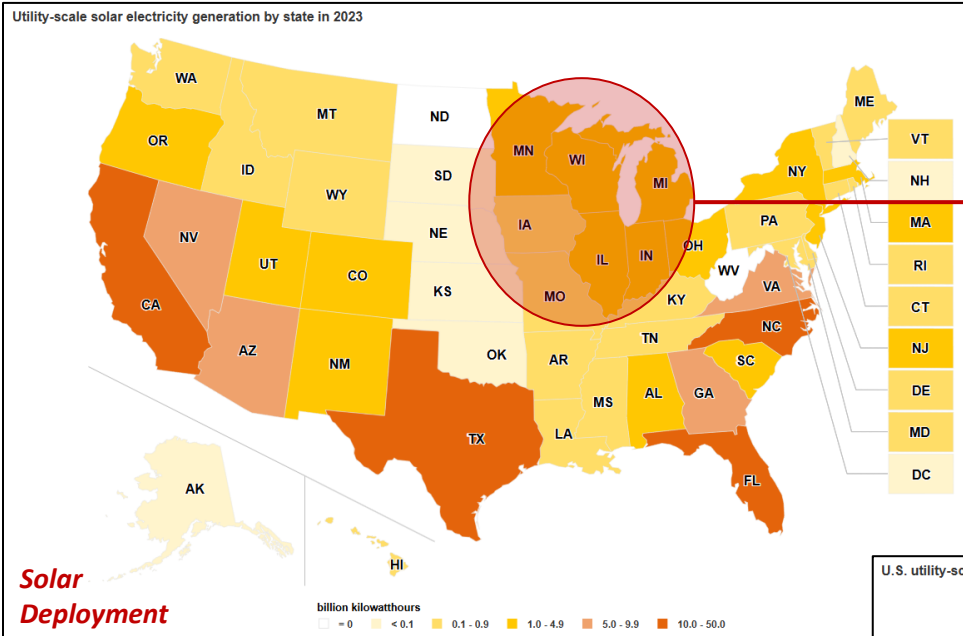
Part I

- DER Infrastructure and Cyber Attack Surface
- CyDERMS Vision and Overview
- Security Operations Center (SOC) for DERMS Control Center– *ISU*
- Conclusion 1

Part II

- Distribution Grid Topology Estimation -- *UMN*
- Conclusion 2

Solar and Wind Generation in the US (2023)



Total Solar Generation for 2023

Illinois – 1.9420 billion kWh

Iowa – 0.52 billion kWh

Minnesota – 1.9960 billion kWh

Wisconsin – 1.2430 billion kWh

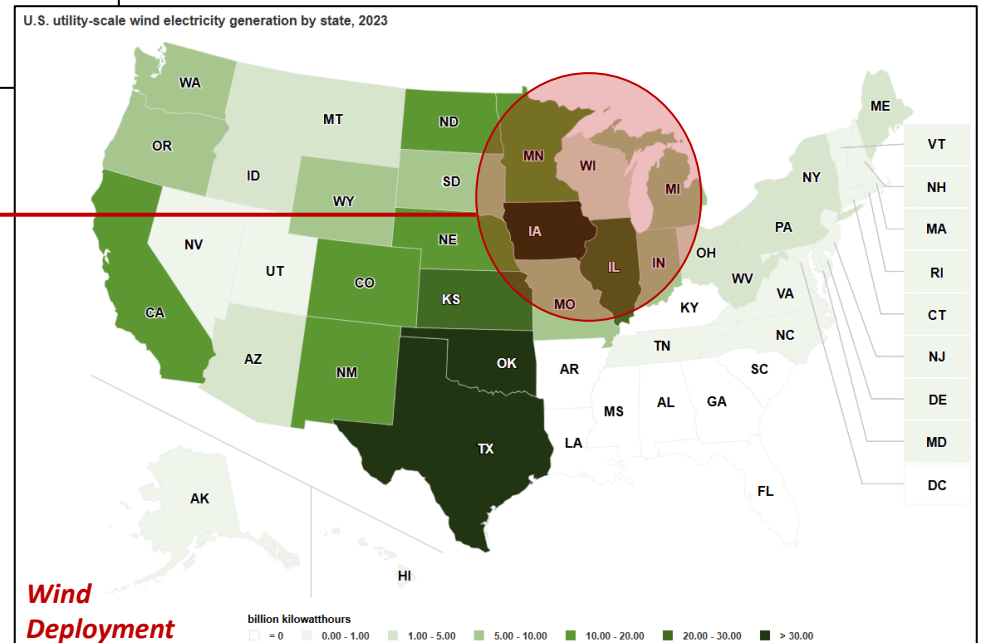
Total Wind Generation for 2023

Illinois – 22.054 billion kWh

Iowa – 41.869 billion kWh

Minnesota – 14.665 billion kWh

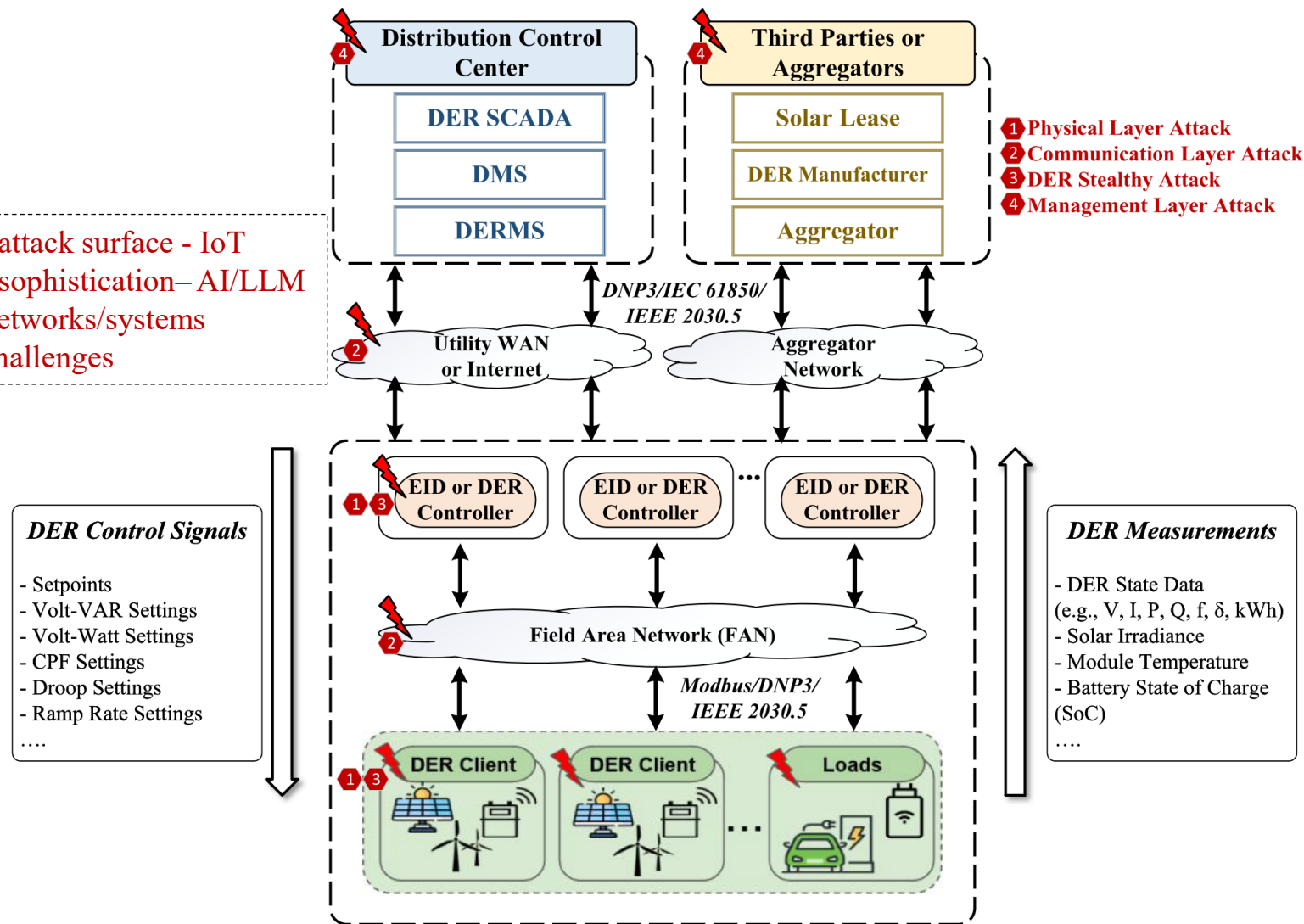
Wisconsin – 1.759 billion kWh



Source: U.S. Energy Information Administration (EIA)

DER System Architecture & Attack Surface

- Expanding cyber attack surface - IoT
- Increasing attack sophistication– AI/LLM
- Legacy devices/networks/systems
- Interoperability challenges



Ref: S. Bose, S. Bhattacharya, N. Saqib, and M. Govindarasu, "ZT-MTD: Zero Trust-enabled Dynamic Moving Target Defense for DER Networks," accepted at the IEEE Power & Energy Society General Meeting (PES GM), 2025

Real-world Cybersecurity Incidents targeting DER Networks

UTILITY DIVE Deep Dive Opinion Library Events Press Releases

Generation T&D Grid Reliability Electrification Load Management

DIVE BRIEF

NERC finds first remote hacker interference on US grid from cyberattack

Published Sep

By HJ Mai



World Business Markets Sustainability Legal Commentary Technology Investigations

Rogue communication devices found in Chinese solar power inverters

Cyber Press

Cyber Attack Threats Cyber AI Data Breach Vulnerability

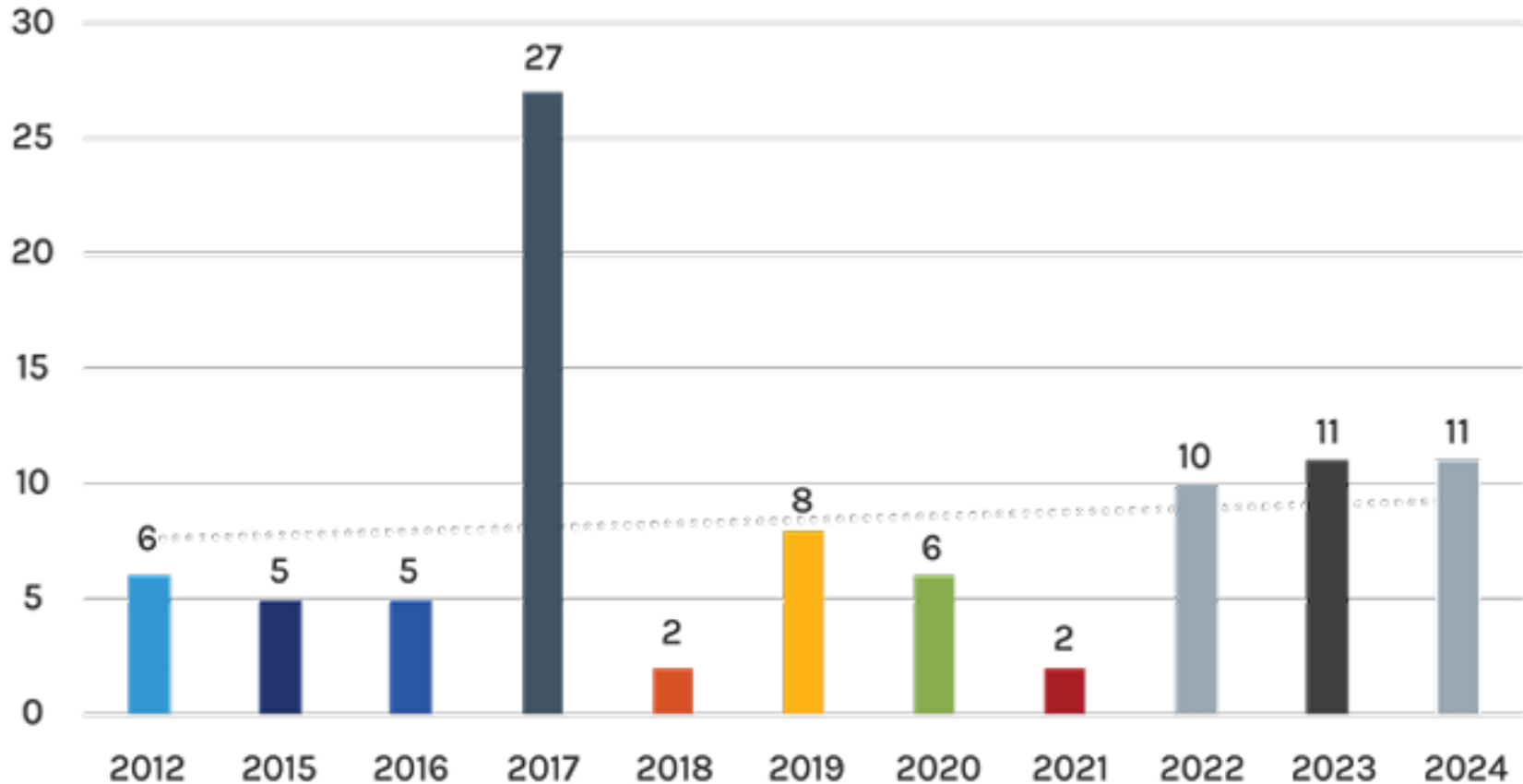
46 New Vulnerabilities in Solar Inverters Let Attackers Manipulate Settings

