Resilience and Distributed Decision-making in a Renewable-rich Power Grid

Anuradha Annaswamy

Active-adaptive Control Laboratory
Department of Mechanical Engineering

Massachusetts Institute of Technology

* Sponsors: US Department of Energy, MIT Energy Initiative

Power Grid: 20th Century

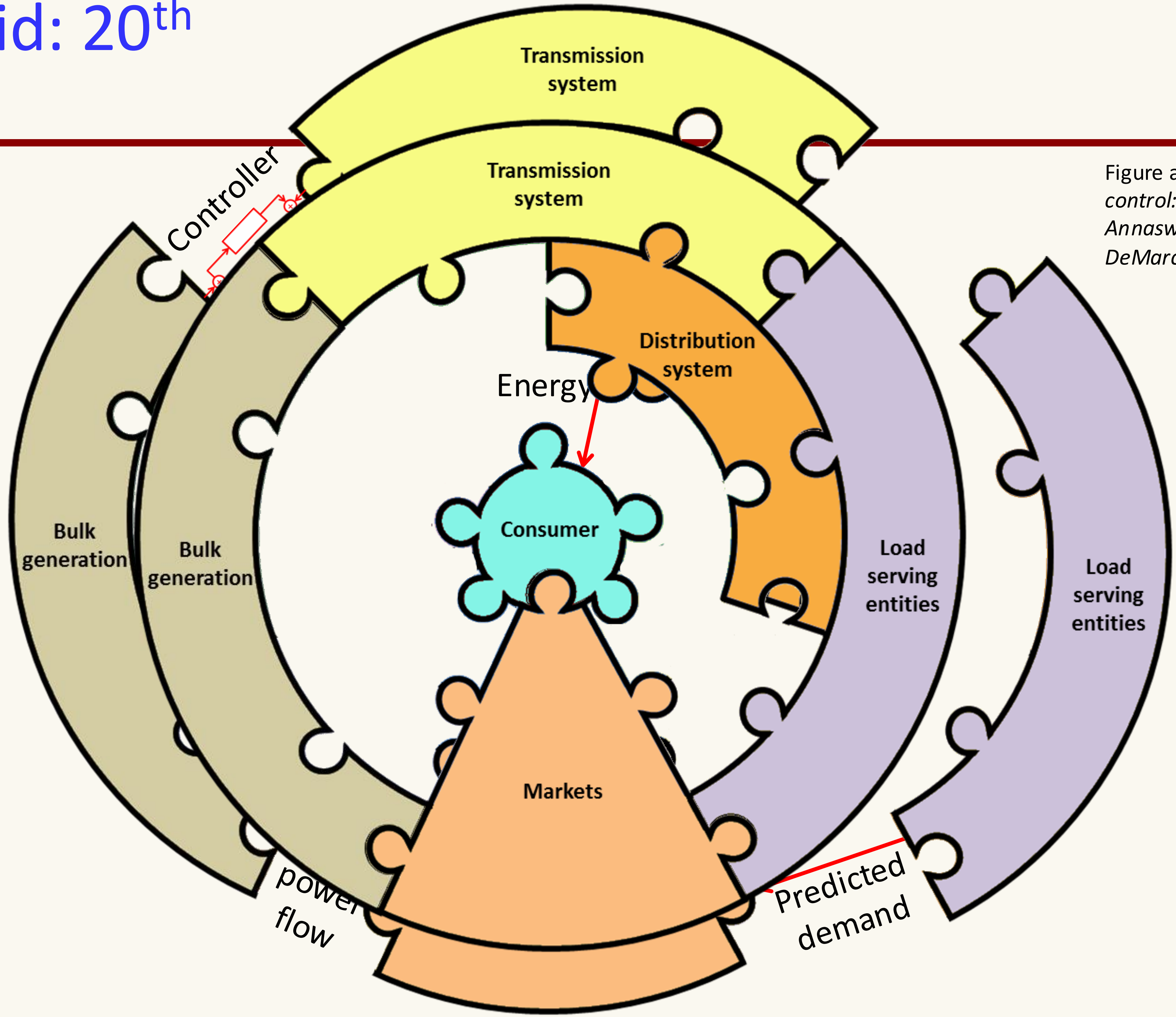
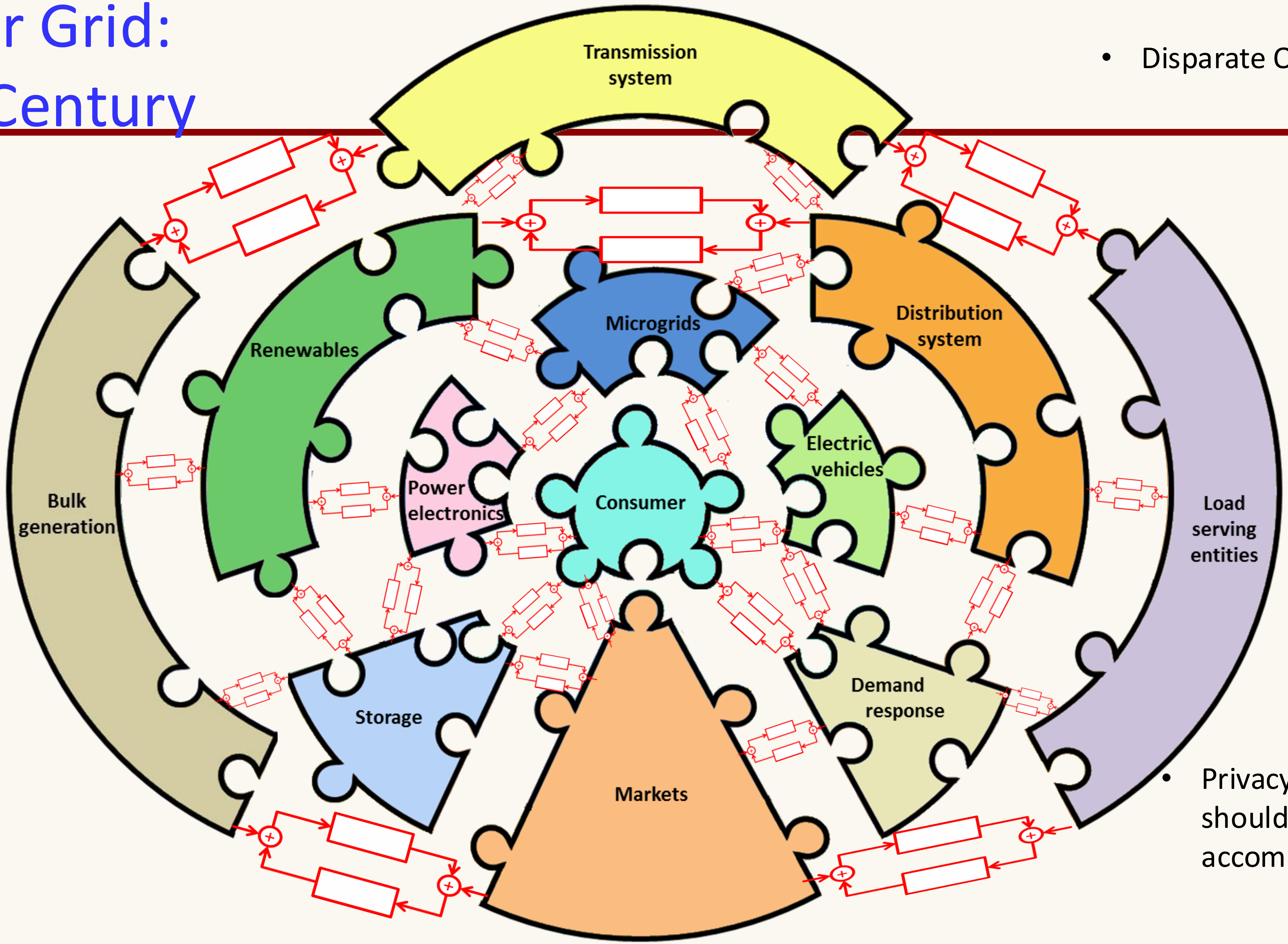


