# Resilience at the Grid-Edge Using Trustable DERs

**Anuradha Annaswamy**

**Active-adaptive Control Laboratory**
**Department of Mechanical Engineering**

Massachusetts Institute of Technology

* Sponsors: US Department of Energy, MIT Energy Initiative

# There is a problem

## Ukraine Power Grid Attack (2015)


Impacted 225,000 customers

Source: Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

# There is a problem

## Ukraine Power Grid Attack (2015)

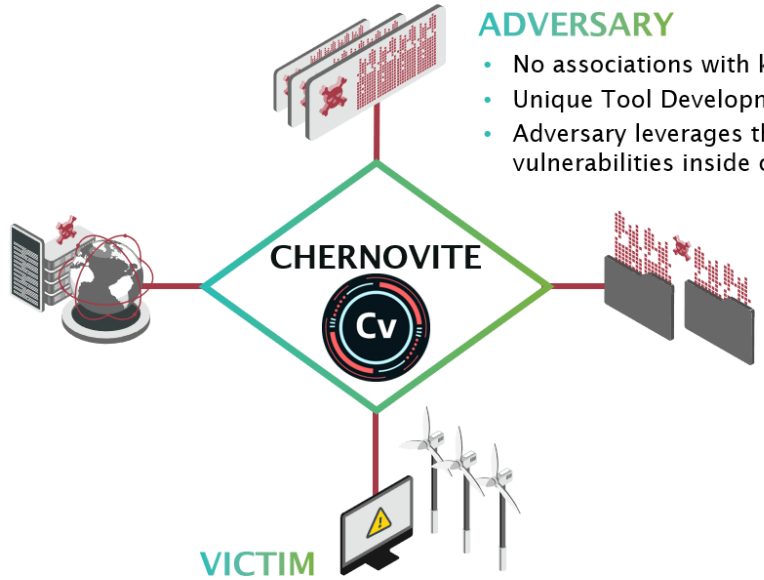

## CHERNOVITE'S PIPEDREAM

### IMPACT

- Loss of safety, availability, and control
- Manipulation of control
- ICS Kill Chain Stage 2 - Install/Modify; Execute ICS Attack

### INFRASTRUCTURE

- Utilizes victim PLCs, engineering workstations, and PLC control software for lateral movement and manipulation.
- Custom operational implant designed for command and control over SSL.




### ADVERSARY

- No associations with known activity groups
- Unique Tool Development
- Adversary leverages the exploitation of vulnerabilities inside of its capabilities.

### CAPABILITIES

- Custom capabilities for manipulating and disabling PLCs.
- Custom capabilities using ICS-specific protocols for internal reconnaissance and manipulation.
- Custom interactive operational capability to perform system enumeration, issue WMI commands, host-based command execution, file operations, and registry manipulation.
- PLC Denial of Service.
- Credential capture and brute forcing of PLCs.

### VICTIM

- Asset owners with Schneider Electric and Omron PLCs
- Other vendor CODESYS-based PLCs likely vulnerable to manipulation by the capabilities.

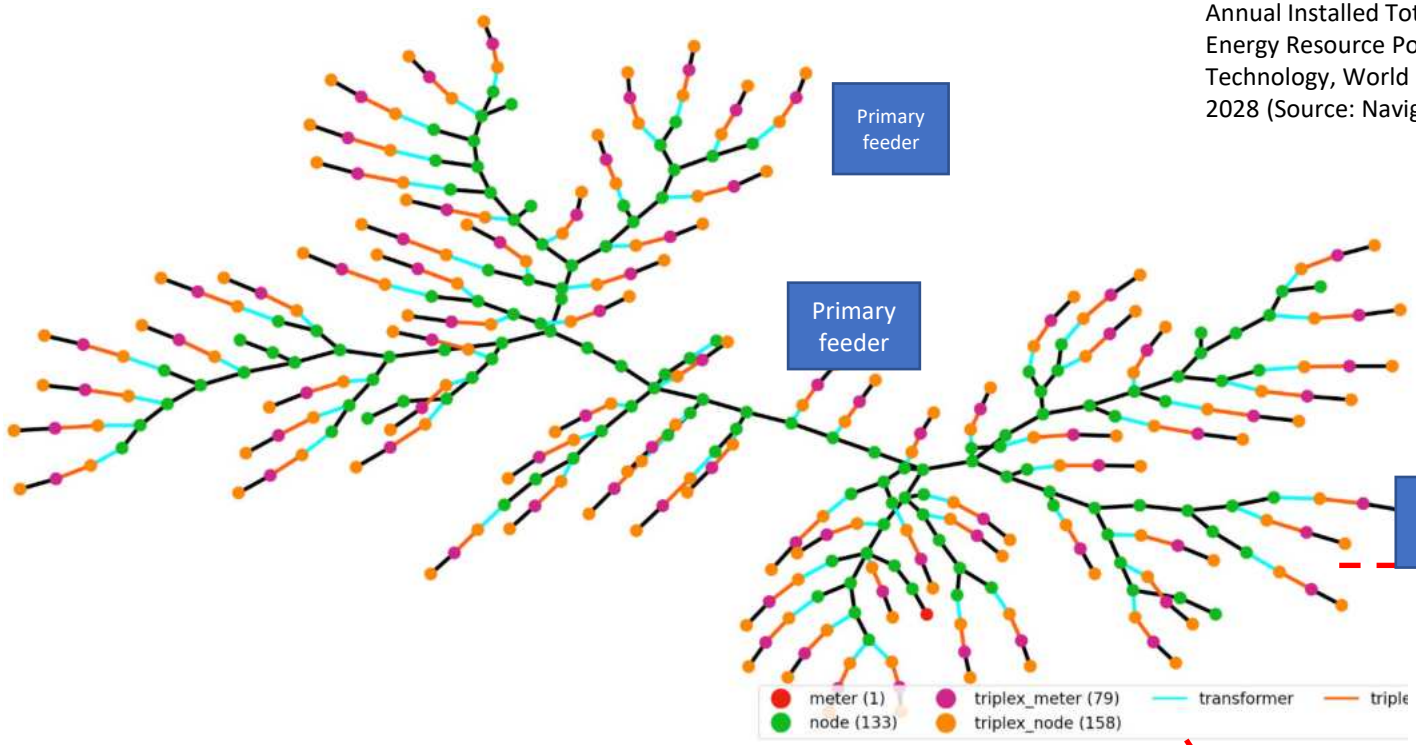
Impacted 225,000 customers

Capable of executing 38% of known attack techniques and 83% attack tactics cataloged by MITRE

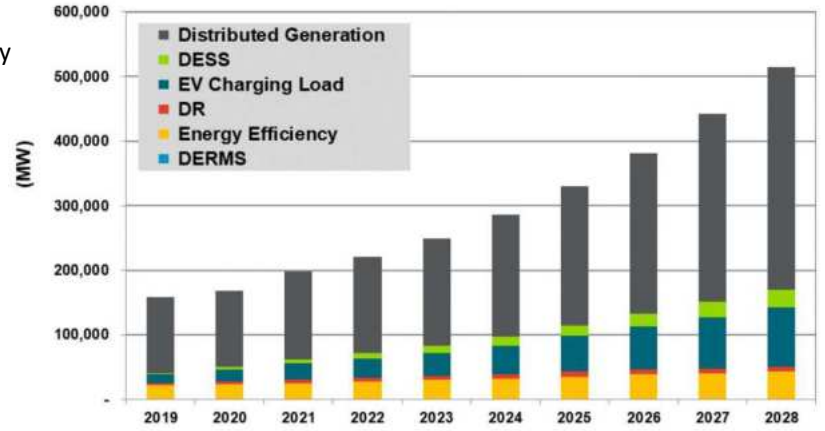
Source: Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

Sources: Dragos, Inc. "PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems." (2022); https://attack.mitre.org/

# Optimization challenging with billions of end-point control

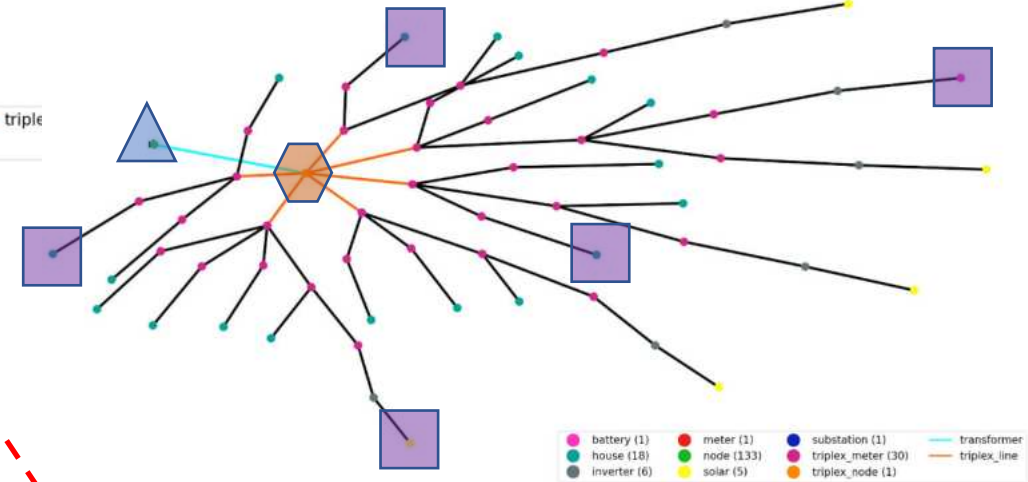



Annual Installed Total Distributed Energy Resource Power Capacity by Technology, World Markets: 2019-2028 (Source: Navigant Research)