BY MANDVI / MARCH 28, 2025

Categories: Cyber Security News Cybersecurity Vulnerability

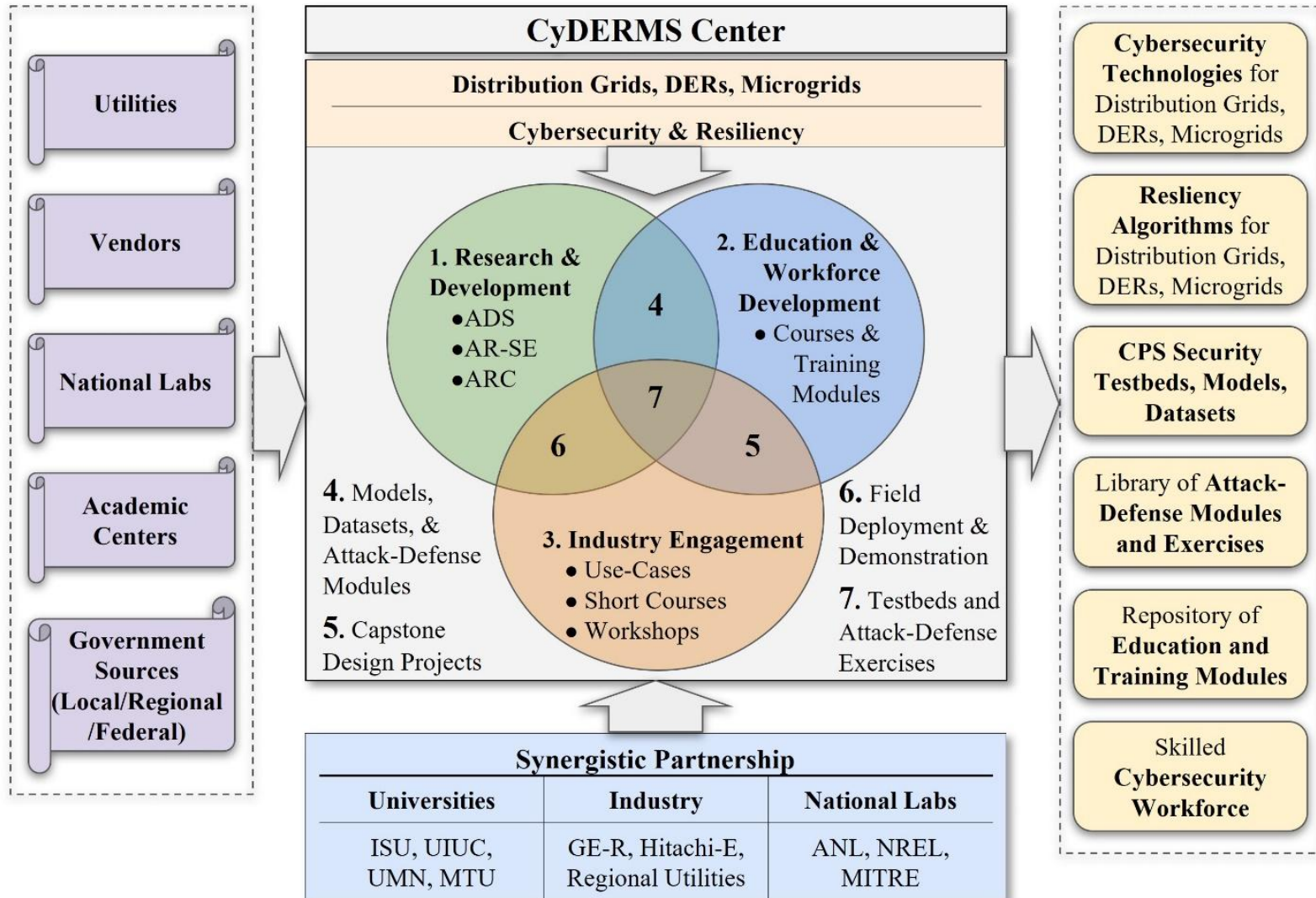
Cyber Vulnerabilities reported by DER Vendors

CVEs on solar power equipment per year of disclosure



Source: Forescout Research Vedere Labs

CyDERMS Project Vision (DOE funded)



Project Team

Phase I R&D Task	Task Description	Institutions
2	ML-based Situational Awareness for DERs and Microgrids	<i>ISU</i> , ANL, NREL, GE-R
3	Attack-resilient SE algorithms for distribution grid with DERs and Microgrids	<i>UMN</i> , UIUC
4	Attack-resilient control algorithms for DER-integrated distribution grid	<i>ISU</i> , MTU, ANL, NREL
5	Attack-resilient control algorithms for Microgrid-integrated distribution grid	<i>UIUC</i> , UMN
6	Education and Workforce Development	<i>ISU</i> , UMN, UIUC, MTU, NREL
Phase II R&D Task	Task Description	Institutions
7	System Integration, Testing, and Evaluation	<i>ISU</i> , UMN, UIUC
8	Tech Transfer and Field Demonstration	<i>ISU</i> , UMN, UIUC



Task 2: ML-based Situational Awareness for DERs and Microgrids

Task Goal:

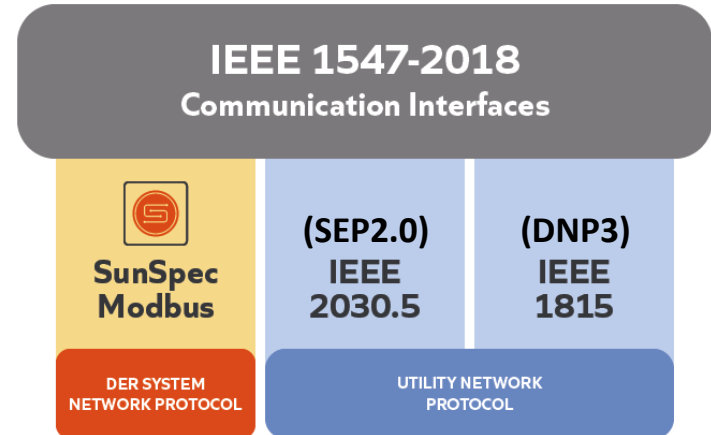
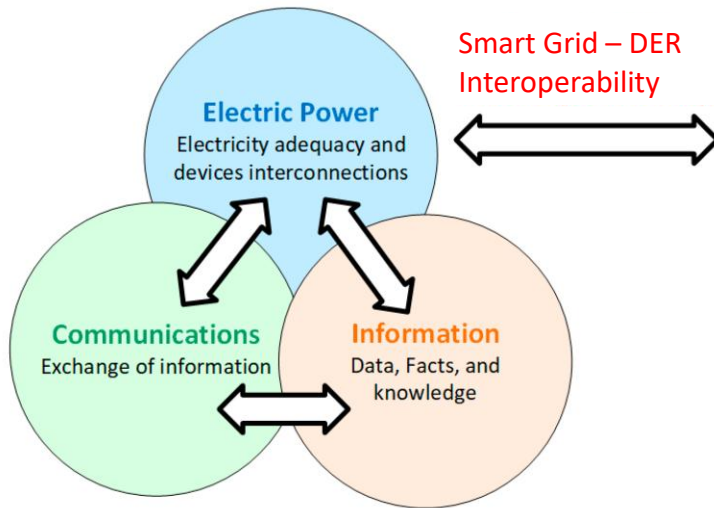
- **Protocol Converter** Module for Interoperability of DER Networks
- **Security Operations Center (SOC)** for DER Communication Infrastructure

Expected outcomes:

- **Tools and technologies** for the Protocol Converter Module and SOC platforms.
- **Realistic DER datasets** for training of ML-based algorithms for anomaly detection.
- **Real-time HIL testbed-based** evaluation and validation of developed solutions for practical implementation.

DER Protocols & Interoperability

IEEE-1547 recommended DER Communication Protocols for Interoperability

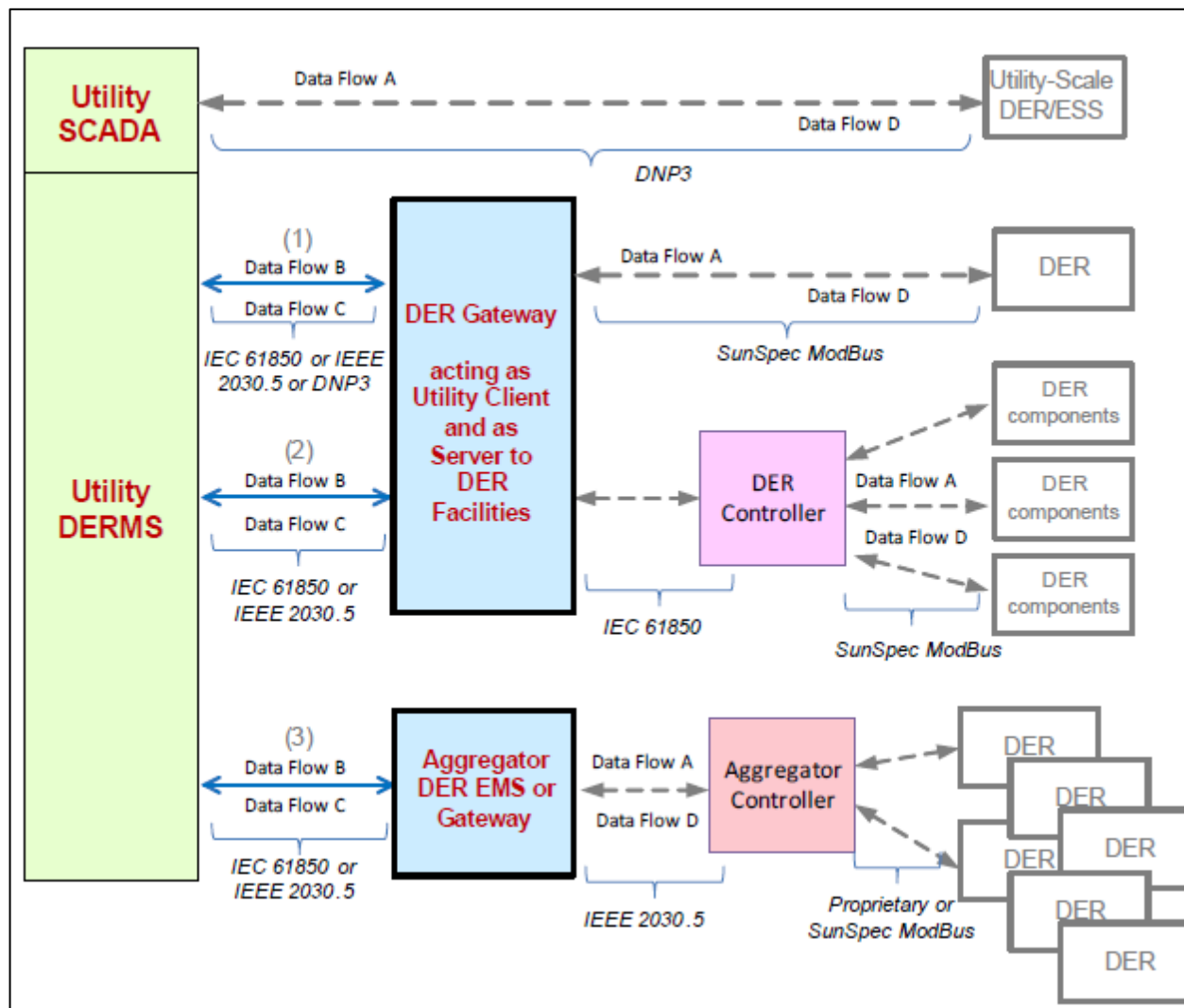


- Interoperability is essential between “**SUNSPEC MODBUS & DNP3**”
- Why?
 - In the US, 90% of the DER Deployed have SunSpec Modbus Interface for Monitoring and Control.
 - In the WAN, DNP3 is the most used protocol and is widely deployed.
- Highlighting a need for seamless **Protocol Conversion**

IEEE 1547-2018, <https://standards.ieee.org/ieee/1547/5915/>

DER Deployment Scenarios & Interoperability

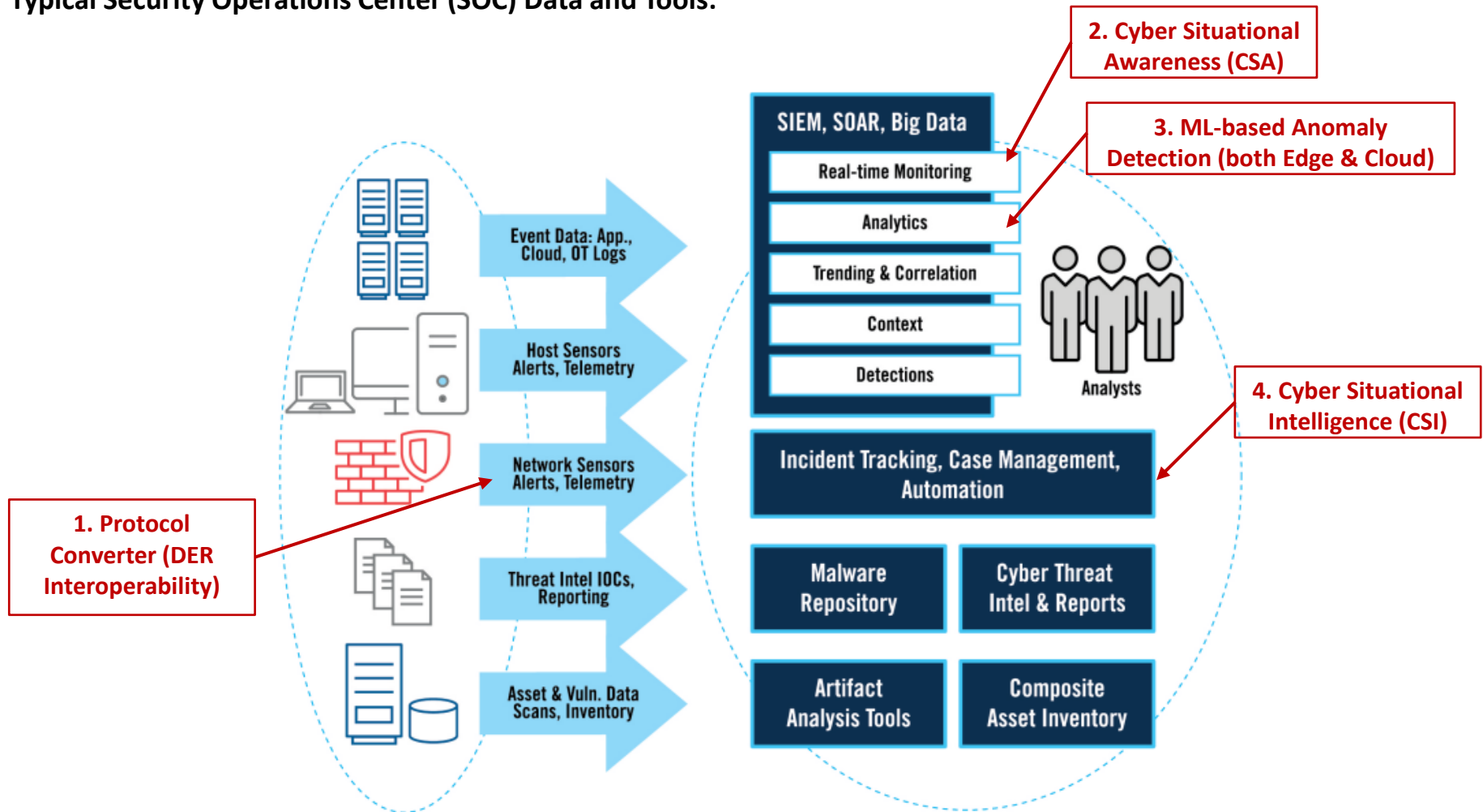
Example Configurations for Communications between Utilities and DER Systems