Figure adapted from *Vision for smart grid control: 2030 and beyond. Eds: A.M. Annaswamy, M. Amin, T. Samad, and C. DeMarco*. IEEE Standards Publication, 2013.

Power Grid: 21st Century

- Disparate Ownership

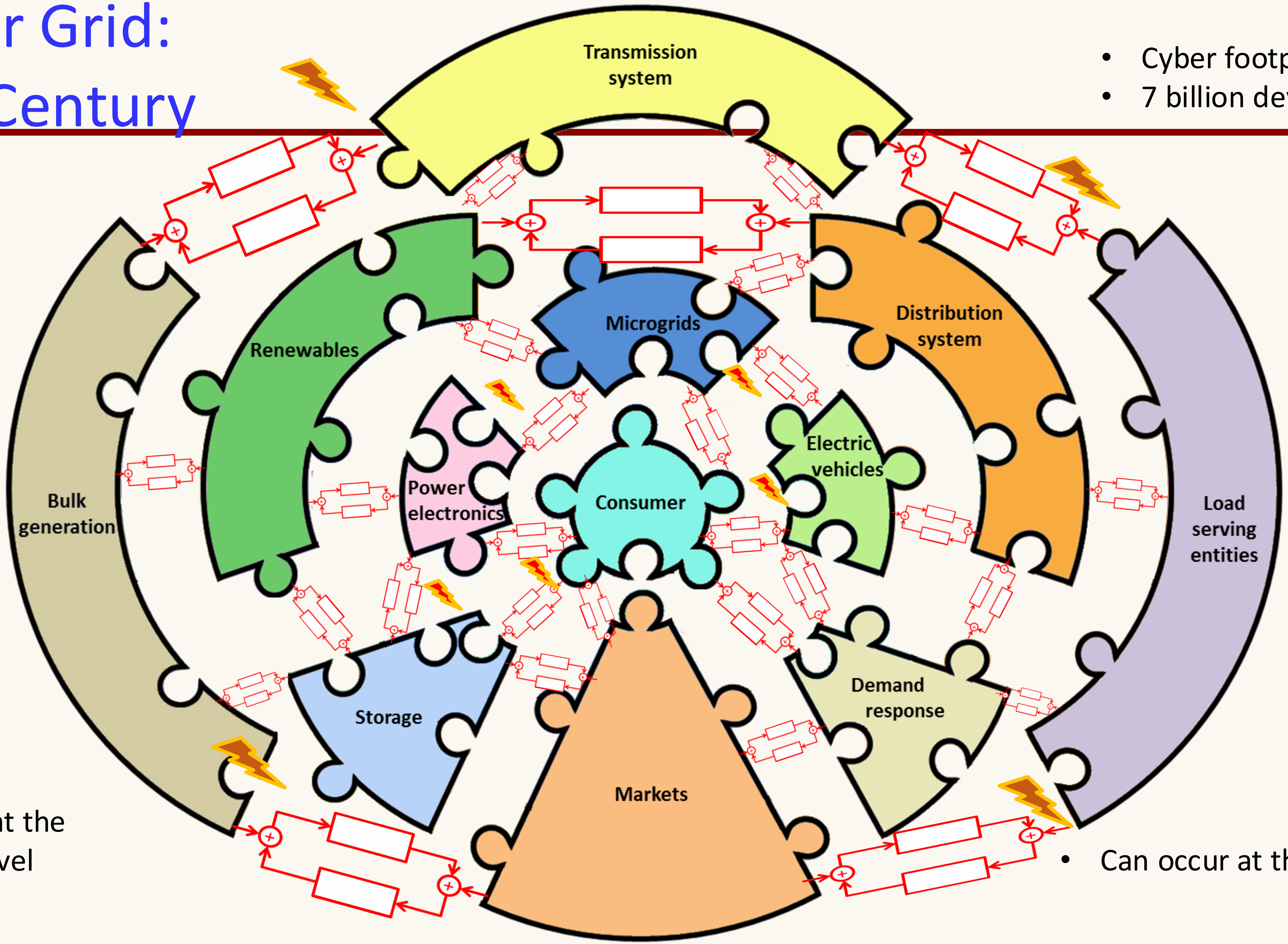


- Privacy boundaries should be accommodated

Figure adapted from *Vision for smart grid control: 2030 and beyond. Eds: A.M. Annaswamy, M. Amin, T. Samad, and C. DeMarco*. IEEE Standards Publication, 2013.

Power Grid: 21st Century