Increasing DER penetration

Secondary feeder




Consumer feeder

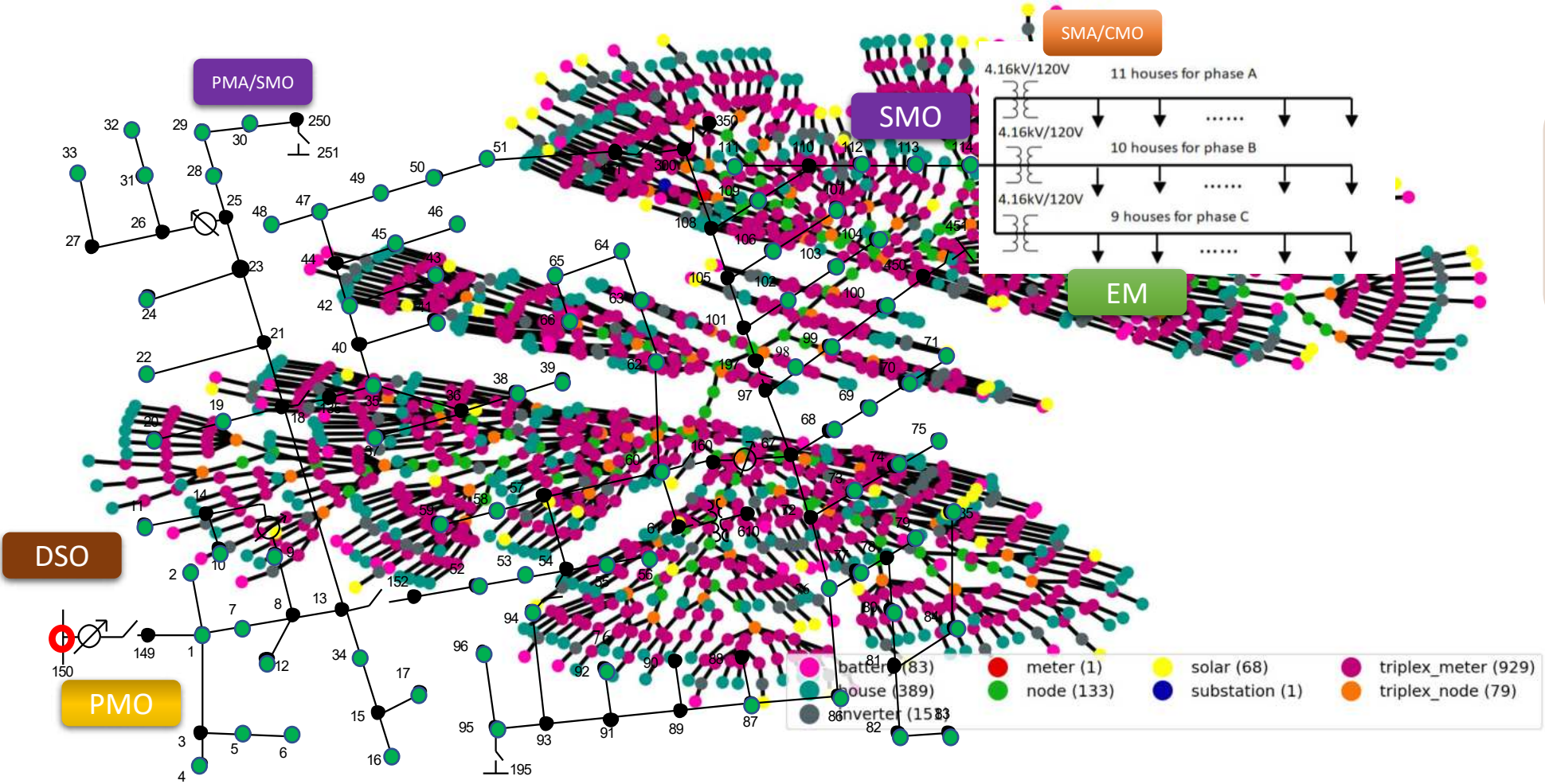
400 Secondary Feeders

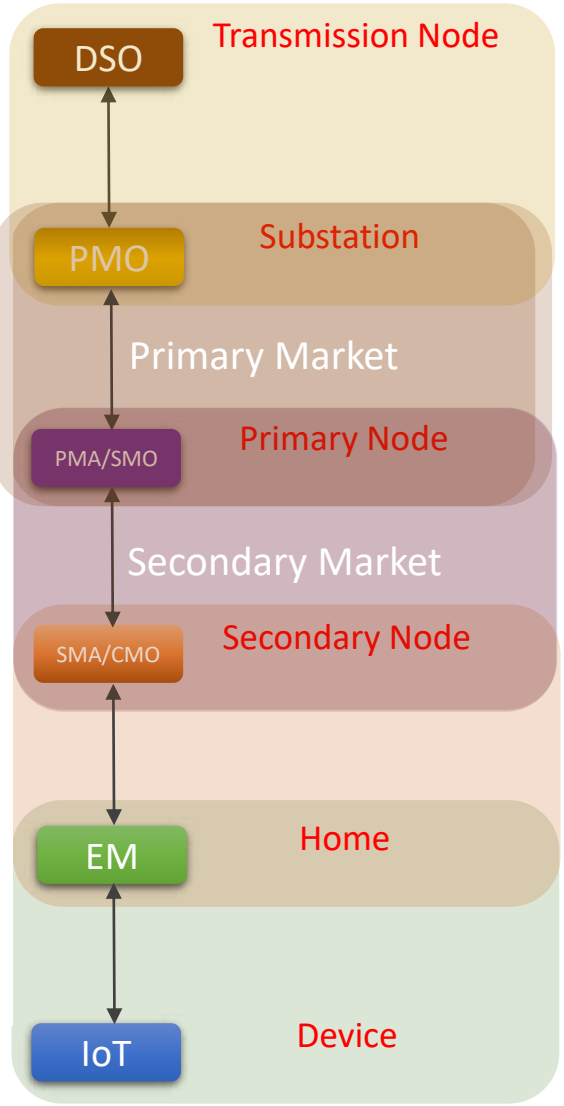
1000 IoT devices
100 PVs (531.5 KW)
200 batteries

Typical distribution grid with many distributed energy resources (DER) (modified IEEE-123 node feeder)