Ref: CReST-VCT System Integration Framework, <https://www.pnnl.gov/publications/crest-vct-system-integration-framework>

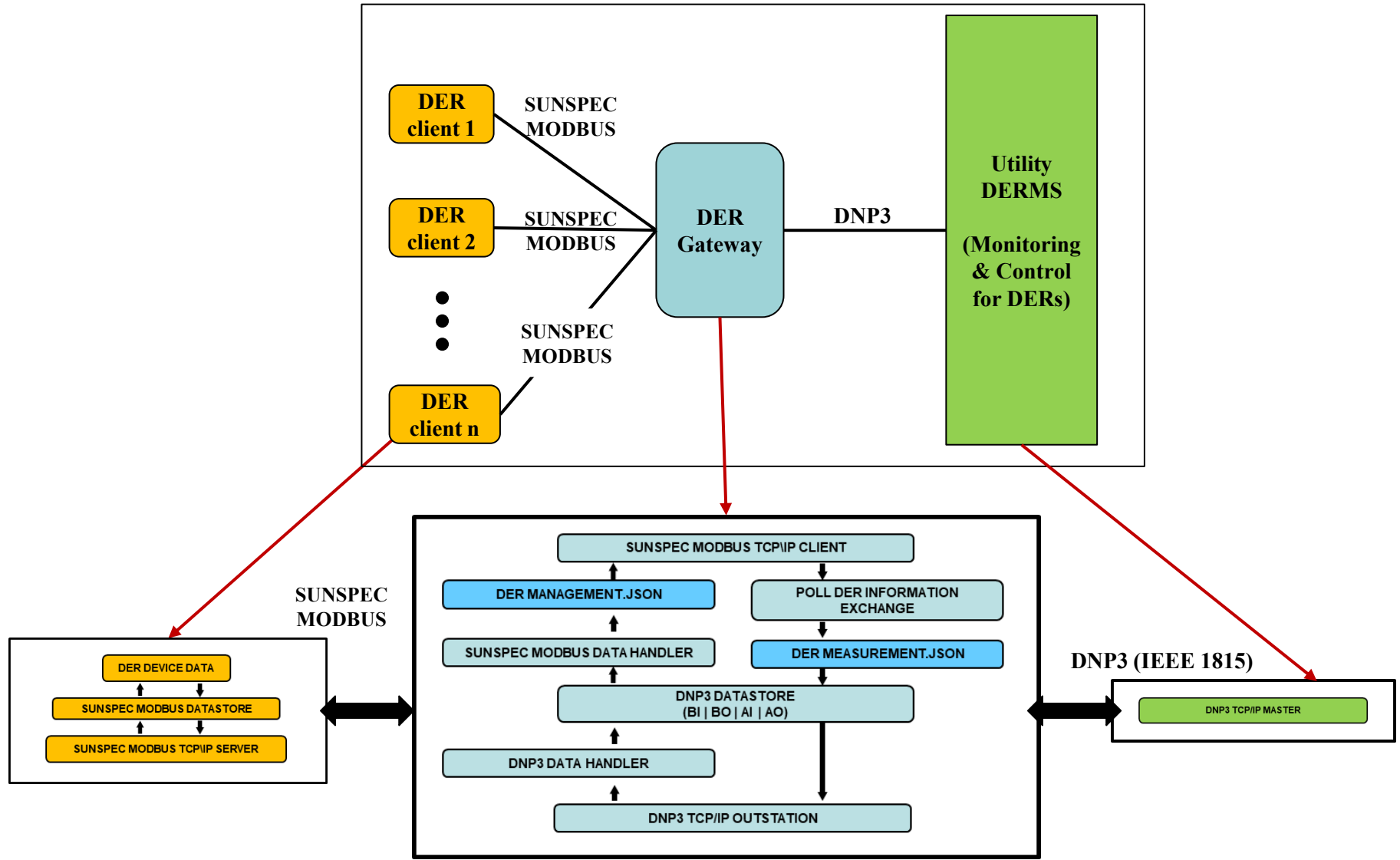
SOC for DERMS Control Center

Typical Security Operations Center (SOC) Data and Tools:

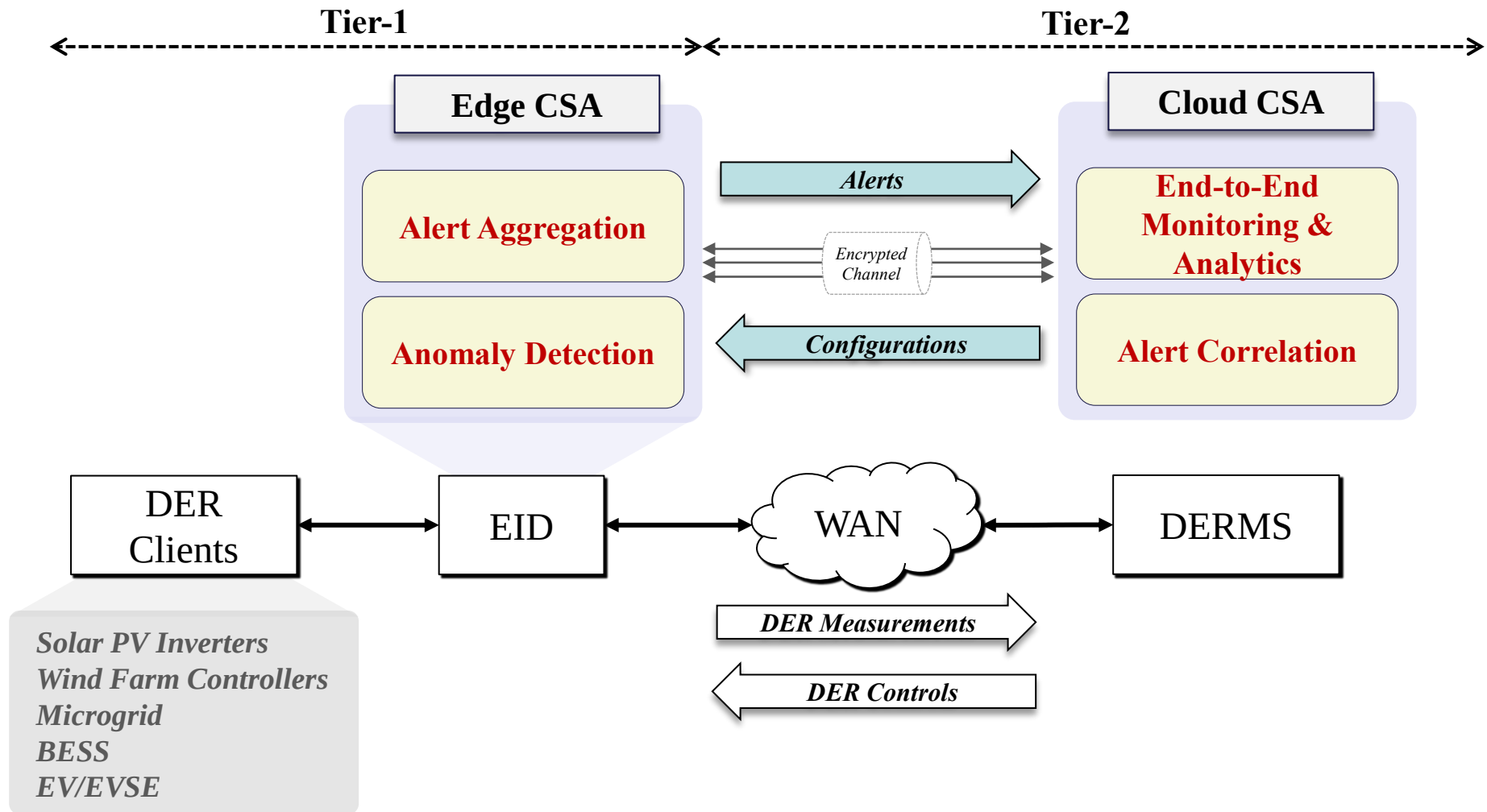


Ref: MITRE, *11 Strategies of a World-Class Cybersecurity Operations Center*

1. DER Protocol Conversion Framework



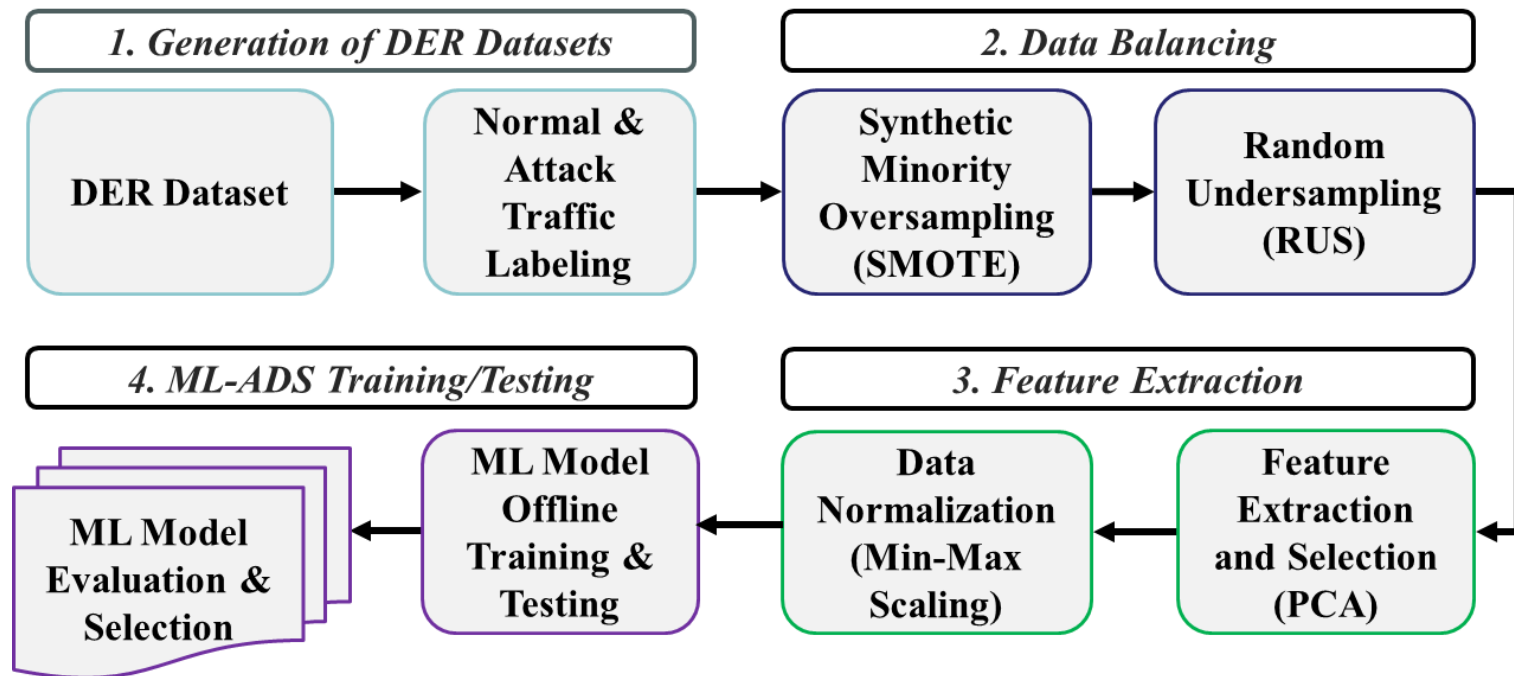
2. Proposed Cyber Situational Awareness (CSA) Platform



Ref: M. Abdelkhalek and M. Govindarasu, "ML-based Alert Correlation Algorithms For DER Cyber Situational Awareness," 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2024, pp. 1-5, doi: 10.1109/ISGT59692.2024.10454168.

3. ML-based Anomaly Detection System (Edge-CSA)

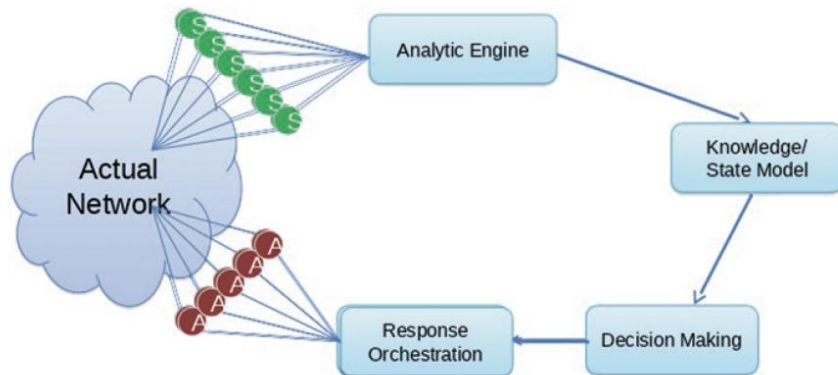
- ML-ADS monitors the DER network and generates alerts in the **Intrusion Detection Message Exchange Format (IDMEF)**.
- Generated IDMEF Alerts are aggregated based on a sliding time window.
- Aggregated Alerts are forwarded to the Cloud CSA Platform.



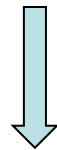
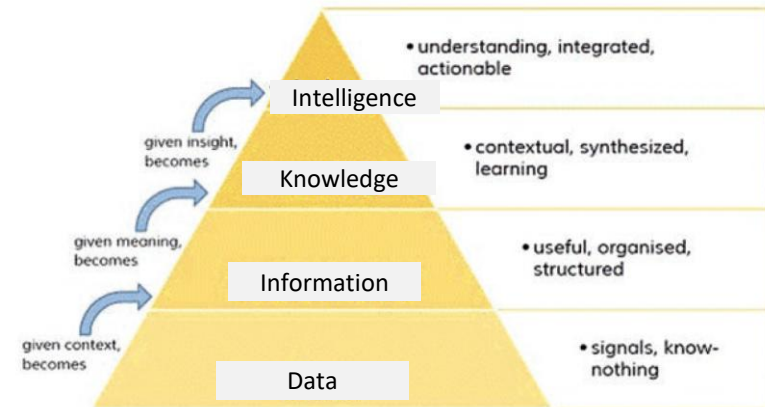
Ref: S. Bhattacharya, N. Saqib and M. Govindarasu, "ML-based Anomaly Detection System for IEC 61850 Communication in Substations," 2024 IEEE Power & Energy Society General Meeting (PESGM), Seattle, WA, USA, 2024, pp. 1-5, doi: 10.1109/PESGM51994.2024.10688773.