- Cyber footprint increases
- 7 billion devices



- Can occur at the planning level
- Can occur at the device level

Figure adapted from *Vision for smart grid control: 2030 and beyond. Eds: A.M. Annaswamy, M. Amin, T. Samad, and C. DeMarco*. IEEE Standards Publication, 2013.

There is a problem

Ukraine Power Grid Attack (2015)

Impacted 225,000 customers

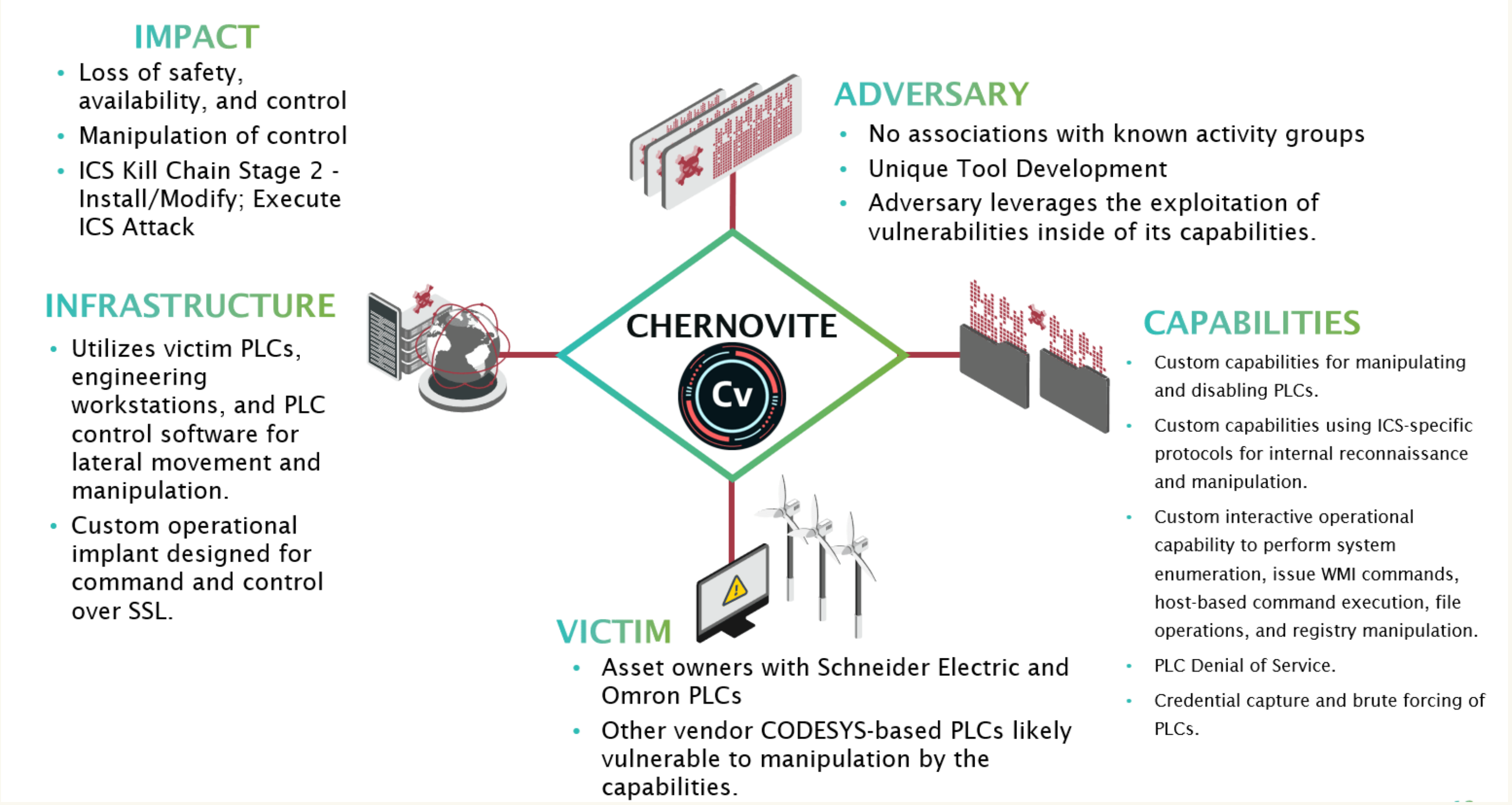
Source: Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