Source: PNNL Gridlab-D Modeling Team

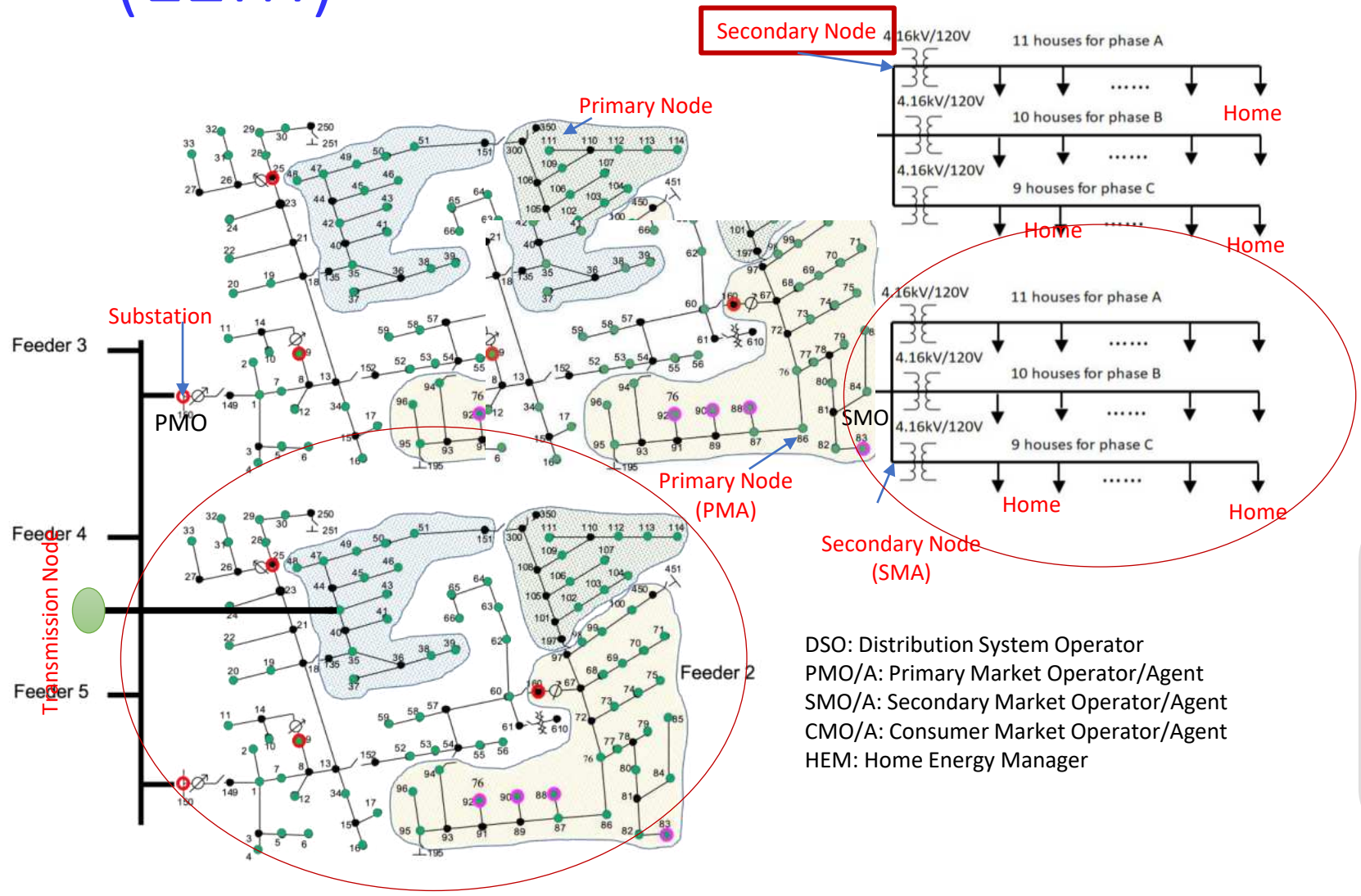
# We have a model*



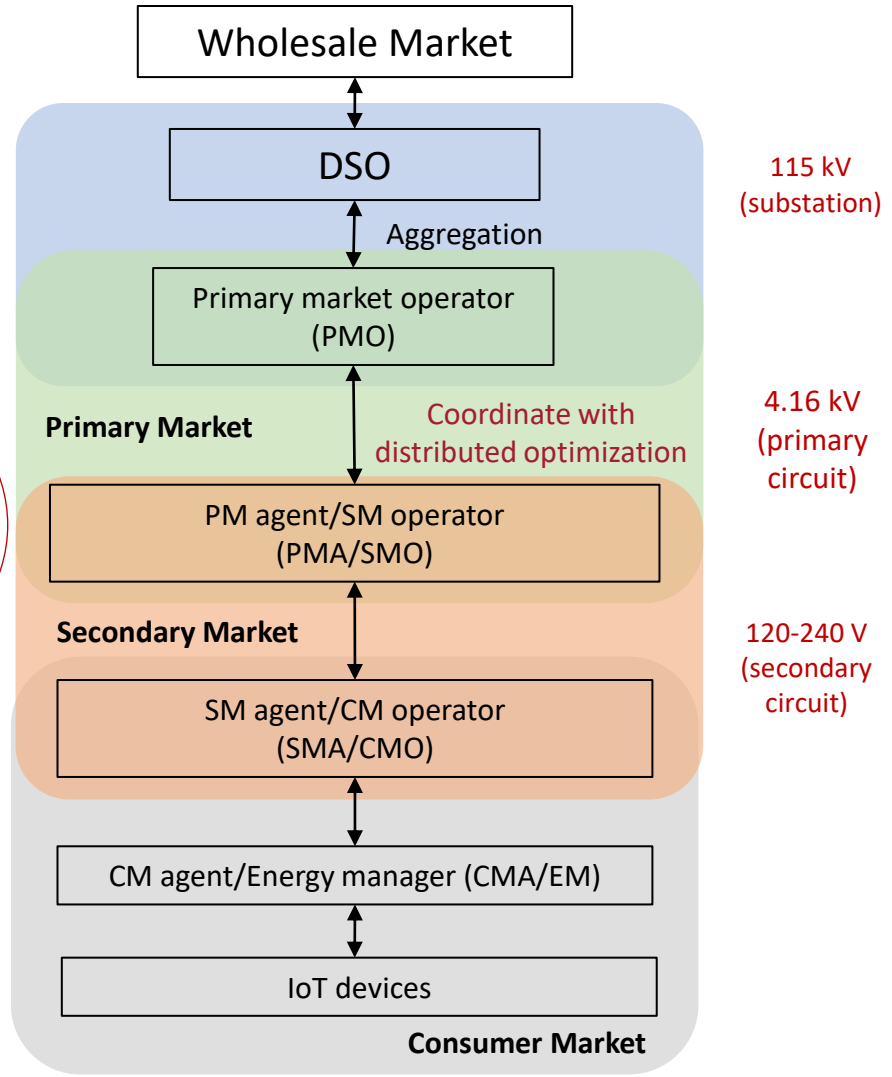




*100,000 nodes, Efficient UltRa Endpoint IoT-enabled Coordinated Architecture (EUREICA), DoE project

# Proposed hierarchical local electricity market (LEM)

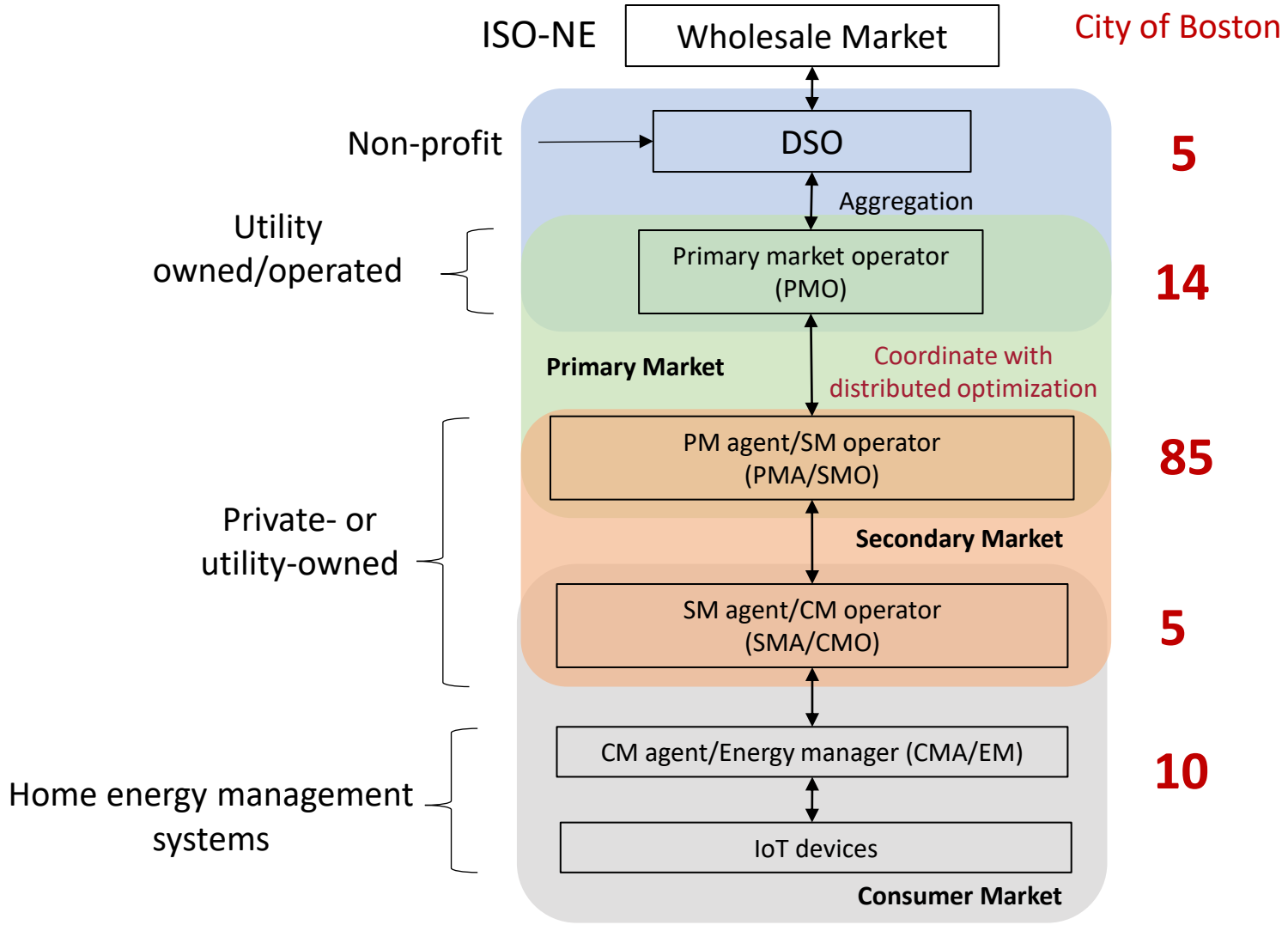



DSO: Distribution System Operator
PMO/A: Primary Market Operator/Agent
SMO/A: Secondary Market Operator/Agent
CMO/A: Consumer Market Operator/Agent
HEM: Home Energy Manager