4. From DER Situational Awareness to Intelligence

Cyber-defense monitoring and decision-making feedback loop



Data-to-Intelligence Pyramid

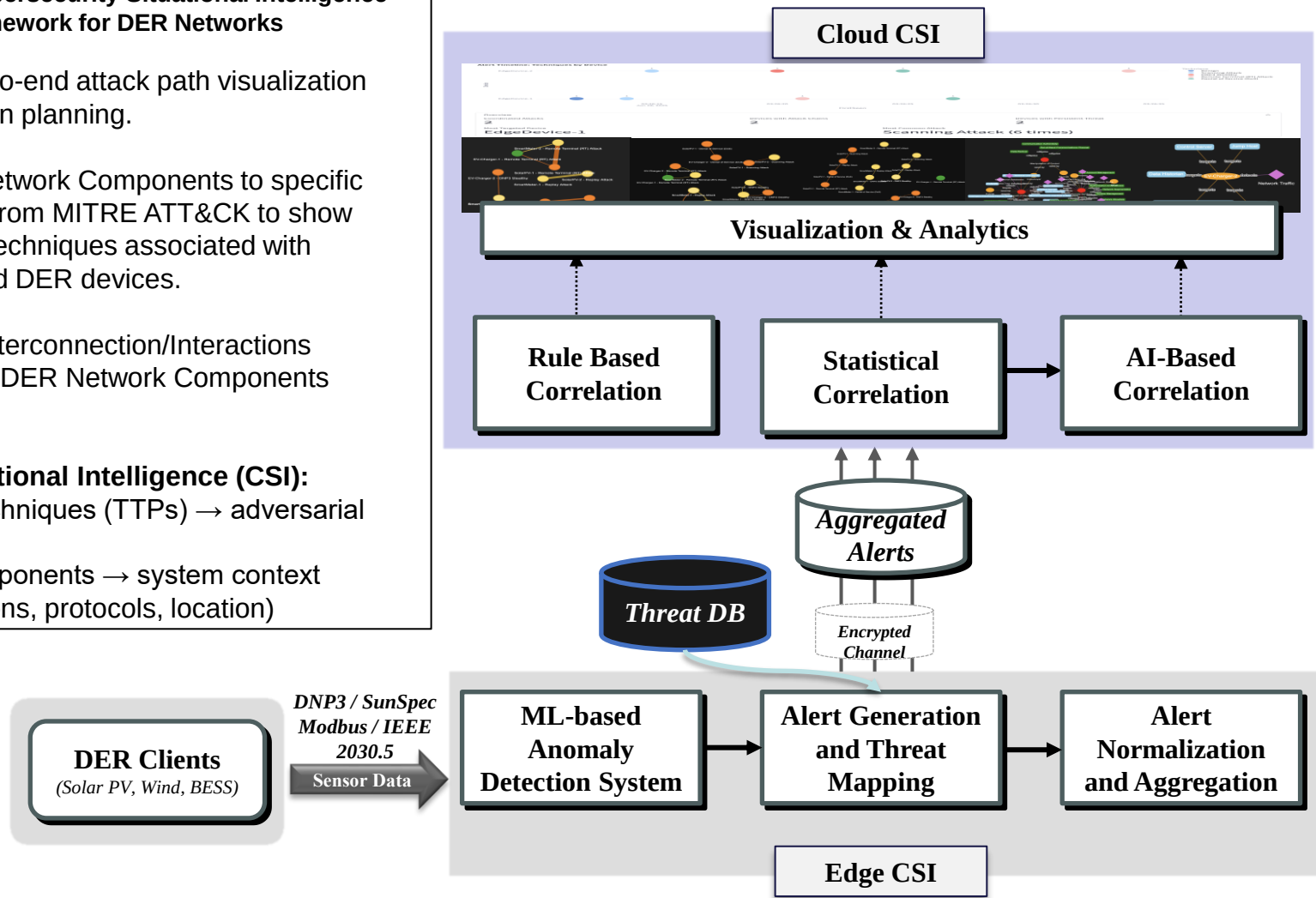


- **Data**: Raw security logs and alerts.
- **Information**: Structured security events, e.g, detected anomalies.
- **Knowledge**: Contextualized threats with relationships (Knowledge Graph).
- **Intelligence**: Actionable intelligence with mitigation strategies (LLM-enhanced).
- **Security Orchestration & Automated Response (SOAR)**: Autonomous Agentic AI security response.

4. Proposed CySIDER Framework

CySIDER: Cybersecurity Situational Intelligence Framework for DER Networks

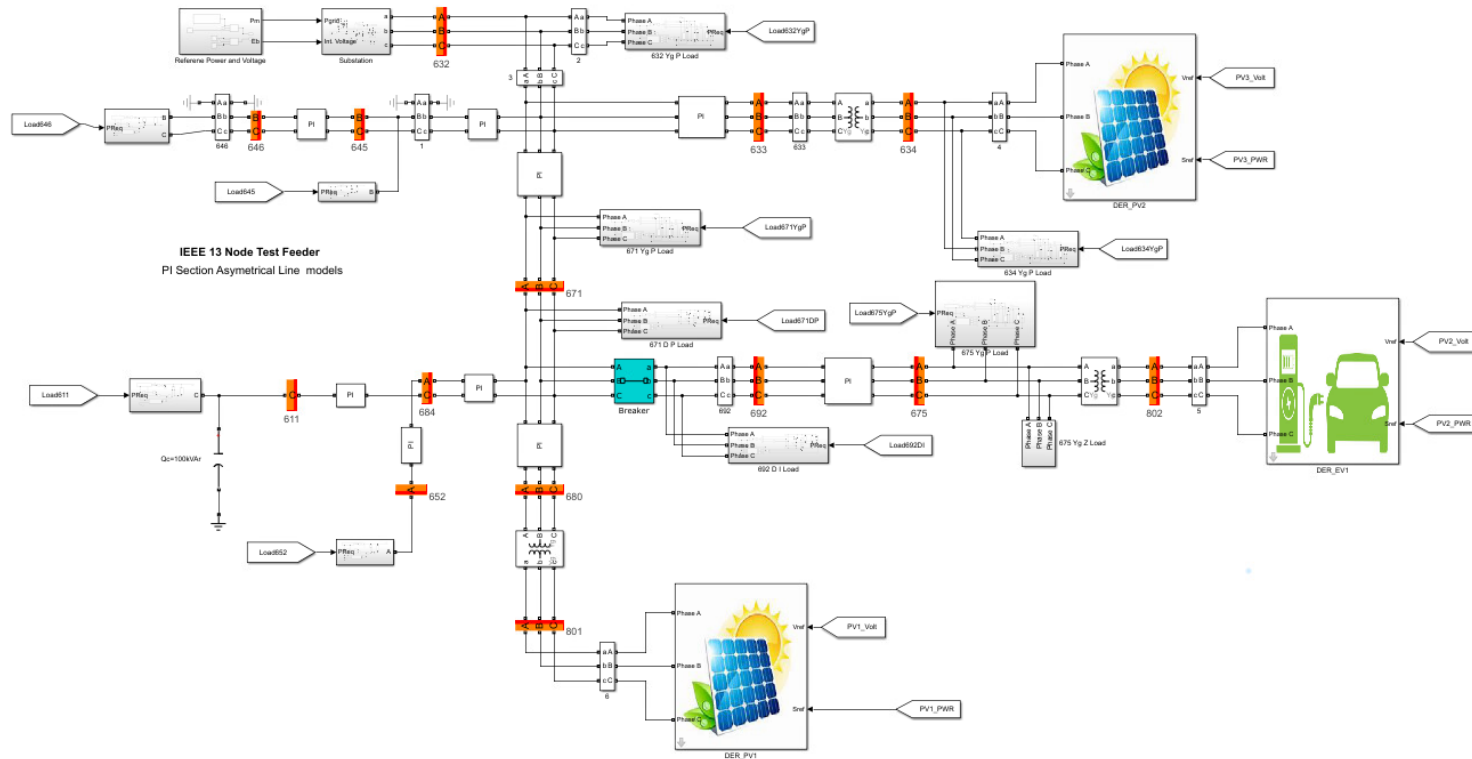
- ✓ Enable end-to-end attack path visualization and mitigation planning.
- ✓ Map DER Network Components to specific Techniques from MITRE ATT&CK to show adversarial techniques associated with compromised DER devices.
- ✓ Define the interconnection/Interactions between the DER Network Components
- ✓ **Cyber Situational Intelligence (CSI):**
 - Attack Techniques (TTPs) → adversarial behavior
 - DER Components → system context (connections, protocols, location)



Ref: D. Popoola, S. Bhattacharya, and M. Govindarasu, "CySIDER: Cybersecurity Situational Intelligence Framework for DER Networks," submitted for review 2025 Resilience Week (RWS), National Harbor, MD, USA, 2025.

Sample DER-integrated Distribution Grid for Experimental Evaluation

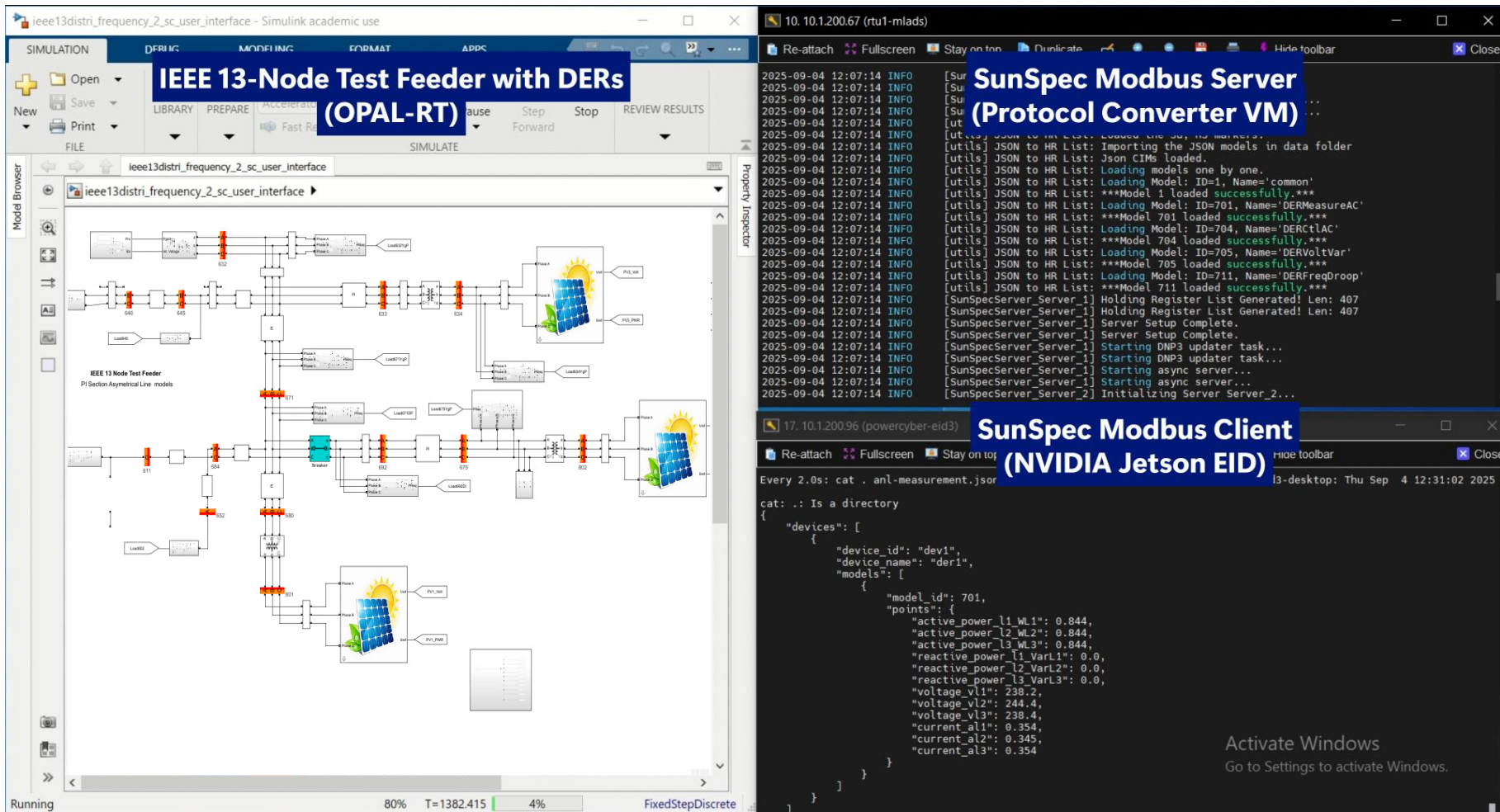
IEEE 13-node Test Feeder with DERs



- Distribution network model, both primary distribution of 4.16 kV and secondary distribution of 240V per phase.
- 3 DERs (2 PVs and 1 EV) are connected using a 4.16kV/480V transformer to the primary distribution section.
- PV plant is modeled using the NERC DERA model, with the following control functions inside for: Power, Voltage, and Q Control based on the user selection.