There is a problem

Ukraine Power Grid Attack (2015)

Impacted 225,000 customers

CHERNOVITE'S PIPEDREAM

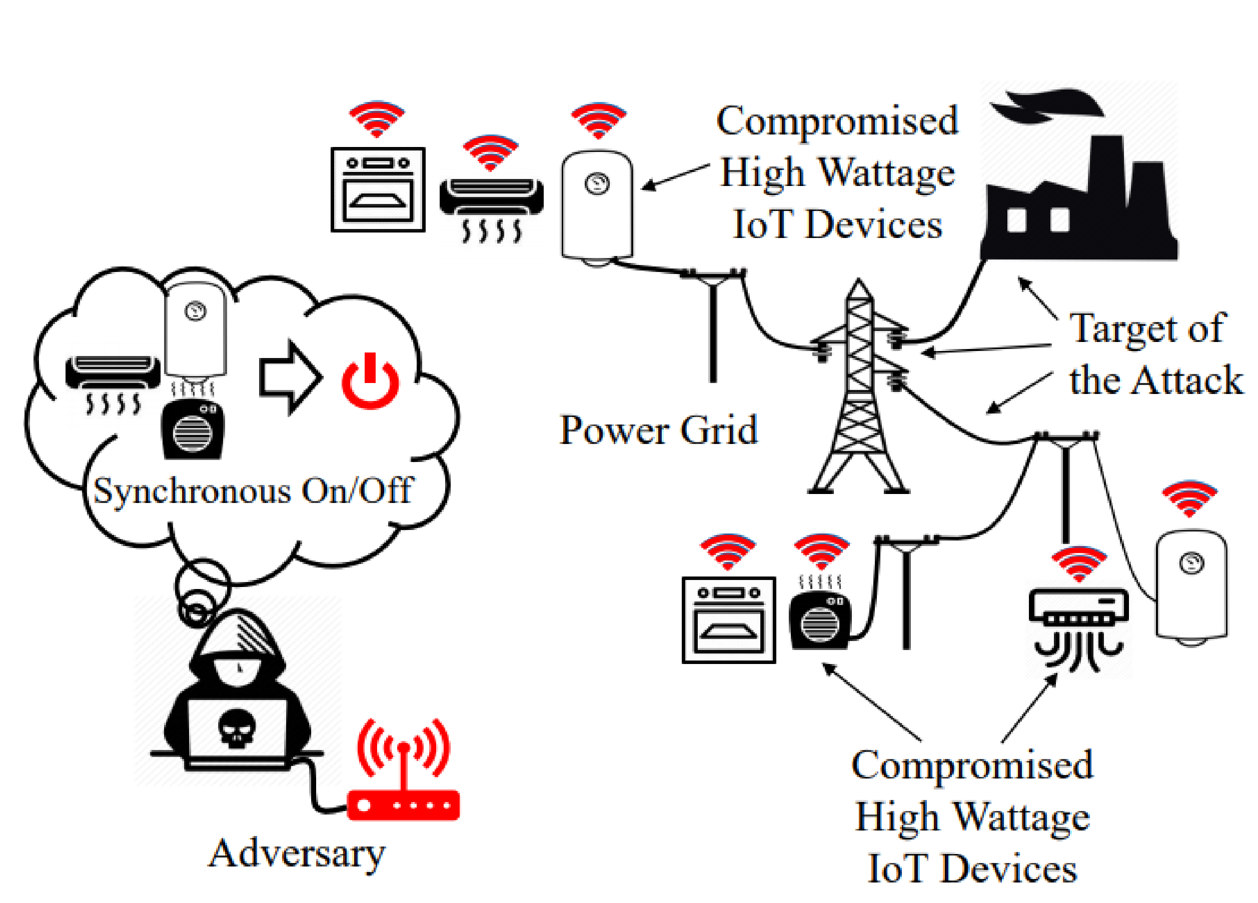


Capable of executing 38% of known attack techniques and 83% attack tactics cataloged by MITRE