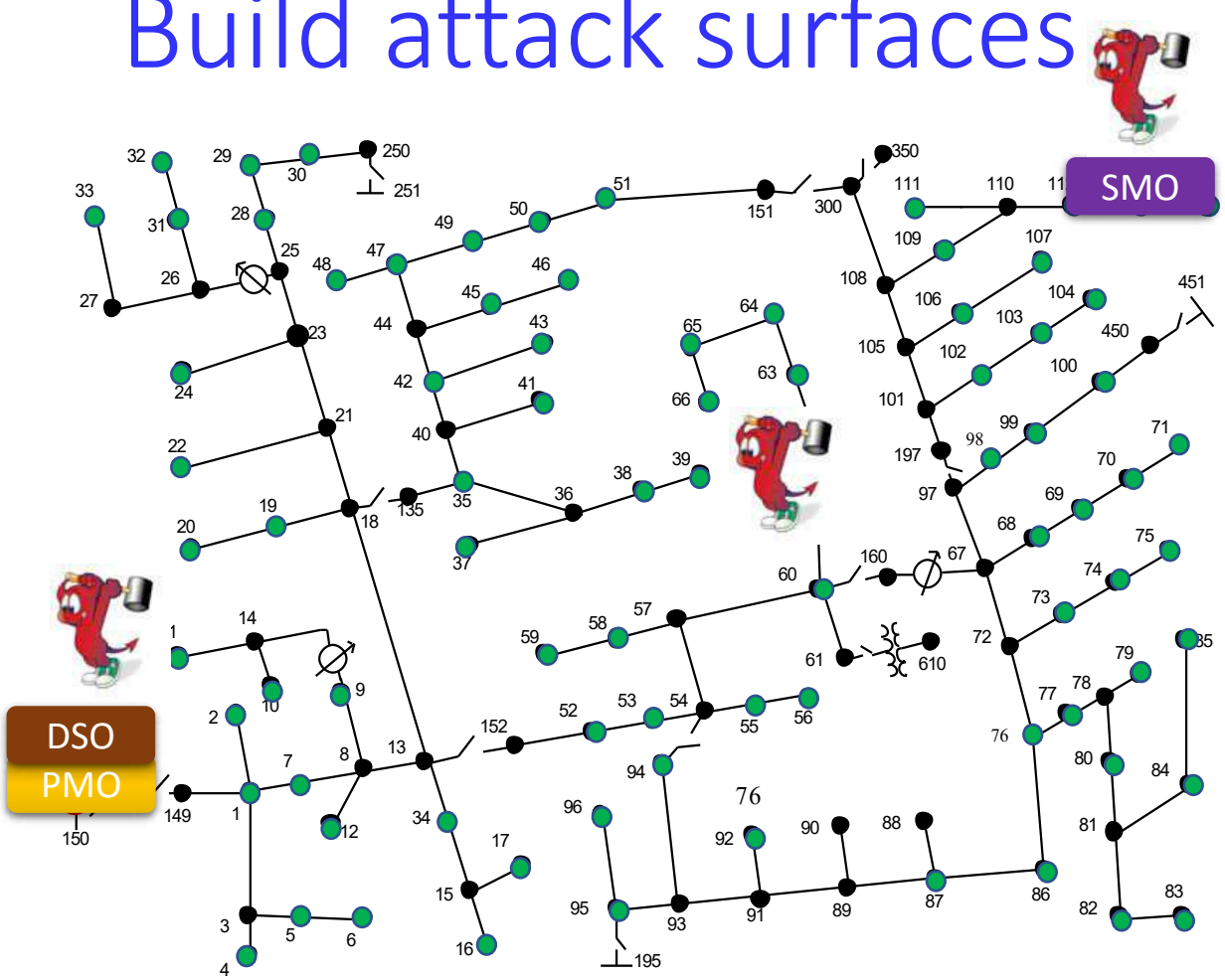


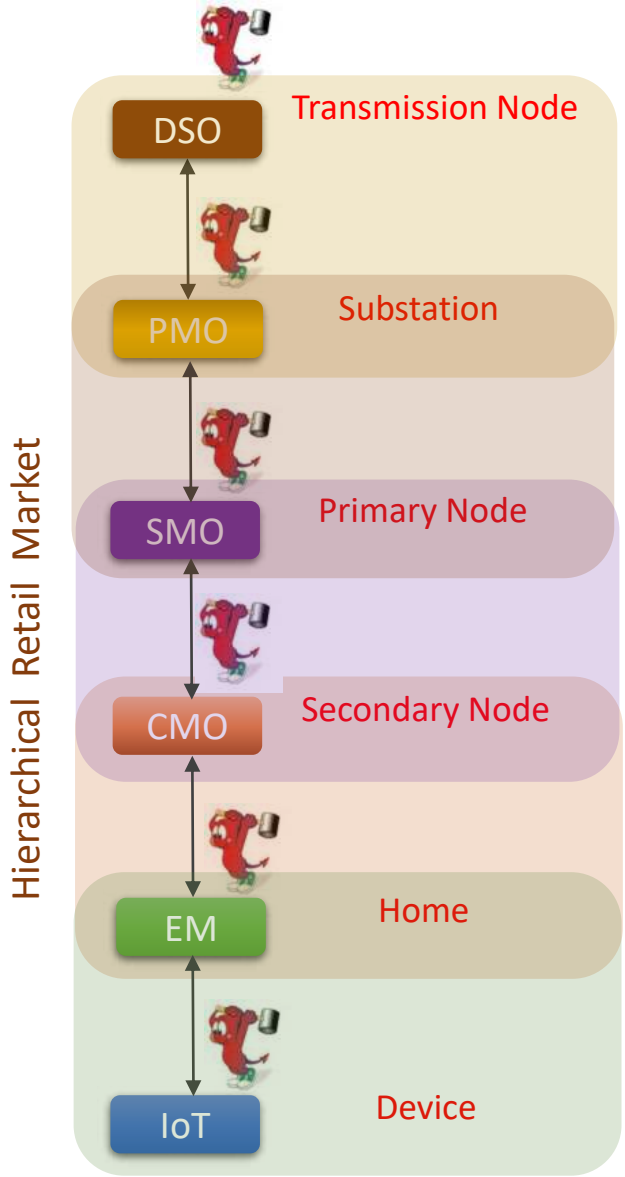
# Different players in the LEM

- DSO participates in WEM
- PMO – May be Utility-operated
- PMA - Large loads or generators can participate directly in PM; Examples:
  - DER aggregators
  - Large industrial loads
  - Microgrids
- SMO – DER aggregators
  - SMA: Smaller loads/DER owners
- Energy Managers
  - Coordinate IoT devices



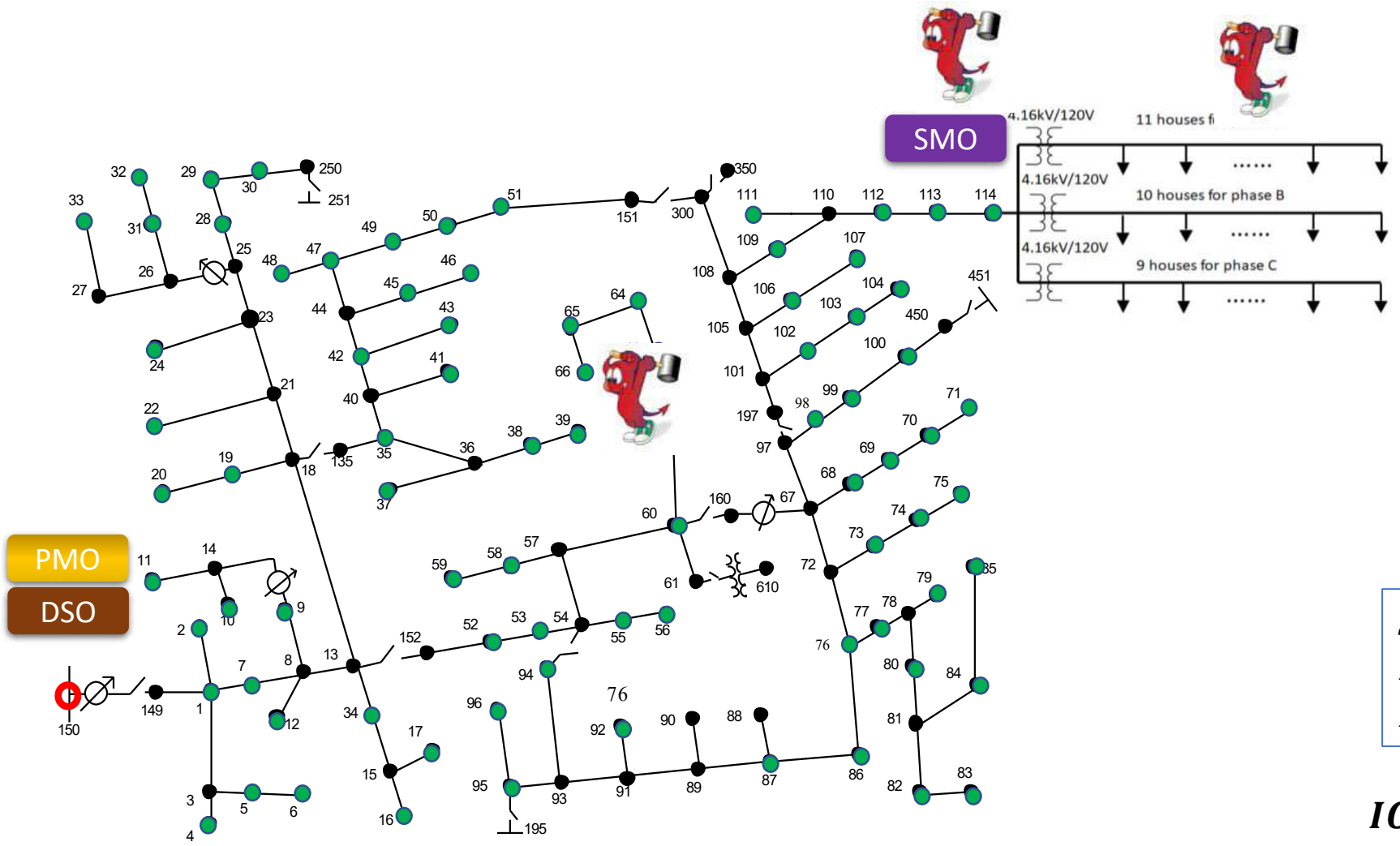
# Leverage the Market Structure: Build attack surfaces

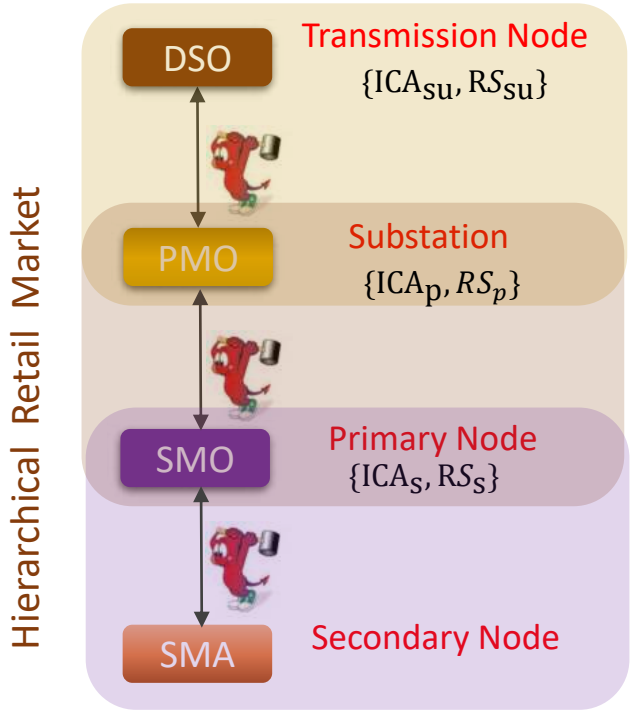



Emulate several large-scale attacks

# Second step: Develop Situational Awareness (SA)



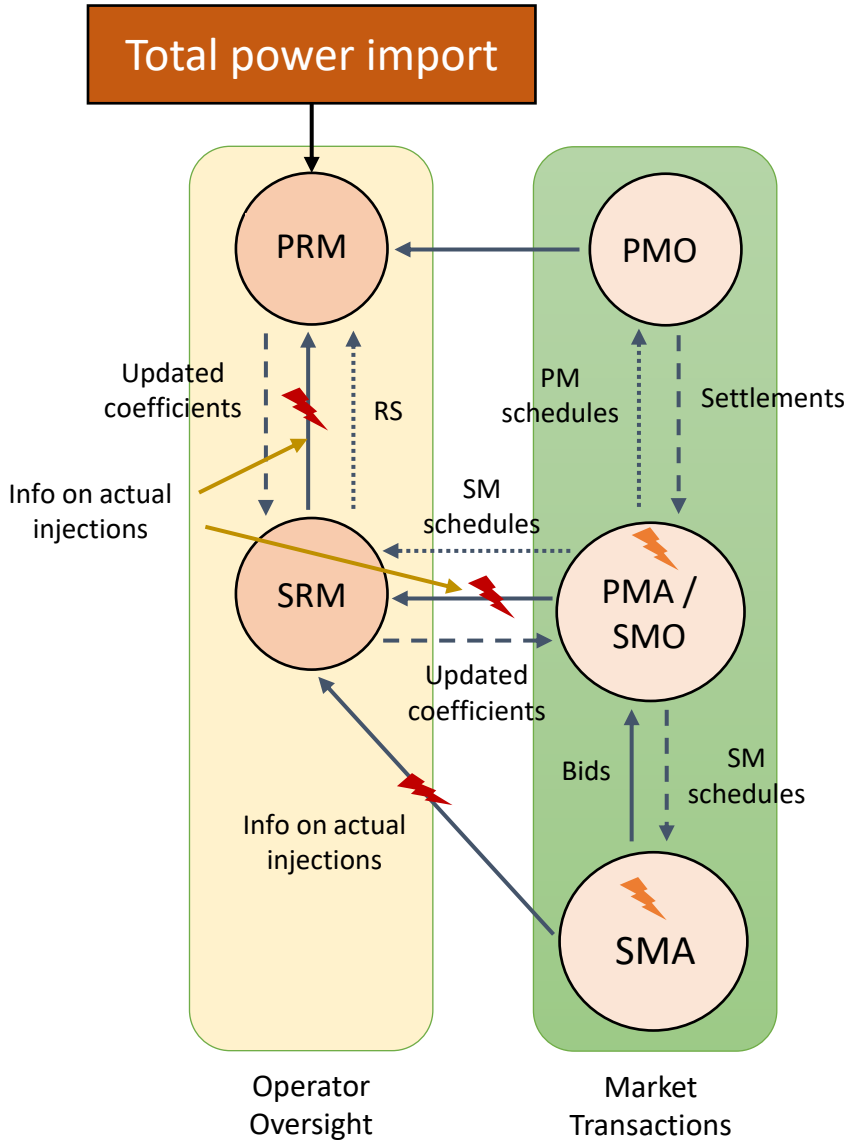




$SA_x = \{ICA_x, RS_x\}$ at node $x$
$ICA_x = \{P_x, Q_x\}$ at node $x$
$RS_x$ =Resilience Score of node $x$