Ref: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/DERStudyReport.pdf

1. Real-time Implementation of DER Protocol Converter



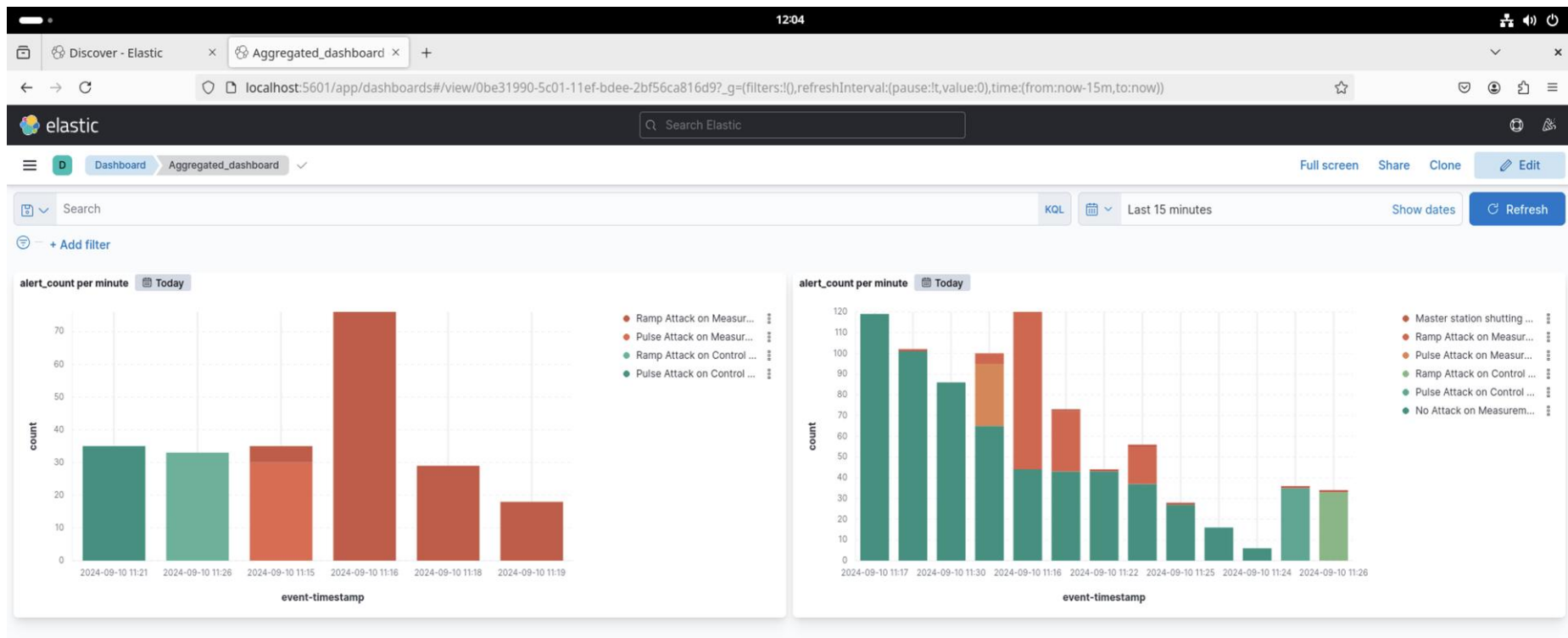
The image displays a real-time implementation setup for DER protocol conversion, consisting of three main components:

- IEEE 13-Node Test Feeder with DERs (OPAL-RT):** A Simulink model showing the IEEE 13-Node Test Feeder with various DERs (Distributed Energy Resources) connected to the network. The model includes components like PV modules, inverters, and controllers. The status bar indicates the simulation is running at 80% completion, with a temperature of 1382.415 and a 4% progress bar.
- SunSpec Modbus Server (Protocol Converter VM):** A terminal window showing the server's operation. It lists loaded models and their IDs, such as DERMeasureAC (ID=701), DERCtrlAC (ID=704), DERVoltVar (ID=705), and DERFreqDrop (ID=711). The server is also shown generating and updating the DNP3 Holding Register List.
- SunSpec Modbus Client (NVIDIA Jetson EID):** A terminal window showing the client's operation. It displays the JSON output of the measurement data, including active power, reactive power, voltage, and current for various DERs.

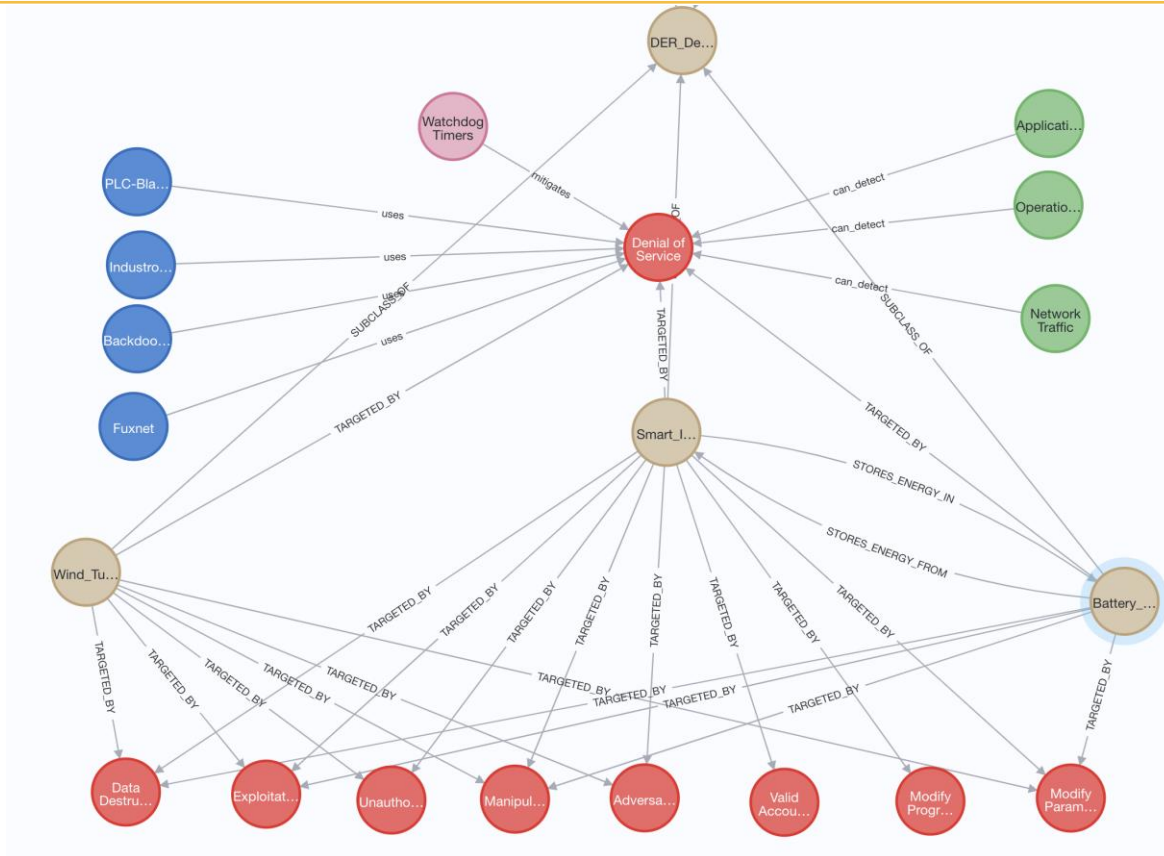
```
cat: ./: Is a directory
{
  "devices": [
    {
      "device_id": "dev1",
      "device_name": "der1",
      "models": [
        {
          "model_id": 701,
          "points": {
            "active_power_l1_WL1": 0.844,
            "active_power_l2_WL2": 0.844,
            "active_power_l3_WL3": 0.844,
            "reactive_power_l1_VarL1": 0.0,
            "reactive_power_l2_VarL2": 0.0,
            "reactive_power_l3_VarL3": 0.0,
            "voltage_vL1": 238.2,
            "voltage_vL2": 244.4,
            "voltage_vL3": 238.4,
            "current_al1": 0.354,
            "current_al2": 0.345,
            "current_al3": 0.354
          }
        }
      ]
    }
  ]
}
```

2 & 3. Cloud CSA - Real-time Situational Awareness Dashboard

- Aggregated Alerts are forwarded to the Cloud via an encrypted MQTT channel.
- Alerts are stored in Logstash and parsed to visualize on the Kibana Dashboard.



4. CSI - Knowledge Graph-driven Alert Correlation



Semantic Enrichment

Alerts enriched with contextual information about devices, vulnerabilities, and attack techniques from the knowledge graph.

Key Knowledge Graph Elements



Attack Techniques



Device Types



Vulnerabilities



Mitigations



Relationships

Device-Specific Analysis

Targeted extraction of device-specific attack paths enables focused security analysis and prioritized remediation.

Mitigation Guidance

Knowledge graph links attacks to specific mitigation strategies, enabling faster and more effective incident response.

4. CSI - AI-based Threat Intelligence

Rules

Decision rules from security systems

Mitigation

STIX-based mitigation strategies

Asset, Infrastructure

System inventory and architecture

Threat-Actor

Known threat actor profiles and TTPs

Observed-Data

Real-time security telemetry

LLM

Correlation & Incident Summary

Based on the high risk score and alerts for the device, it's subject to critical threats, including DNP3 Stealthy, Denial of Service (DoS) attacks, and Replay Attacks. These techniques can disrupt energy operation, manipulate data, and enable unauthorized access, which could potentially lead to catastrophic outcomes for the distributed energy resources.

Immediate action steps are:

1. Strengthen authentication processes to thwart the DNP3 Stealthy attacks. This includes stronger passwords and implementing multi-factor authentication.
2. Expand network monitoring to spot anomalous activities, which provides protection against DoS attacks.
3. Introduce network segmentation and timely system updates to protect against Replay Attacks.
4. Conduct a detailed security audit to identify other potential vulnerabilities and establish new mitigation strategies.
5. Lastly, consider creating an incident response plan specifically for these threats to minimize disruption in the future.



Input Processing

The LLM ingests structured and unstructured data from multiple security sources, normalizing formats and extracting key entities and relationships.



Contextual Analysis

By correlating across data sources, the LLM establishes context between threats, assets, and mitigations that might otherwise remain disconnected.

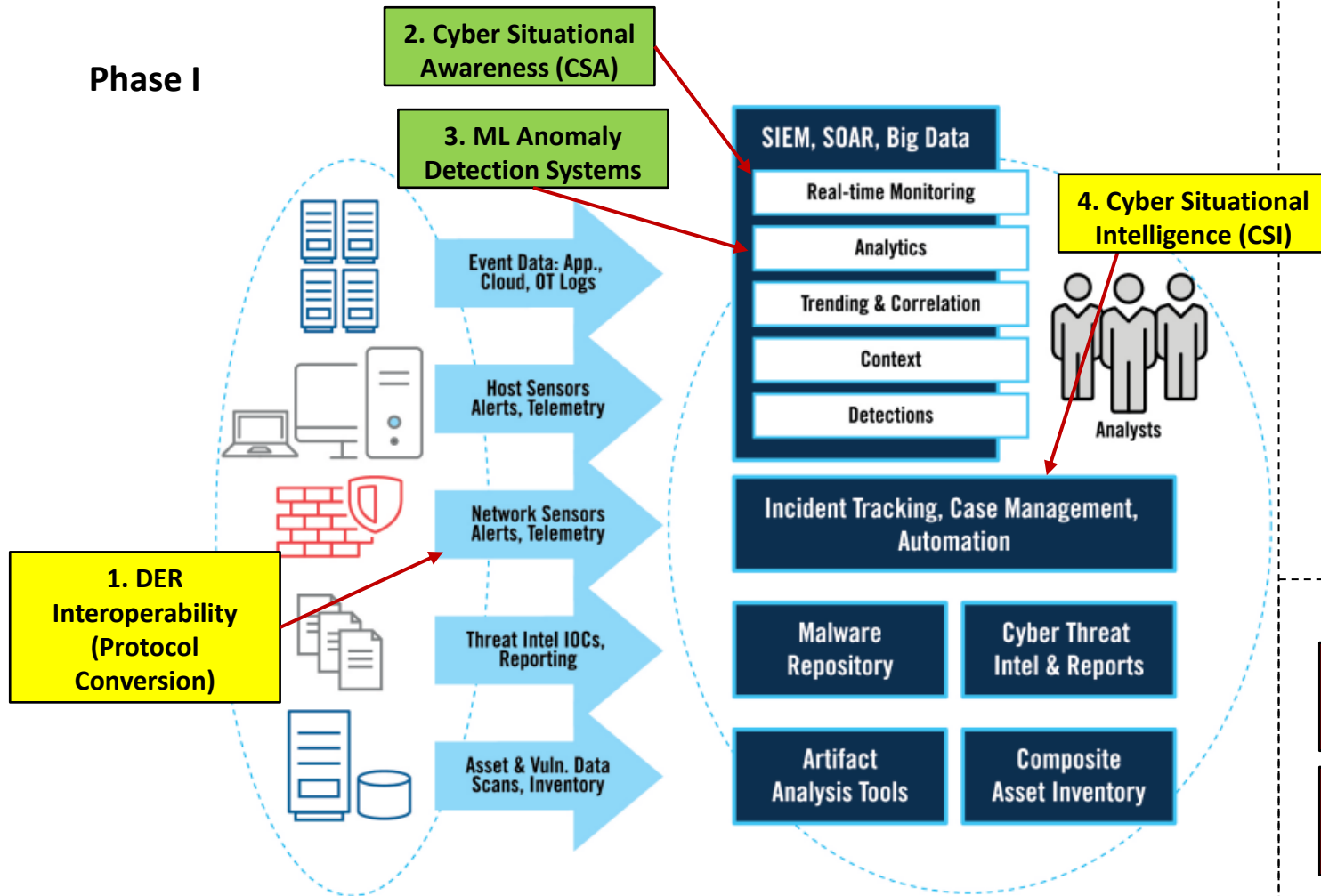


Actionable Output

The LLM transforms technical data into prioritized, human-readable intelligence with specific mitigation steps tailored to the organization's environment.