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/

MaDIoT: Load alteration using IoT-networks*



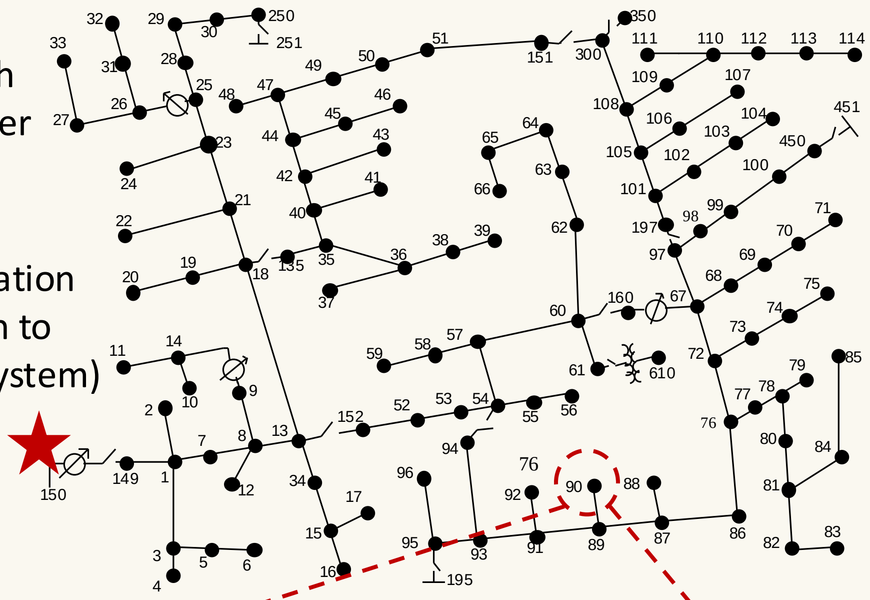
- Large scale manipulation of IoT devices – *botnets,* like Mirai botnets
- A 900MW step change in load with a tightly coordinated 600,000 IoT devices each controlling a 1500W HVAC unit

** Shekari, T., Cardenas, A.A. and Beyah, R., 2022. MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. In 31st USENIX Security Symposium*

IoT network: Challenges

PMO for each primary feeder

DSO at substation (Connection to transmission system)



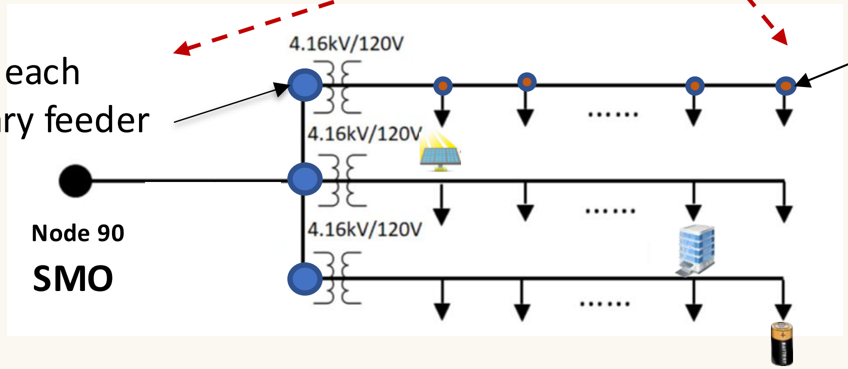
Primary feeder distribution network

IEEE 123 taxonomy feeder system

SMO for each primary feeder node

3 IoT devices per house
* 10 houses per secondary feeder
* 15 secondary feeders
* 11 primary feeders for a distribution feeder node
→ 3*10*15*11*123 = ≈ 600,000 IoT devices at transmission node

DCA for each secondary feeder



Energy managers at each secondary feeder node

3 radial secondary feeders (DCA) fanned out to each node with houses, PV, battery, EV etc.