$ICA_x$: IoT-Coordinated Assets

# Overview of attack scenario

- RM = Resilience manager
  → Monitors grid & provides SA
  → Manages attack mitigation
- MO = Market operator
  → Handles market bidding, clearing, settlement
- Setpoints are corrupted at nodes ( )
  - DG: Distributed generation attack
    e.g. PV/batteries shut down
  - LA: Load alteration attack
- Simultaneously, key communication links are disrupted ( )
- No visibility: PRM doesn't know which nodes have been attacked
- Goal is to provide local resilience
  - Minimize power import from bulk grid




RS: Resilience Scores

# Attack detection & mitigation

- PRM monitors power injection at substation (PCC)
  - Detects attack if injection deviates significantly from forecasted value i.e. $\left|\mathbf{P}_{cc} - \overline{\mathbf{P}}_{cc}\right| > \epsilon$
- PRM doesn't have direct control over SMOs → Use distributed coordination
- PRM modifies objective function coefficients for all SMOs

$$\text{Cost function: } \sum_{i=1}^{n}\left(\frac{1}{2}\alpha_i P_i^{G^2} + \beta_i\left(P_i^L - P_i^{L0}\right)^2\right) + \xi \cdot \text{ losses} \qquad (1)$$

$$\Delta = \mathbf{P}_{cc} - \overline{\mathbf{P}}_{cc} \qquad (2)$$

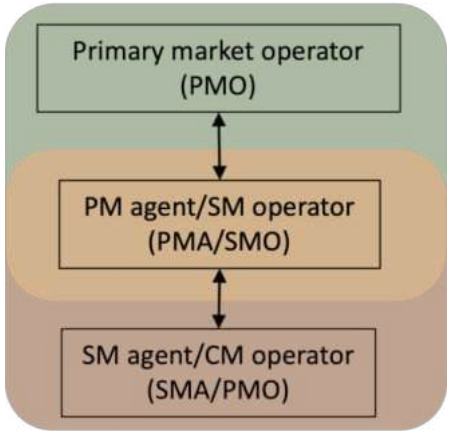
$$Z_i\left(\delta_i\right) = 1 + \frac{RS_i\Delta^\top\delta_i}{\mu\sum_i RS_i} \Longrightarrow \gamma_{i\delta} = \frac{1}{Z_i\left(\delta_i\right)} \qquad (3)$$

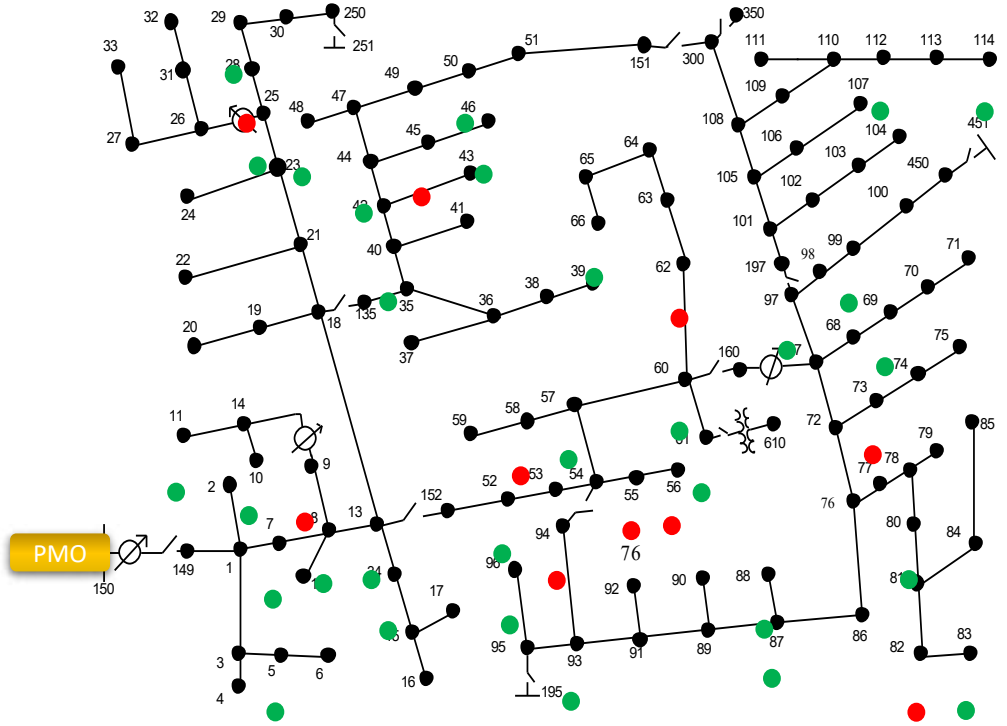
$$\overline{\boldsymbol{\alpha}}_i = \gamma_{i\alpha}\boldsymbol{\alpha}_i, \quad \overline{\boldsymbol{\beta}}_i = \gamma_{i\beta}\boldsymbol{\beta}_i, \quad \overline{\boldsymbol{\xi}} = \left(\frac{\sum_i \gamma_{i\alpha} + \gamma_{i\beta}}{2n}\right)^{-1}\boldsymbol{\xi} \qquad (4)$$

- Optimally redispatch resources at primary/secondary level ($ICA_s, ICA_p$) with new reweighted objective → Update $\{\alpha_i, \beta_i, \xi\}$ as $\{\overline{\boldsymbol{\alpha}}_{\boldsymbol{i}}, \overline{\boldsymbol{\beta}}_{\boldsymbol{i}}, \overline{\boldsymbol{\xi}}\}$

# Types of attack surfaces*

| Attack | Type | Attack surface | Model |
|---|---|---|---|
| 1 | 45 kW loss of DG | PMA | GridLAB-D |
| 2 | 681kW loss of DG | PMA, SMA | IEEE 123 |
| 3 | Islanded | PMA | IEEE 123 |