Conclusion & Future Work

Phase I



Phase II

5. System Integration

6. Tech Transfer & Field Demonstration

Cybersecure Power Grid via Online Change Detection



Arnab Dey



Soham Chakraborty



Mohammed Tuhin
Rana

Murti V Salapaka

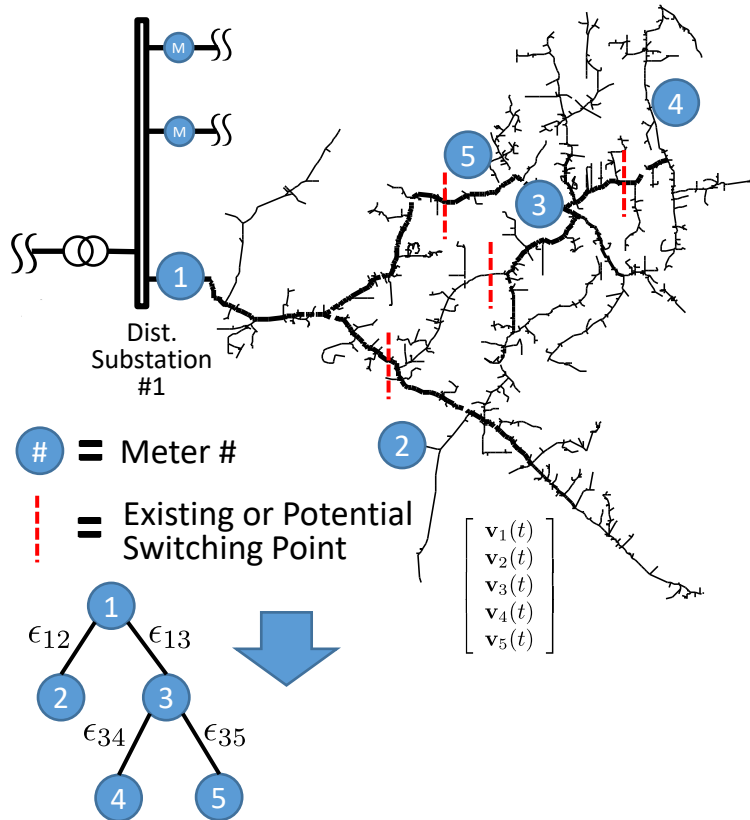
Electrical Engineering Department
University of Minnesota, Twin-Cities

<https://salapakalab.ece.umn.edu>

murtis@umn.edu

Support: CyDerms: DE-CR0000040, NSF: ECCS 2412435

Grid Data Analytics: Situational Awareness



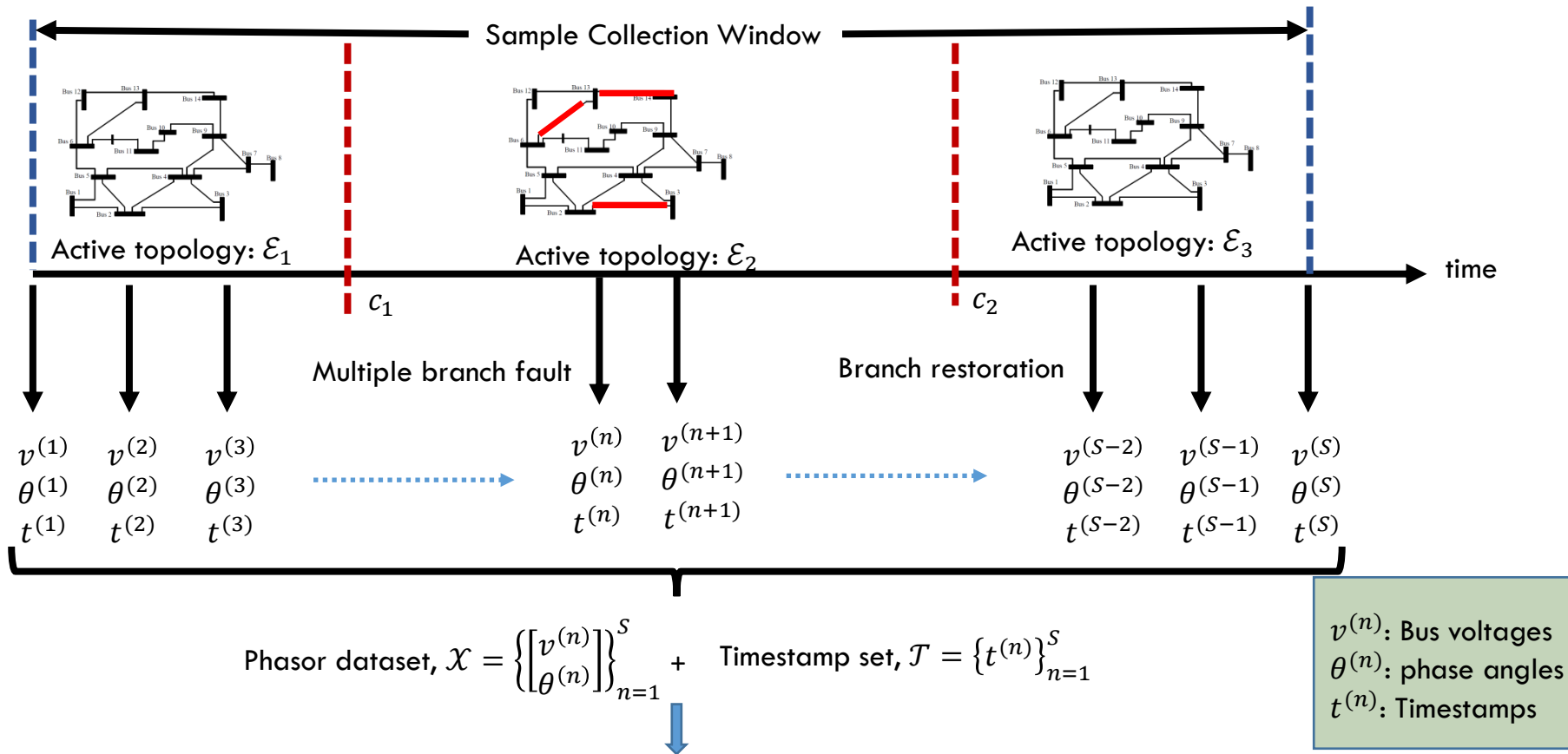
■ Aim:

- Obtain state awareness
- Fault detection
- Grid monitoring

■ Challenges

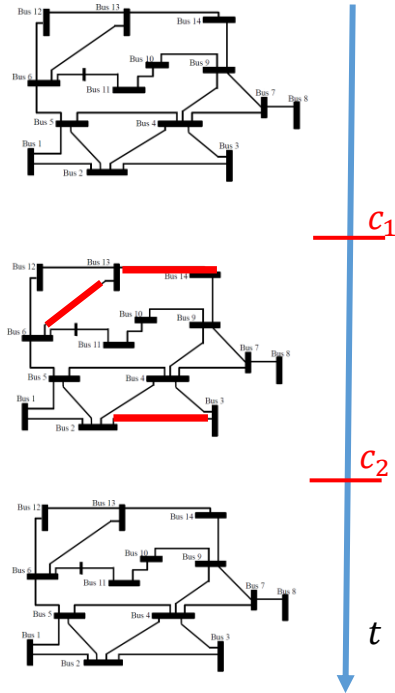
- Topology only partially known
- Changing with time
- Partial measurements
- Active probing impractical
- Latent Nodes
- Paucity of data

Scenario



Given data determine (1) When change occurs (2) Estimate topology effective between changes

Problem Description



- From phasor data with timestamps:
 - Detect number of topologies: K
 - Estimate total no. of changes and change instants: C and $\{c_i\}_{i=1}^C$
 - Localize changes: By estimating $\{\mathcal{E}_i\}_{i=1}^K$
- Control center:
 - does not know K , $\{\mathcal{E}_i\}_{i=1}^K$, and C , $\{c_i\}_{i=1}^C$, a priori
 - Has access to phasor data

A1: Determine Number of Topologies and Optimal Parameters

Input Data: phasor data and associated time-stamps

Output: (1) Number of topologies (2) Assign phasor measurement to most likely topology

Notation

- $\mathbf{X} = [\mathbf{v}^T \ \boldsymbol{\theta}^T]^T$: The vector of phasor measurements at all N nodes
 - $\mathbf{x}^{(n)}$: the vector of phasor measurement at time $t^{(n)}$.
 - Consider the case where there are K topologies.
 - Let $\mathbf{Z} = [z_1 \ z_2 \ \dots \ z_K]^T$ be a K -dimensional random vector of indicator variables
 - Z can take values in $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_K\}$
 - $\mathbf{e}_k = [0 \ \dots \ 0 \ 1 \ 0 \ \dots \ 0]^T \in \mathbb{R}^K$: Standard basis vectors of $\mathbb{R}^K$
 - Event $\{\mathbf{Z} = \mathbf{e}_k\}$ represents topology is k^{th} topology with probability
- Probability density X takes value x under k^{th} topology:

$$f_{X|\mathbf{Z}, \boldsymbol{\phi}_k}(\mathbf{x} | \mathbf{Z} = \mathbf{e}_k) = \frac{1}{(2\pi)^N |\boldsymbol{\Sigma}_k|^{\frac{1}{2}}} e^{-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k^{-1} (\mathbf{x} - \boldsymbol{\mu}_k)}$$

where $\boldsymbol{\phi}_k := (\boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)$

Probability Distribution of Phasor Data

- Probability distribution function of X_K

$$f_{X|\Phi_K}(\mathbf{x}) = \sum_{k=1}^K \pi_k f_{X|Z, \phi_k}(\mathbf{x} | Z = \mathbf{e}_k) \frac{e^{-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k^{-1} (\mathbf{x} - \boldsymbol{\mu}_k)}}{(2\pi)^N |\boldsymbol{\Sigma}_k|^{\frac{1}{2}}}$$

Annotations: Red arrows point from $\mathbb{P}[Z = \mathbf{e}_k]$ to π_k and from the Gaussian term to ϕ_k .

- Parameter: $\Phi_K := (\pi_1, \pi_2, \dots, \pi_K, \phi_1, \phi_2, \dots, \phi_K)$

- log-likelihood is

$$\mathcal{L}(\Phi_K | \mathcal{X}) := \ln(\prod_{n=1}^S f_{X|\Phi_K}(\mathbf{x}^{(n)}))$$

- Solve

$$\hat{\Phi}_K = \underset{\Phi_K}{\operatorname{argmax}} \mathcal{L}(\Phi_K | \mathcal{X})$$

Annotation: A red arrow points from $\operatorname{argmax}_{\Phi_K}$ to the data set in the next block.

such that $\sum_{k=1}^K \pi_k = 1, \pi_k \geq 0$.

Annotation: Red text "Data" is above the sum, and red arrows point from the data set to the π_k terms.

- Hard to solve

Probability Distribution of Phasor Data

- $f_{X|\Phi_K}(x) = \sum_{k=1}^K \pi_k f_{X|Z, \phi_k}(x|Z = e_k)$

- Parameter: $\Phi_K := (\pi_1, \pi_2, \dots, \pi_K, \phi_1, \phi_2, \dots, \phi_K)$

- log-likelihood is

$$\mathcal{L}(\Phi_K|\mathcal{X}) := \ln\left(\prod_{n=1}^S f_{X|\Phi_K}(x^{(n)})\right)$$

- Solve

$$\hat{\Phi}_K = \operatorname{argmax}_{\Phi_K} \mathcal{L}(\Phi_K|\mathcal{X})$$

$$\text{such that } \sum_{k=1}^K \pi_k = 1, \pi_k \geq 0.$$

- Hard to solve.

- Suppose an estimate, Φ_K^ℓ of $\widehat{\Phi}_K$ is available.

- $h_k^{n,\ell} :=$ likelihood that n^{th} data, $x^{(n)}$ comes from topology k

$$\bullet h_k^{n,l} = \frac{\pi_k^l |\Sigma_k^l|^{-0.5} e^{-0.5(x^{(n)} - \mu_k^l)^T (\Sigma_k^l)^{-1} (x^{(n)} - \mu_k^l)}}{\sum_{k=1}^K \pi_k^l |\Sigma_k^l|^{-0.5} e^{-0.5(x^{(n)} - \mu_k^l)^T (\Sigma_k^l)^{-1} (x^{(n)} - \mu_k^l)}}$$

- Maximization

$$\Phi_K^{l+1} = \operatorname{argmax}_{\Phi_K} \sum_{n=1}^S \left[\mathbb{E}_{Z \sim f_{Z|X, \Phi_K^l}} [\ln(f_{X,Z|\Phi_K}(x^{(n)}, Z)) | X = x^{(n)}] \right]$$

$$\text{such that } \sum_{k=1}^K \pi_k = 1, \pi_k \geq 0.$$

$$\bullet \pi_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l}}{S}$$

$$\bullet \mu_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l} x^{(n)}}{\sum_{n=1}^S h_k^{n,l}}, \Sigma_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l} (x^{(n)} - \mu_k^{l+1})(x^{(n)} - \mu_k^{l+1})^T}{\sum_{n=1}^S h_k^{n,l}}$$

Algorithm Iterations

- Given parameter $\Phi_K^\ell := (\pi_1^\ell, \pi_2^\ell, \dots, \pi_K^\ell, \mu_1^\ell, \dots, \mu_K^\ell, \Sigma_1^\ell, \dots, \Sigma_K^\ell)$ determine

$$h_k^{n,l} = \frac{\pi_k^\ell |\Sigma_k^\ell|^{-0.5} e^{-0.5(x^{(n)} - \mu_k^\ell)^T (\Sigma_k^\ell)^{-1} (x^{(n)} - \mu_k^\ell)}}{\sum_{k=1}^K \pi_k^\ell |\Sigma_k^\ell|^{-0.5} e^{-0.5(x^{(n)} - \mu_k^\ell)^T (\Sigma_k^\ell)^{-1} (x^{(n)} - \mu_k^\ell)}}.$$

- update:**

$$\pi_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l}}{S}, \mu_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l} x^{(n)}}{\sum_{n=1}^S h_k^{n,l}}, \Sigma_k^{l+1} = \frac{\sum_{n=1}^S h_k^{n,l} (x^{(n)} - \mu_k^{l+1})(x^{(n)} - \mu_k^{l+1})^T}{\sum_{n=1}^S h_k^{n,l}}.$$

- Iterate till Convergence:**

- $|\mathcal{L}(\Phi_K^{l+1}|\mathcal{X}) - \mathcal{L}(\Phi_K^l|\mathcal{X})| \leq \epsilon$
 - $\mathcal{L}(\Phi_K|\mathcal{X}) := \ln(\prod_{n=1}^S f_{X|\Phi_K}(x^{(n)}))$

Closed form for iterates. Thus, very fast

Estimating Number of Topologies

Use Silhouette Score

- For each value of $K \in \{1, \dots, \overline{K}\}$, after running EM
 - we have estimates of which sample belongs to which topology (classification)
- $\mathcal{X}_k := \left\{ \mathbf{x}^{(n)} : k = \arg \max_{k \in \{1, \dots, K\}} \mathbb{P}[\mathbf{Z} = \mathbf{e}_k | \mathbf{X} = \mathbf{x}^{(n)}, \hat{\Phi}_K] \right\}$
 - Set of phasor samples classified under topology k after running EM

Likelihood that n^{th} phasor comes from k^{th} topology
- Suppose, $\mathbf{x}^{(n)} \in \mathcal{X}_k$
- $s(\mathbf{x}^{(n)})$: Silhouette score of $\mathbf{x}^{(n)}$
- Silhouette score assesses the optimal number of classes by analyzing
 - Mean intra-class distance
 - Mean inter-class distance