A coordinated attack on all 600,000 IoT devices can lead to a **900MW** step change and a cascading failure

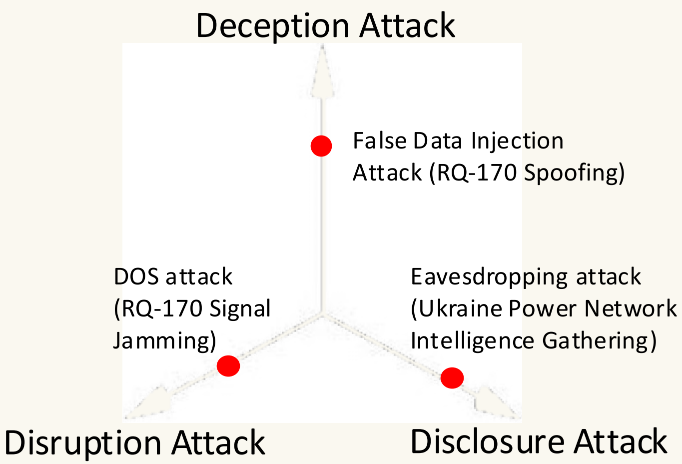
IoT – EV/HVAC/Critical loads etc.

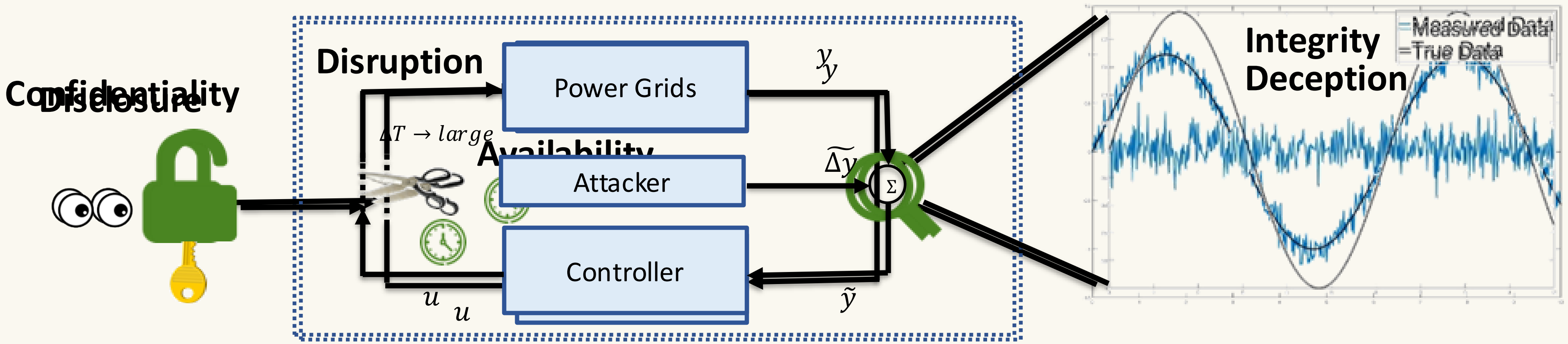
Residential Customer/DG

CIA and DDD: Defender/Attacker Perspectives

CIA Breaches / DDD Attacks

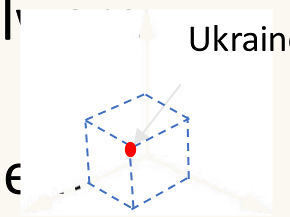
Cyber-security	Attacker Perspective
Confidentiality breach	**D**isclosure attack – ex. eavesdrop
Integrity breach	**D**eception attack – corrupt signals
Availability breach	**D**isruption attack – block, delay