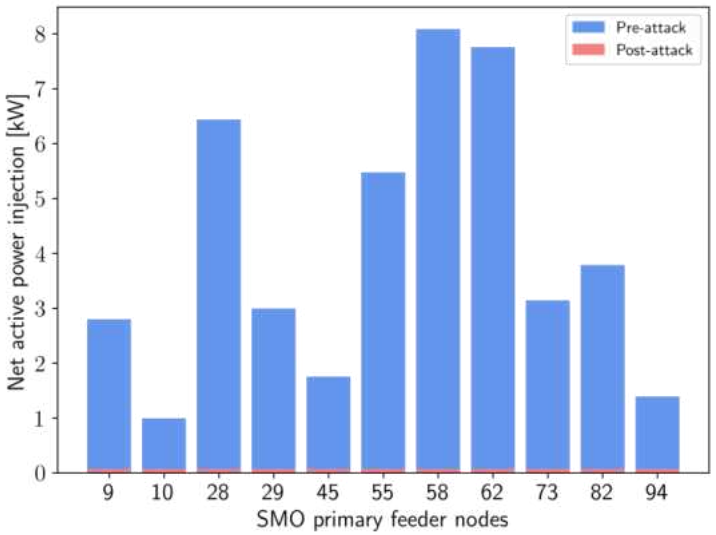


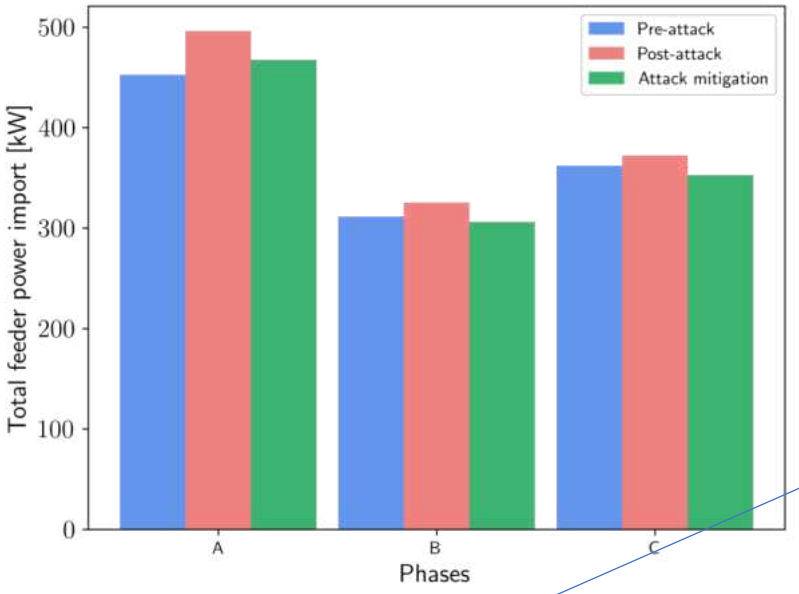



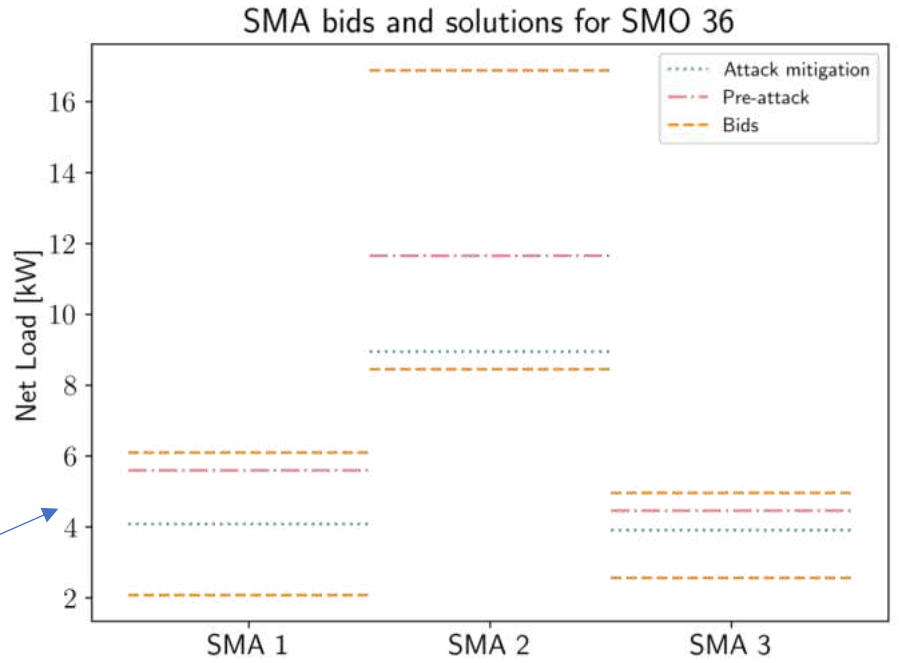

: Attacked Nodes : Trustable EUREICA-Nodes

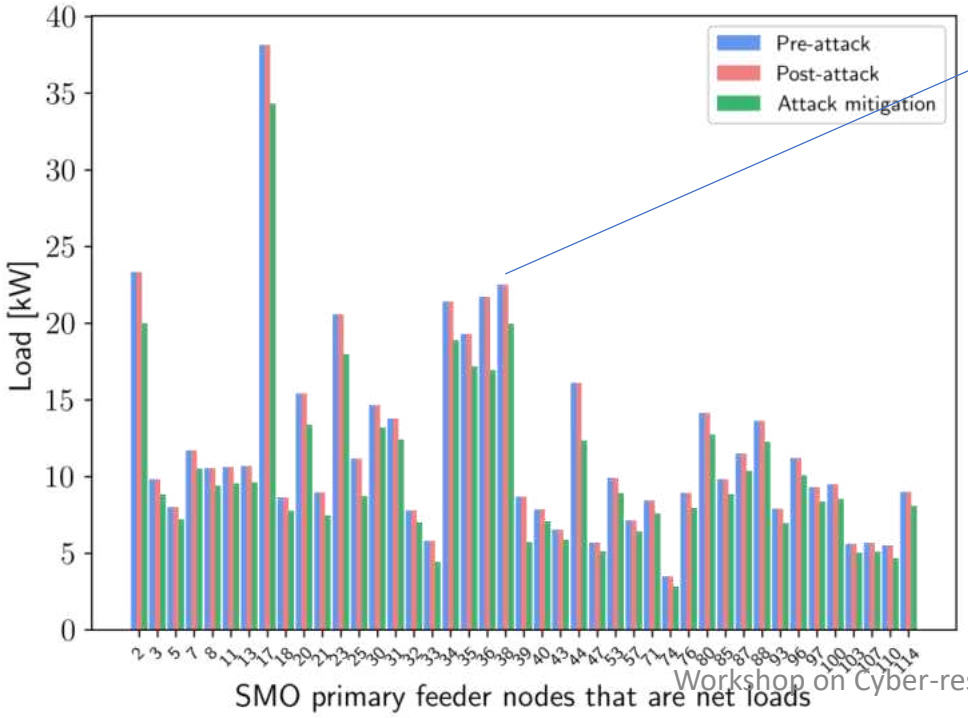
EUREICA: Efficient, Ultra-Resilient IoT-coordinated Assets

* https://arxiv.org/abs/2406.14861




| Metric | Value [kW] |
|---|---|
| Total load without attack | 1167.52 |
| Total load with attack | 1190.44 |
| Total load after attack mitigation | 1123.31 |
| Minimum SMO load curtailment | 0.12 |
| Maximum SMO load curtailment | 4.77 |
| Total import w/o attack | 1125.91 |
| Total import w/ attack | 1193.87 |
| Total import w/ attack mitigation | 1126.35 |

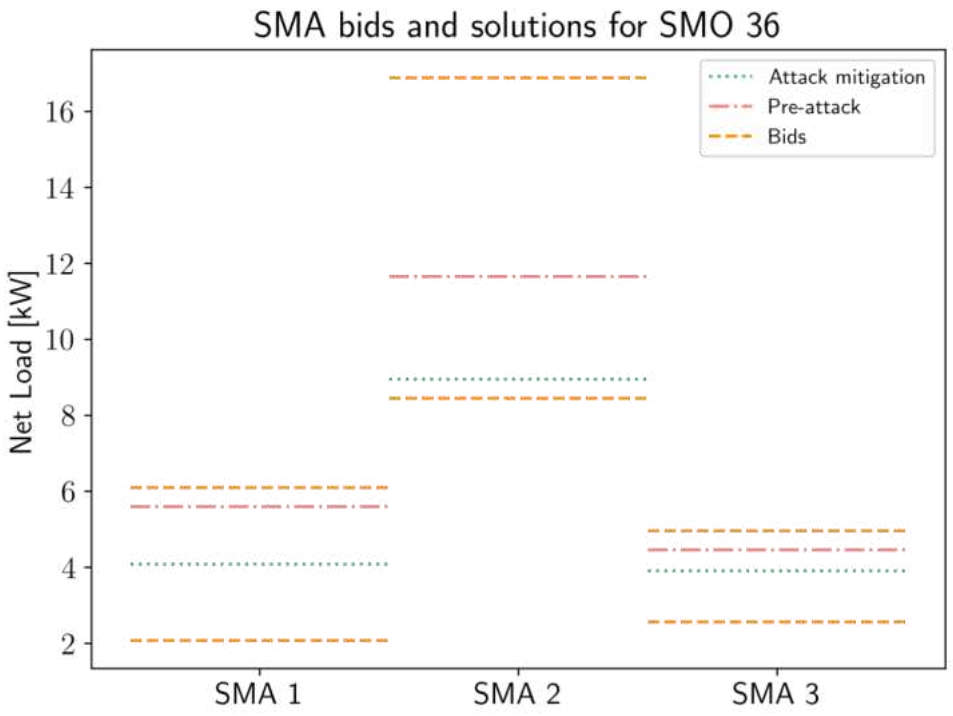


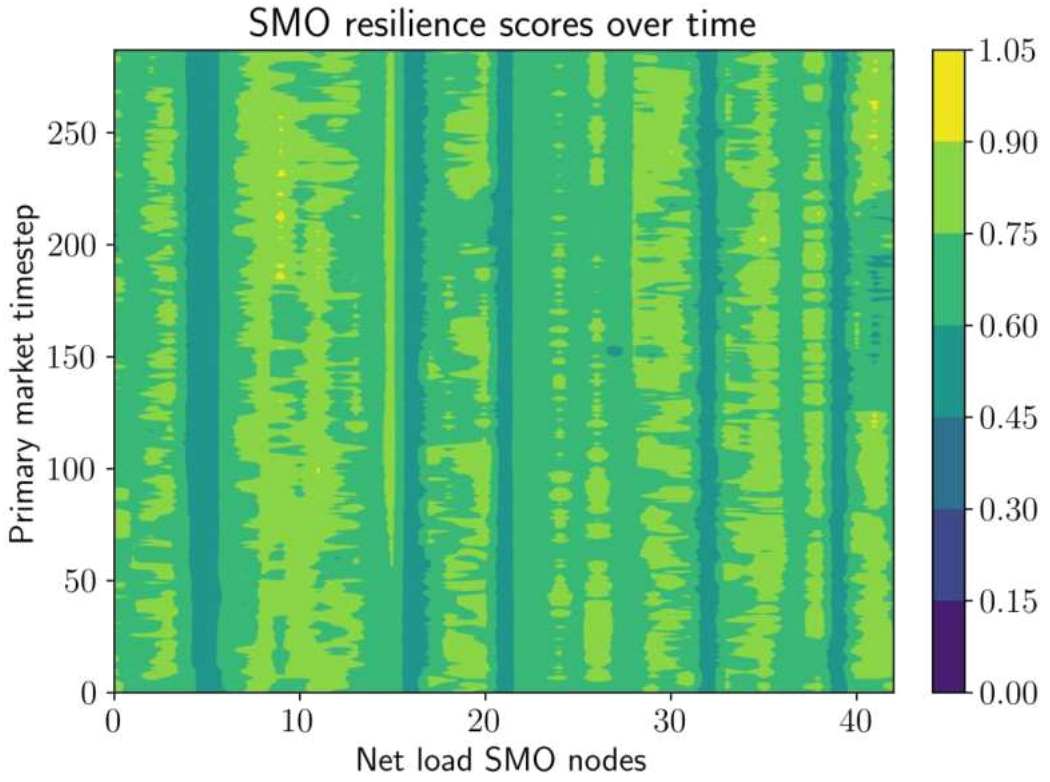
* https://arxiv.org/abs/2406.14861

# SMA disaggregation and RS

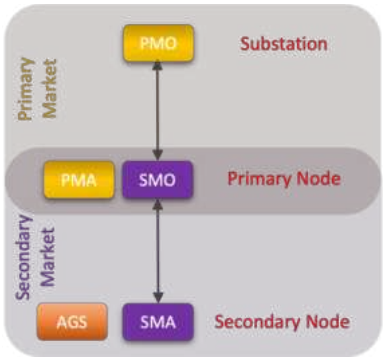
- Distribute flexibility (curtailment) among SMAs based on their individual RS
- Generally allocate more flexibility to SMAs with higher RS

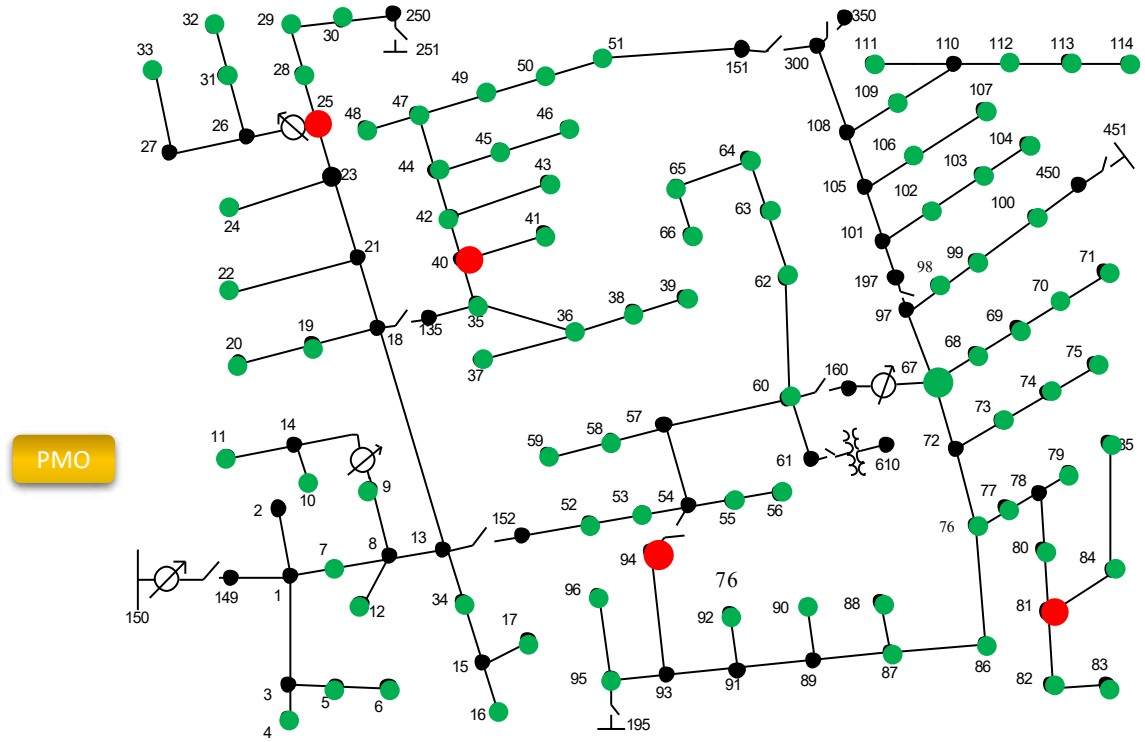
| SMA | RS |
|---|---|
| SMA 1 | 0.947 |
| SMA 2 | 0.985 |
| SMA 3 | 0.493 |