Algorithm

Algorithm 1: Topology change detection

```

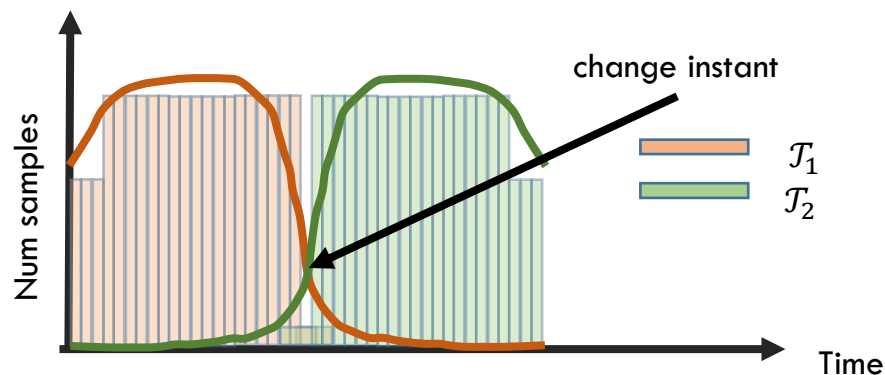
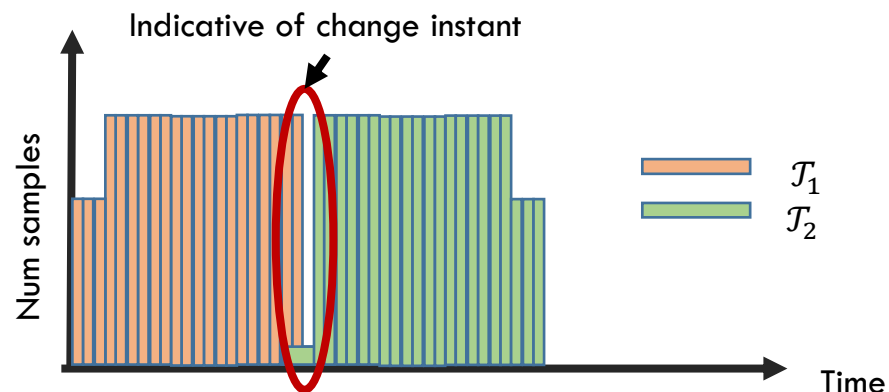
Function detectChanges ( $\mathcal{X} = \{\mathbf{x}^{(n)}\}_{n=1}^S, \bar{K}, \bar{l}, s_{th}, \epsilon$ ):
  for  $K = 1$  to  $\bar{K}$  do
    for  $l = 0$  to  $\bar{l}$  do
      Initialize  $\Phi_K^0$ ;
       $\mathcal{L}(\Phi_K^0 | \mathcal{X}) \leftarrow \sum_{n=1}^S \ln [f_{\mathbf{X} | \Phi_K^0}(\mathbf{x}^{(n)})]$ ;
      for  $k = 1$  to  $K$  do
        /* E-step */
        for  $n = 1$  to  $S$  do
          Compute  $h_k^{n,l}$  using (10);
        end
        /* M-step */
        Compute  $\pi_k^{l+1}, \mu_k^{l+1}$ , and  $\Sigma_k^{l+1}$  using (13);
      end
       $\mathcal{L}(\Phi_K^{l+1} | \mathcal{X}) \leftarrow \sum_{n=1}^S \ln [f_{\mathbf{X} | \Phi_K^{l+1}}(\mathbf{x}^{(n)})]$ ;
       $\hat{\Phi}_K \leftarrow \Phi_K^{l+1}; \hat{\mathcal{L}}_K(\hat{\Phi}_K | \mathcal{X}) \leftarrow \mathcal{L}(\Phi_K^{l+1} | \mathcal{X}); \hat{l} \leftarrow l;$ 
      if  $|\mathcal{L}(\Phi_K^{l+1} | \mathcal{X}) - \mathcal{L}(\Phi_K^l | \mathcal{X})| \leq \epsilon$  then
        break;
      end
      /* Computation of silhouette score */
      if  $K \neq 1$  then
        Compute the average silhouette score  $s_K$ ;
      end
    end
     $\hat{K} \leftarrow \operatorname{argmax}_{K \in \{2, \dots, \bar{K}\}} s_K$ ;
    if  $s_{\hat{K}} \leq s_{th}$  then
       $\hat{K} = 1$ ;
    end
    for  $n = 1$  to  $S$  do
       $k^{(n)} \leftarrow \operatorname{argmax}_{k \in \{1, \dots, \hat{K}\}} h_k^{n, \hat{l}}$ ;
    end
  return  $\hat{K}, \hat{\Phi}_{\hat{K}}, \{k^{(n)}\}_{n=1}^S$ ;

```

Estimating Change Instants

Change Instant Detection: Idea

- We know the optimal likelihood topology that the $x^{(n)}$ comes from given by $k^{(n)}$.
- If we plot histograms of timestamps for each $\mathcal{T}_k$
- The overlapping regions between the histograms indicate the change instants
- We smoothen the histogram to approximate the density function of samples in $\mathcal{T}_k$
- The crossover point is representative of the change instant



Change instants detection: an example with two topologies

Algorithm for Change Instants Determination

Algorithm 2: Change instant detection

```
Function getChangeInstants  
( $\mathcal{T} = \{t^{(n)}\}_{n=1}^S, \hat{K}, h, K_r(\cdot), \overline{C}, \epsilon_n$ ):  
    /* Initialization */  
     $\mathcal{C} \leftarrow []$ ;  $j \leftarrow 0$ ;  
    for  $k = 1$  to  $\hat{K}$  do  
         $\mathcal{L}_k \leftarrow \text{zeroes}(S)$ ;  
        Compute  $\mathcal{T}_k$ ;  
        for  $n = 1$  to  $S$  do  
             $\mathcal{L}_k[n] \leftarrow \ln [\hat{f}_{T|k}(t^{(n)})]$ ;  
        end  
    end  
    for  $k_1 = 1$  to  $\hat{K} - 1$  do  
        for  $k_2 = k_1 + 1$  to  $\hat{K}$  do  
             $d \leftarrow |\mathcal{L}_{k_1} - \mathcal{L}_{k_2}|$ ;  
             $d_s \leftarrow \text{argsort } d \text{ in ascending order}$ ;  
            for  $i = 0$  to  $\overline{C}$  do  
                if  $i == 0$  then  
                    Append  $c_j = t^{(d_s[i])}$  to  $\mathcal{C}$ ;  $j \leftarrow j + 1$ ;  
                end  
                else  
                     $q \leftarrow |t^{(d_s[i])} - t^{(d_s[i-1])}|$ ;  
                    if  $q \geq \epsilon_n$  then  
                        Append  $c_j = t^{(d_s[i])}$  to  $\mathcal{C}$ ;  $j \leftarrow j + 1$ ;  
                    end  
                end  
            end  
        end  
    end  
    return  $\mathcal{C}$ ;
```

Estimating the k^{th} Topology

Determine Topology from Precision Matrix

Algorithm 3: Learning Grid Topology [17]

```

Function getTopology ( $\{\hat{\Sigma}_k\}_{k=1}^{\hat{K}}, \tau \in \mathbb{R}^+, \mathcal{V}$ ):
    for  $k = 1$  to  $\hat{K}$  do
         $\mathcal{E}_k \leftarrow \phi$ ;
         $\begin{bmatrix} J_{VV,k} & J_{V\theta,k} \\ J_{\theta V,k} & J_{\theta\theta,k} \end{bmatrix} \leftarrow \text{inverse}(\hat{\Sigma}_k)$ ;
        foreach  $i, j \in \mathcal{V}$  do
            if  $J_{VV,k}(i, j) + J_{\theta\theta,k}(i, j) < -\tau$  then
                 $\mathcal{E}_k \leftarrow \mathcal{E}_k \cup \{\{i, j\}, \{j, i\}\}$ ;
            end
        end
    end
    return  $\{\mathcal{E}_k\}_{k=1}^{\hat{K}}$ ;

```

Linearized model

- $X = \begin{bmatrix} v \\ \theta \end{bmatrix} = H_{\mathcal{E}_k}^{-1} \begin{bmatrix} p \\ q \end{bmatrix}$
- $H_{\mathcal{E}_k} := \begin{bmatrix} H_{\mathcal{E}_k, g} & H_{\mathcal{E}_k, \beta} \\ H_{\mathcal{E}_k, \beta} & -H_{\mathcal{E}_k, g} \end{bmatrix}$
- $\mu_k = H_{\mathcal{E}_k}^{-1} \mu_{pq}; \Sigma_k = H_{\mathcal{E}_k}^{-1} \Sigma_{pq} H_{\mathcal{E}_k}^{-1}$

Nodes active and reactive power mutually independent

- Quality of reconstruction is guaranteed

Aside

- With voltage magnitude only: possible for resistive grids



Dr. Deepjyoti Deka
MIT



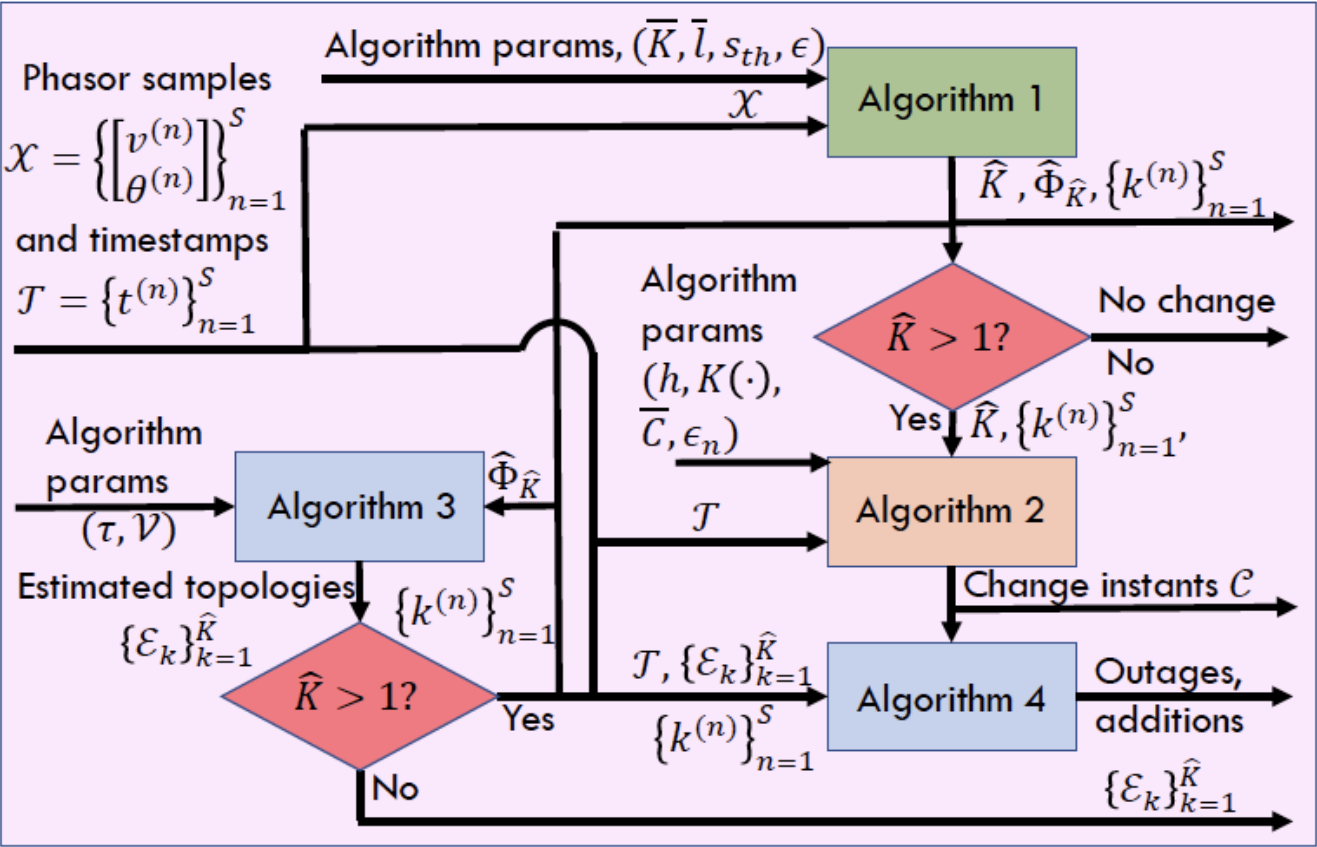
Dr. Saurav Talukdar
Verrus



Dr. Harish Doddi
Nvidia

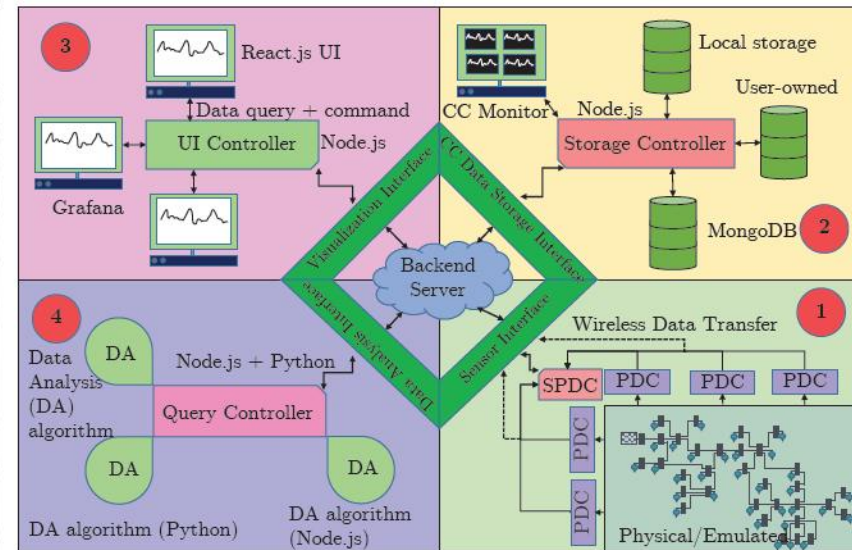
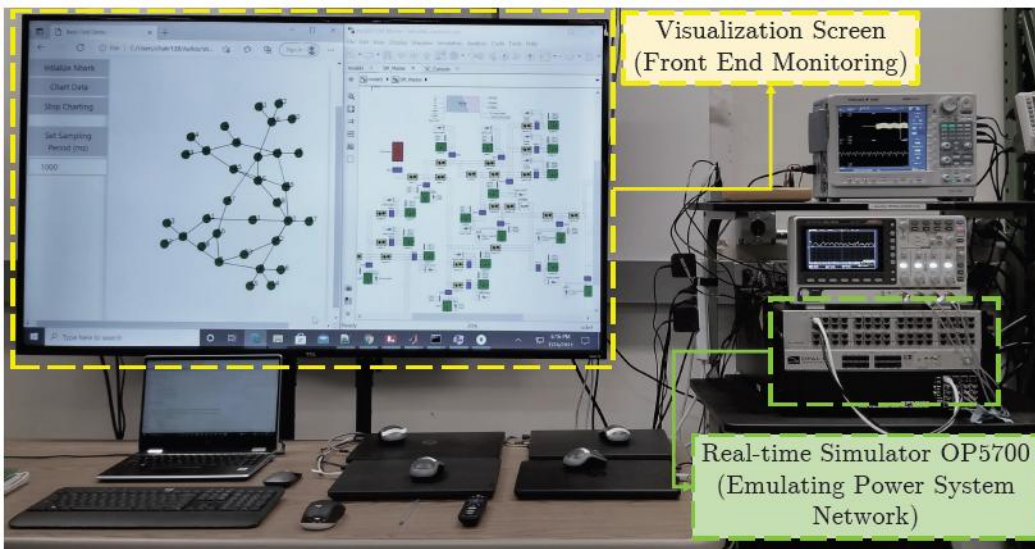
- Deka, Deepjyoti, Saurav Talukdar, Michael Chertkov, and Murti V. Salapaka. "Graphical models in meshed distribution grids: Topology estimation, change detection & limitations." IEEE Transactions on Smart Grid 11, no. 5 (2020): 4299-4310.