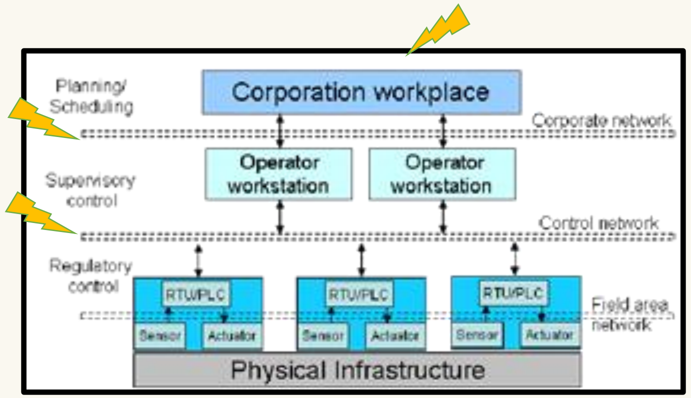




Ukraine Attack in 2015-16*

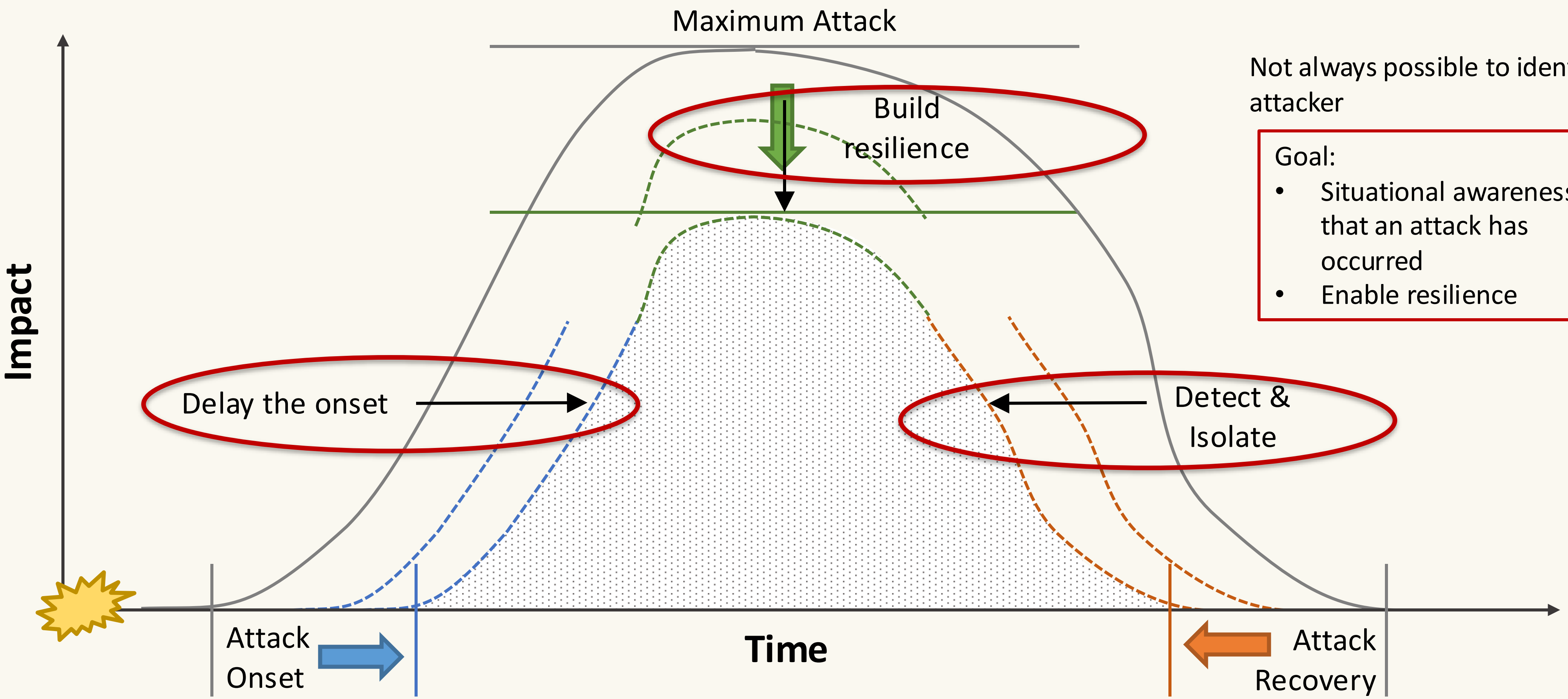
- **Confidentiality Attack (Disclosure)**:
  - Attack introduced via phishing emails containing BlackEnergy mal
  - Enabled attacker communication with hacked systems
  - Enabled attacker to steal critical data and study system environme
- **Integrity Attack (Deception)**:
  - Accessed control level over compromised VPN
  - Spoofed control commands
- **Availability Attack (Disruption)**:
  - Overwrote substation firmware, permanently ensuring remote inoperability of breakers
- 30 substations switched off
- 230,000 customers left without power
- The 2016 attack corrupted transmission control





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

Cyber-Physical Security in Power Grids



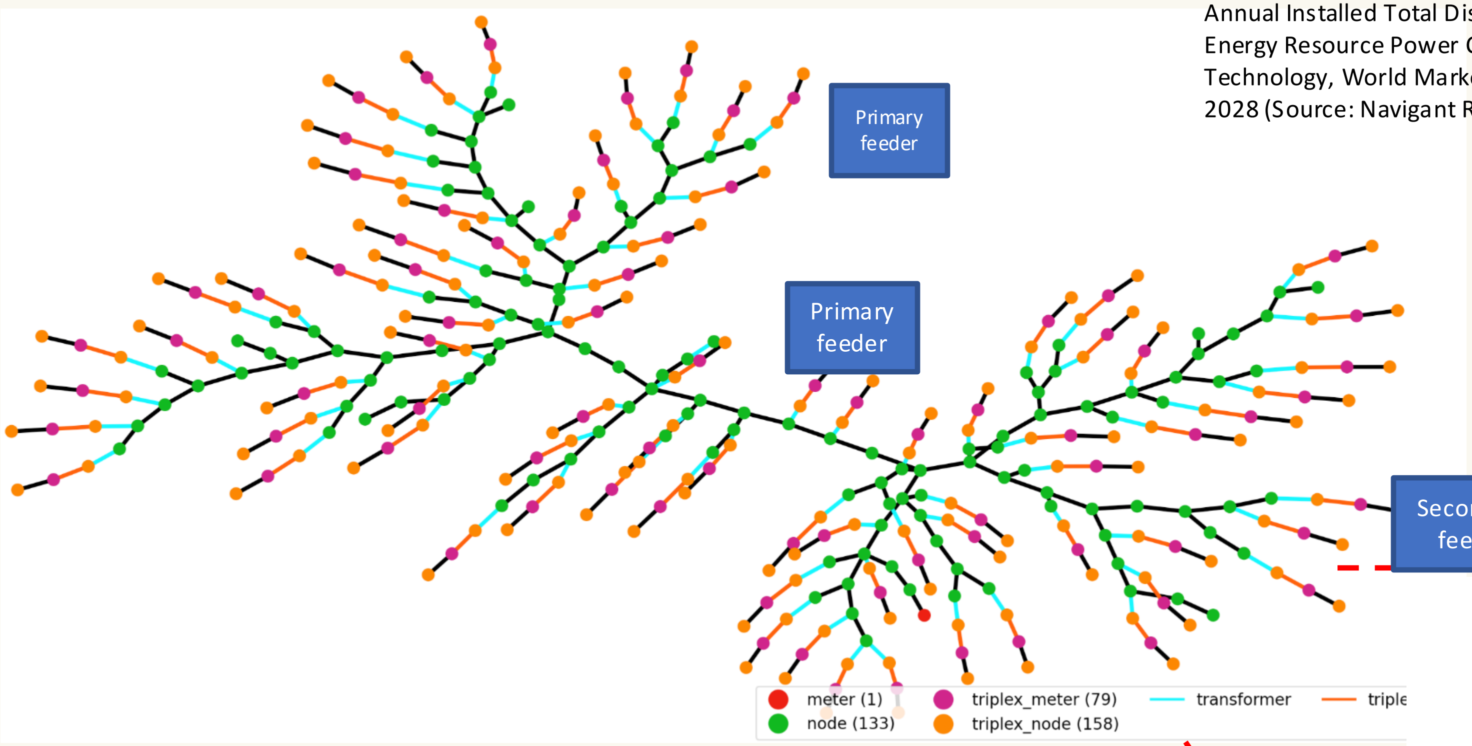
Not always possible to identify the attacker