# Attack 2: Large scale attack with mitigation



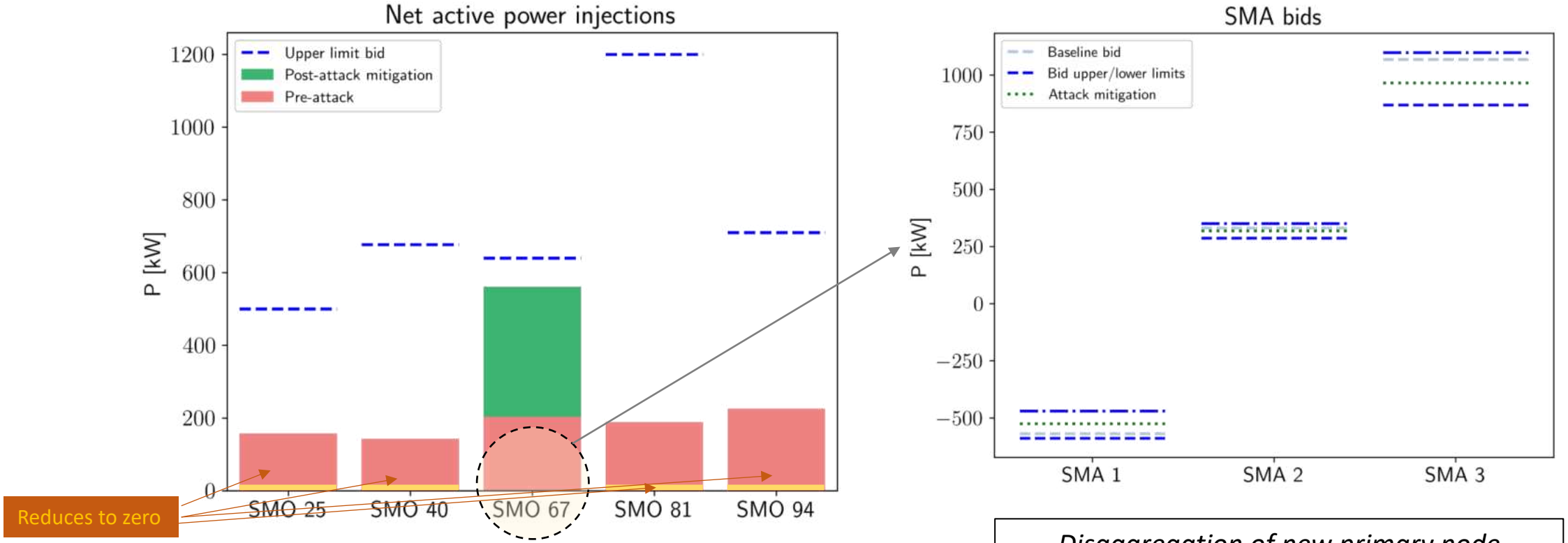

1. A total of 641 kw generation loss
2. PRM alerts other trustable PMAs/SMOs to redispatch their generation assets
3. Trustable PMAs/SMOs will curtail flexible loads to respond & mitigate attack
4. SMOs redispatch SMAs who provide correct setpoints
5. Total import from the main grid stays at the same level

82 flexible load nodes respond

: Attacked Nodes

: Trustable EUREICA-Nodes

# Large scale attack 2: Mitigation

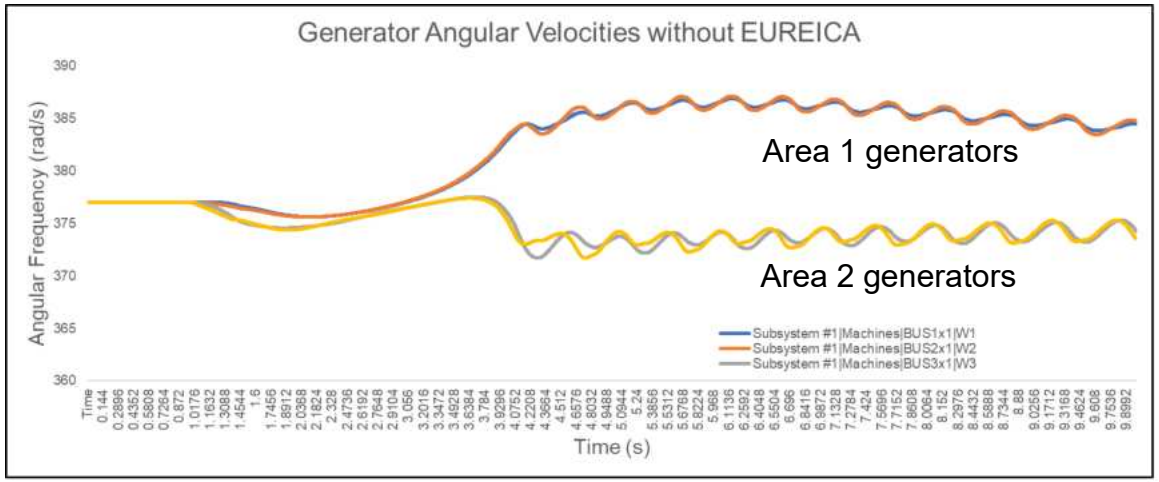


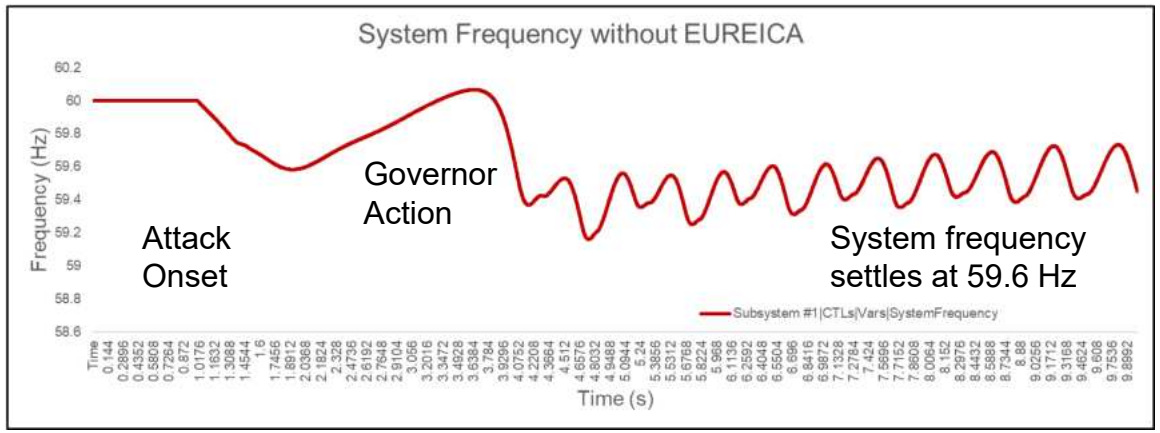

*Changes in dispatch at key primary nodes*

*Disaggregation of new primary node setpoints across secondary feeders*

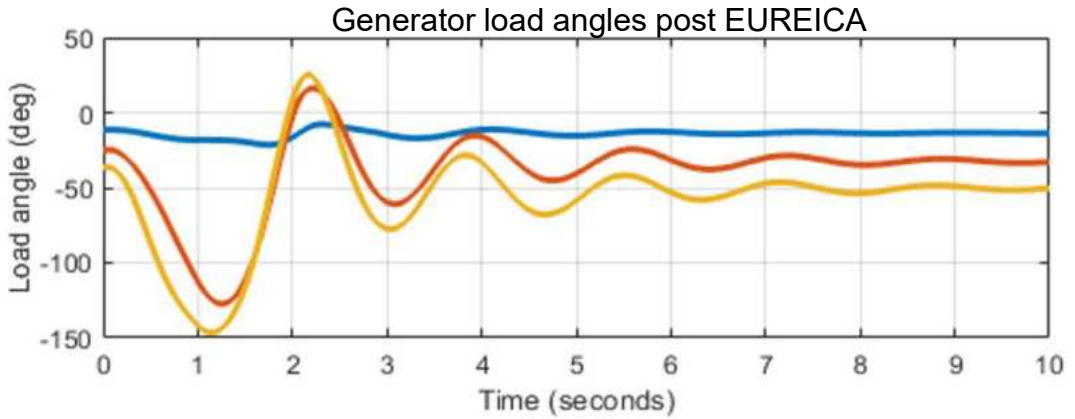
- 4 generators attacked: At nodes 25, 40, 81, 94
  - Physical outage → **All drop to zero (650kw generation loss)**
  - Cyber attack → **Communication with Market Operator compromised**
- Leverage available upward flexibility of remaining generator at SMO 67
- Increase in generator output does not violate capacity limits imposed by power flow/network constraints

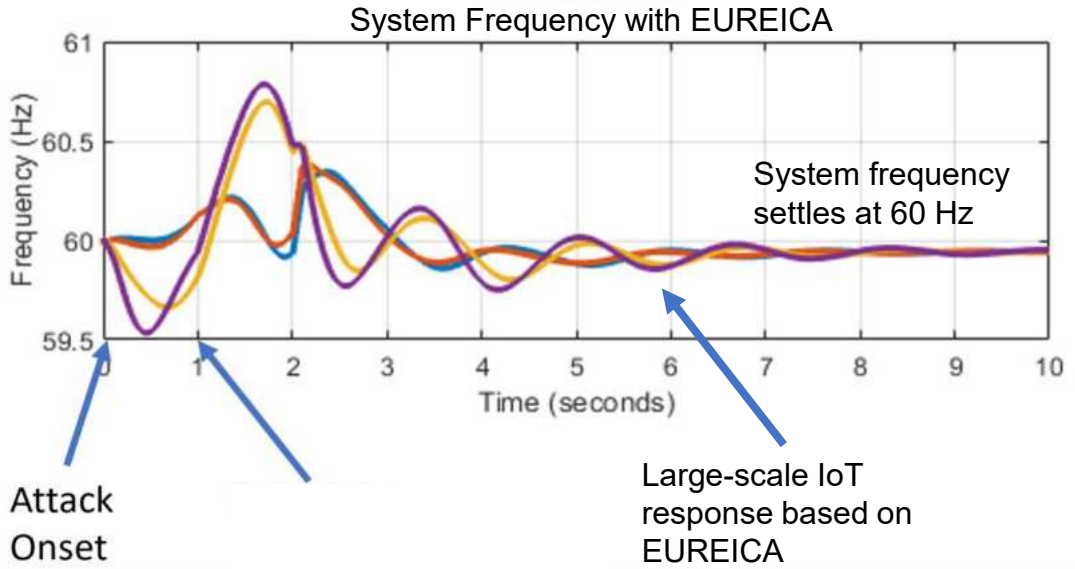
# Attack 2 – Validation at the Transmission Level