Flowchart



Experimental Results

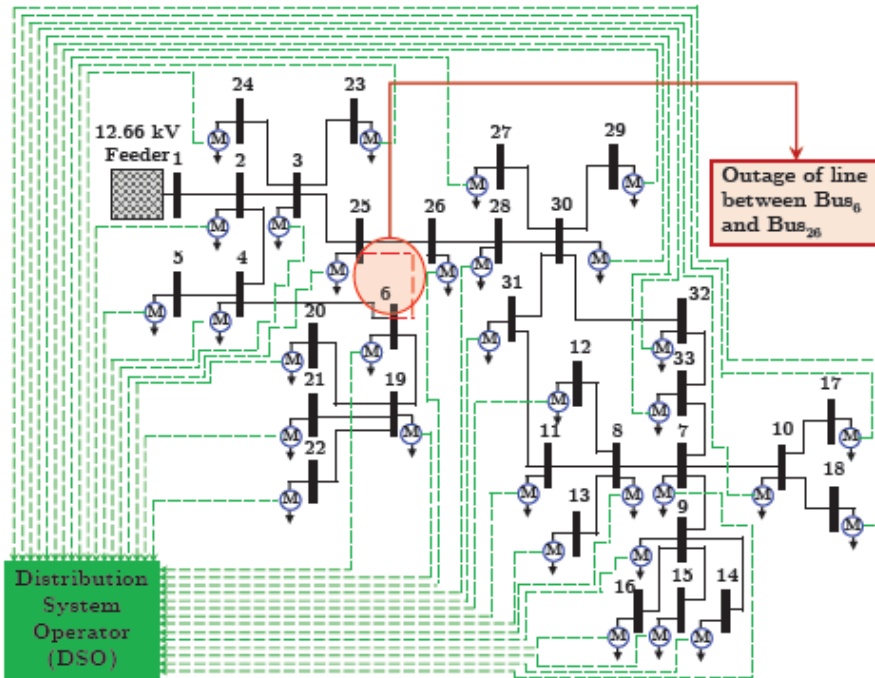
Experimental Set-Up



Software Components

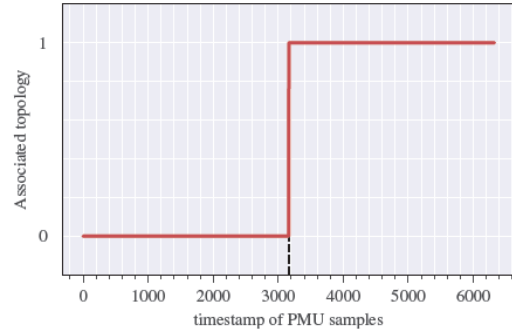
- OPAL-RT based real-time simulator.
- Custom built end to end cyber physical infrastructure for data collection, algorithm implementation and visualization.

Modified IEEE-33 Bus System

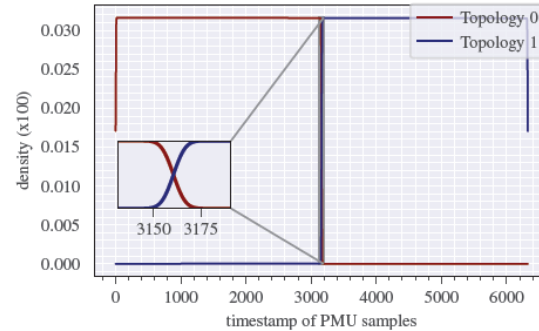


- Physical system
 - Number of buses: 33
 - Feeder voltage: 12.66 kV
 - Total active load: 3.7 MW
 - Total reactive load: 2.3 MVar
- Sensors
 - PMUs considered at
 - Each bus
 - Subset of buses (Latent nodes)
- Communication system
 - Centralized Control Center (CC)
 - Measurements sent wirelessly to CC

Experimental Results: IEEE-33 bus System

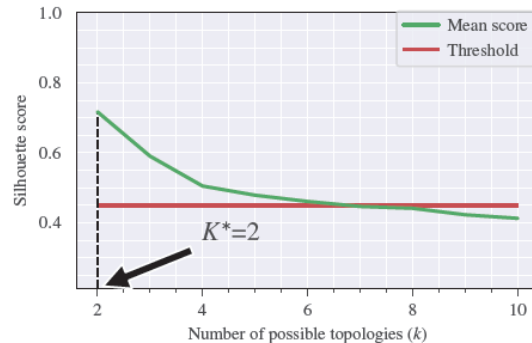


True time stamp of topology change



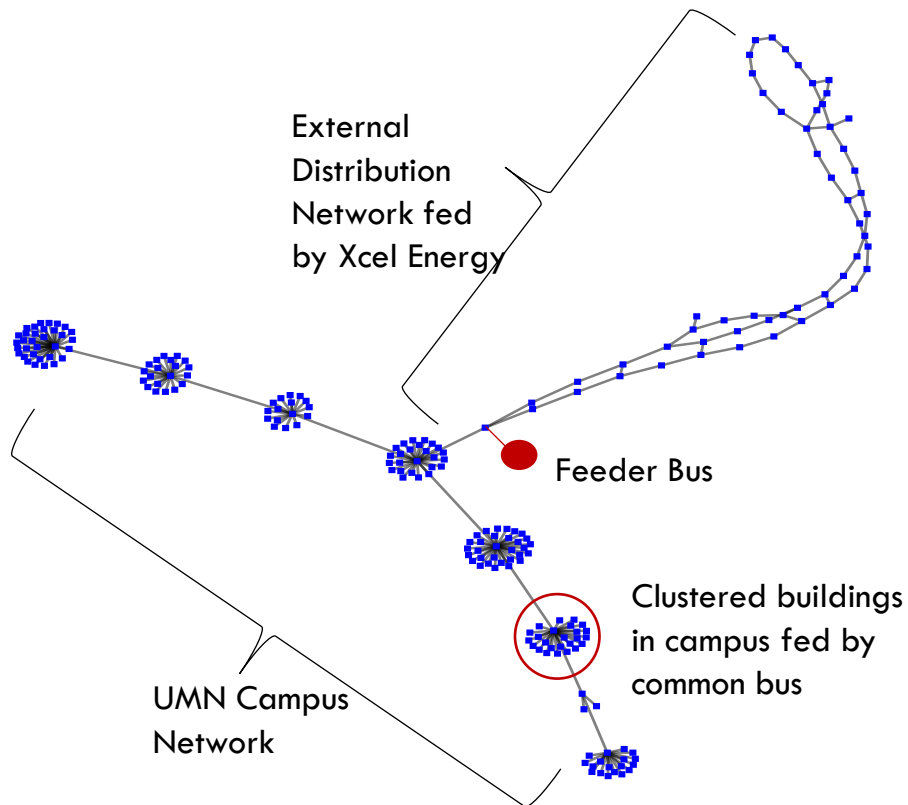
Density plot with estimated time stamp of change

- Line outage between bus 6 and 25 at timestamp value of 3160.
- Here $K = 2$.
- Density plot shows detected change instant as 3160.
- Silhouette score shows optimal K detected as 2.



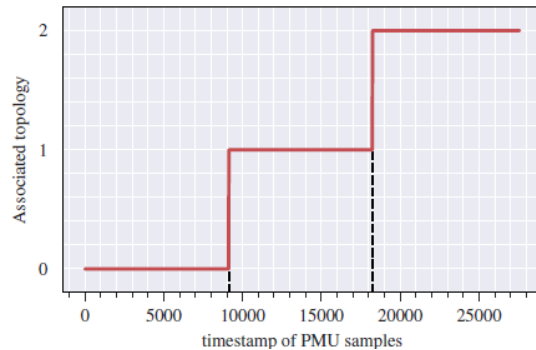
Silhouette score for different values of K

226-Bus System

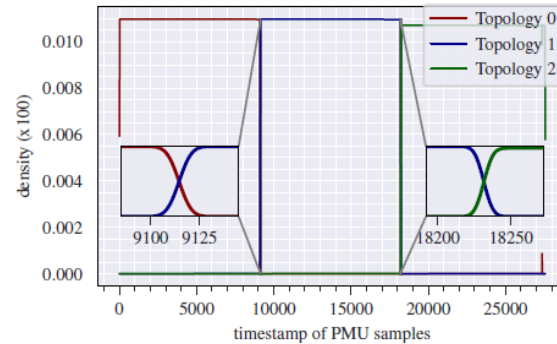


- Physical system
 - Number of buses: 226
 - Network provided by
 - UMN Energy Management Service
 - Xcel Energy
 - Voltage level: 13.8 kV
 - Total load: 5.12 MW
 - controllable, and non-controllable
 - 1 medical center of 700 kVA
 - Includes rooftop PV, battery
- Sensors
 - PMUs considered at each bus
- Communication system
 - Centralized Control Center (CC) at feeder
 - Measurements sent wirelessly to CC

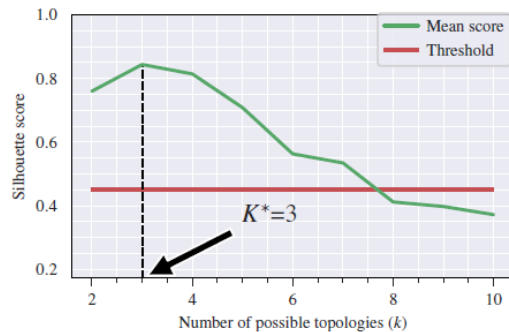
Experimental Results: 226-bus Network



True time stamp of topology change



Density plot with estimated time stamp of change



Silhouette score for different values of K

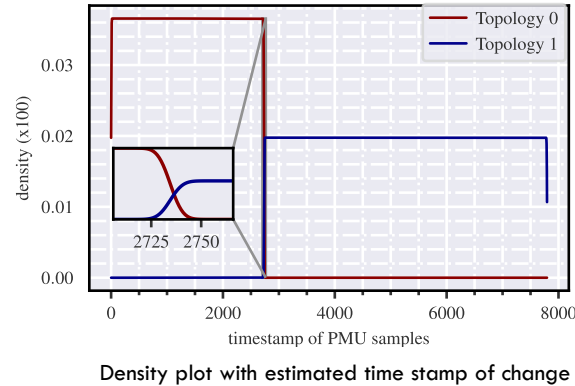
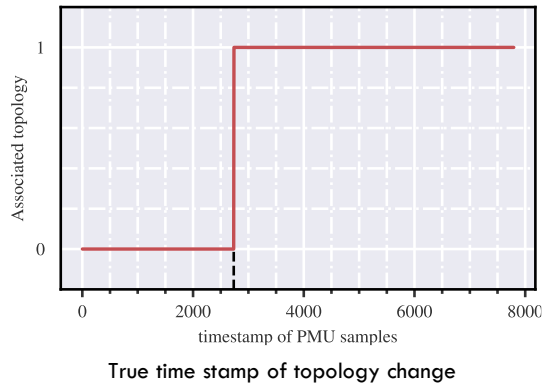
- Line outage between bus 104 and 204 and line addition between bus 106 and 206 at timestamps 9115 and 18232.
- Here $K = 3$.
- Density plot shows detected change instants as 9115 and 18232.
- Silhouette score shows optimal K detected as 3.

1262-Bus System

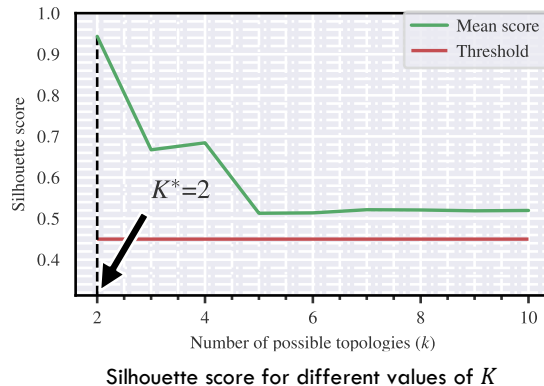


- Physical system
 - Number of buses: 1262
 - 'ckt7' of the large representative feeder, developed by the Electric Power Research Institute (EPRI)
 - Voltage level: 12.5 kV
 - 5964 customer loads
 - Primary length of network: 8 miles
- Sensors
 - PMUs considered at each bus
- Communication system
 - Centralized Control Center (CC)
 - Measurements sent wirelessly to CC

Experimental Results: 1262-bus Network



- Multiple line outage and addition at timestamp value of 2736.
- Here $K = 2$.
- Density plot shows detected change instant as 2736.
- Silhouette score shows optimal K detected as 2.



Experimental Results: 226-bus Network **Random Changes**

	Count	Accuracy (%)	False positive (%)	False negative (%)
Total changes	350	-	-	-
Correct detection	338	96.57	-	-
False detection	4	-	0.014	-
Missed detection	12	-	-	0.034

- 350 random changes including line addition and outage over a span of 1 hour.
- 96.57% of the random changes were detected correctly.

Conclusions

- An effective method determined for online change detection
 - Number and time instants of change
 - Topology estimation and location of changes

- Challenges
 - Need for sensing, Phasor measurements
 - Corrupted data (packet loss, noise in measurements, delays)



Thank you !

Acknowledgement:

Project funded by US Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response
(CESER) DOE Award: DE-CR0000040

Project Website:

<https://cyderms.iastate.edu/>