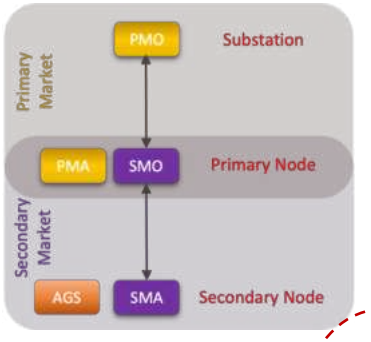

RESPONSE WITHOUT EUREICA

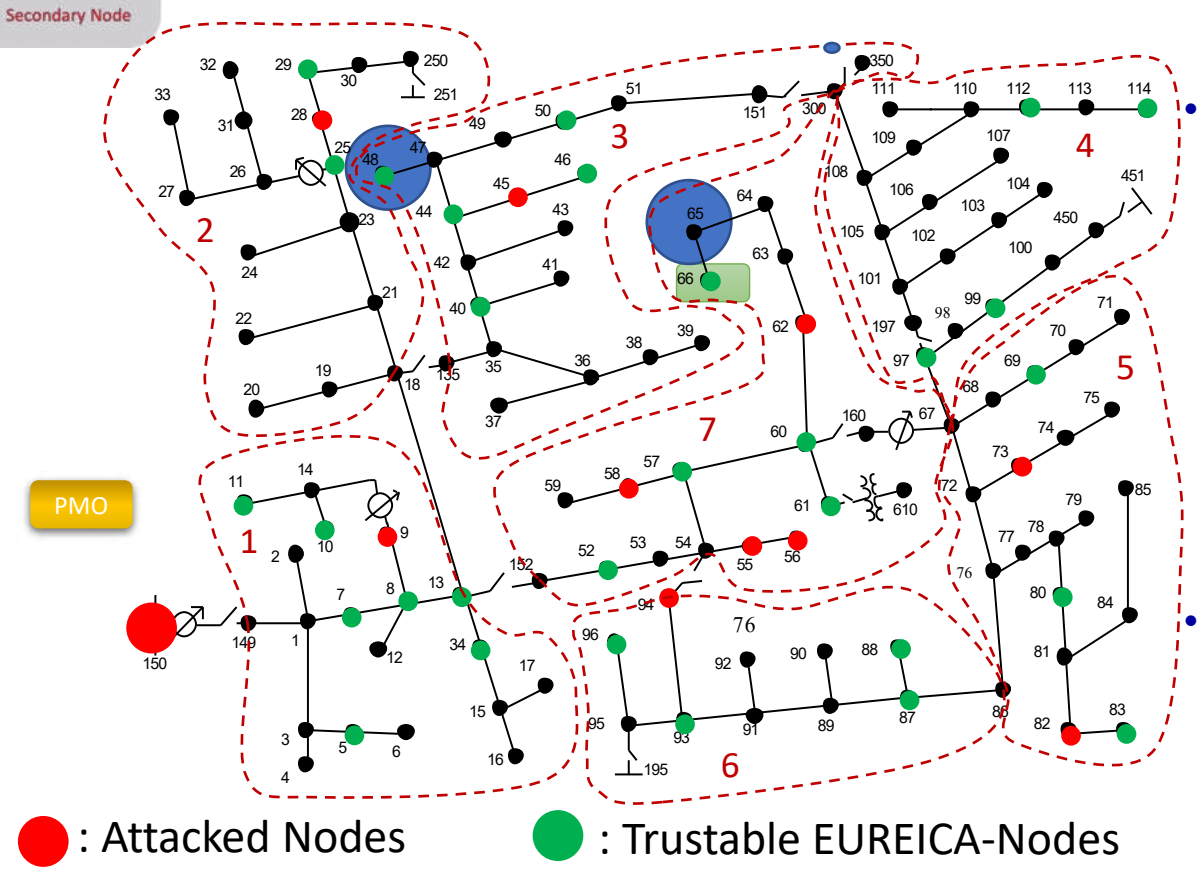



RESPONSE WITH EUREICA

# Overall timeline of Attack 3.0




● : Attacked Nodes ● : Trustable EUREICA-Nodes

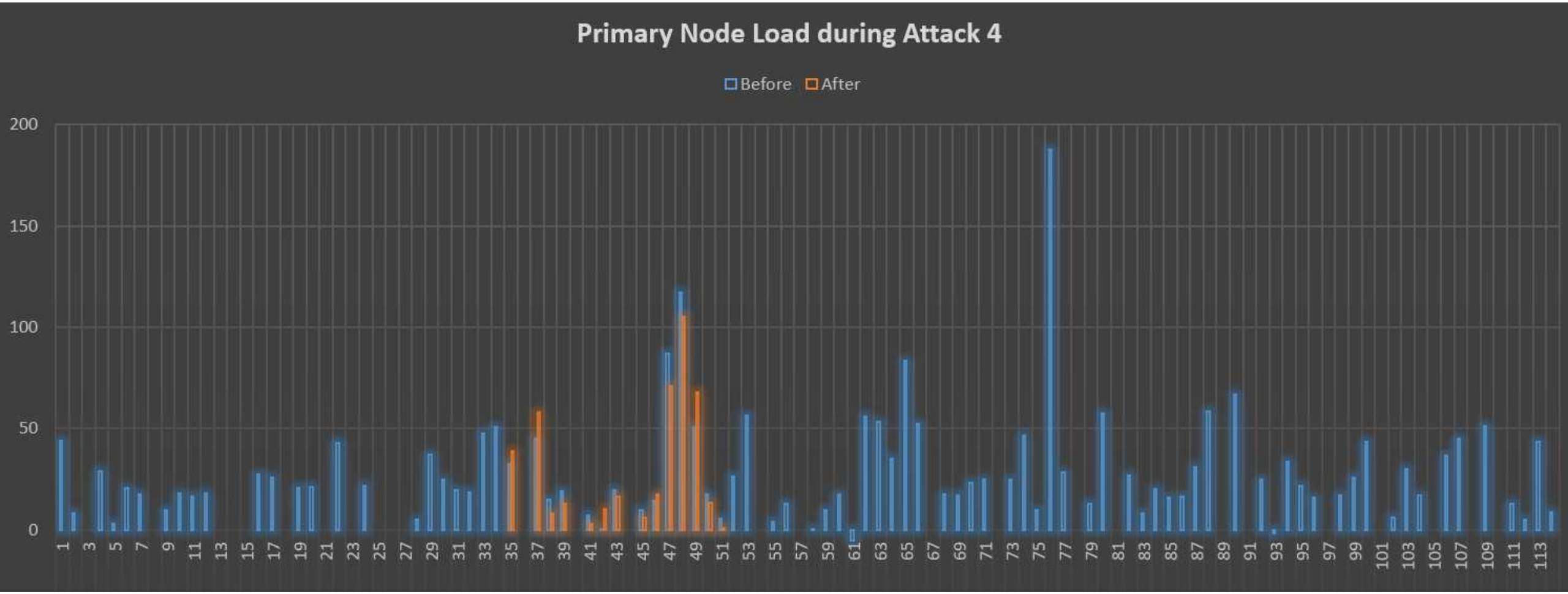
- Fault occurs at Node 150
- SW 150 to 149 is disconnected
- DG at node 48 is connected through reconfiguration

- With no Situational Awareness: Distribution system is disconnected, loads are shed

- With Our Approach:
  - Situational awareness is increased – ability to shed load intelligently
  - DERs added at 48 (270 kW) and 65 (15 kW)
  - Appropriate reconfiguration follows, and all critical loads across the entire feeder (30% of all loads) are picked up
  - Alternatively, the critical loads could be situated in the same zone – here, all loads in Zone 3 are picked up

- With additional microgrid:
  - Military microgrid at node 66 (1.7 MW)
  - Situational awareness helps trustable DR reduce consumption by 20%
  - 80% all loads picked up

# Attack 3 ADMS Verification – Microgrid




1. Shows the primary node load change comparison between 12:59 and 13:00
2. DG 48 pickup all expected load in region 3 with 430 kW generation

# Resilience at the Grid-Edge Using Trustable DERS

Deep decarbonization in a power grid introduces several communication windows of vulnerabilities & opportunities

***Approach***

- Development of attack surfaces that can induce a range of threat levels in a distribution grid
- A resilience-based approach that determines Situational Awareness (SA) as well as Resilience Scores (RS) of all assets to operators who are strategically located

***Results***

- Two large-scale attacks were emulated on an IEEE 123-Feeder
- Attack impact was mitigated using SA and RS

***Key Take-aways***

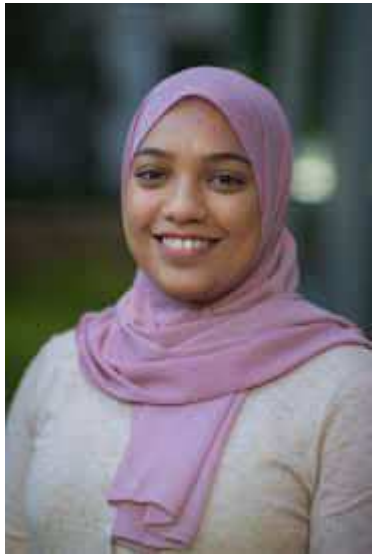
1. Distributed IoT-coordinated Assets can be ascertained
2. They provide opportunities for enhancing resilience
3. Local resilience through trustable DERs

# The Team

Venkatesh Venkataramanan

Vineet Nair

Priyank Srivastava



Rabat Haider

Past students: David Dachiardi, Tom Nudell, Sandra Jenkins, Stefanos Baros, Milos Cvetkovic

# Sponsors

- US Department of Energy, “Efficient Ultra-Resilient IoT-coordinated Assets (EUREICA)”
- US Department of Energy, “USA-India Collaborative for Smart Distribution System with Storage”
- MIT Energy Initiative, “Maximizing Security and Resilience to Cyber-attacks in a Power Grid”
- US National Science Foundation, Resilient Interdependent Processes and Systems

# Collaborators

- Washington State University: Anurag Srivastava
- National Renewable Energy Laboratory: Venkatesh Venkataramanan
- Pacific Northwest National Laboratory: Laurentiu Marinovici, Karan Kalsi
- Princeton: Vince Poor, Prateek Mittal

# Thank you!


# Questions?