Goal:

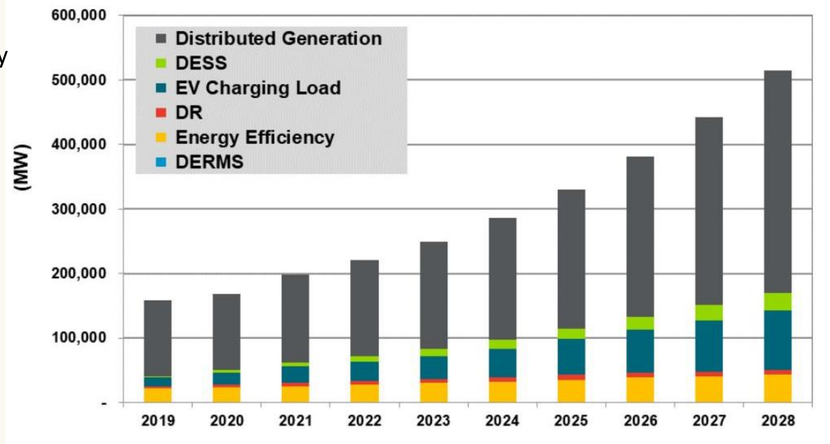
- Situational awareness that an attack has occurred
- Enable resilience

Goal: Develop methods to reduce the central region

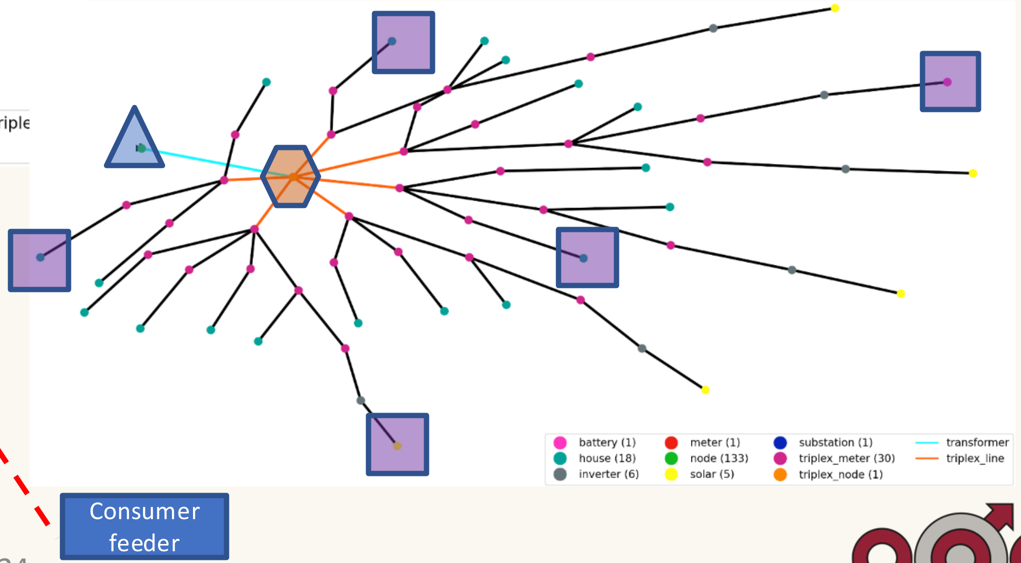
Optimization challenging with billions of end-point control



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



Increasing DER penetration



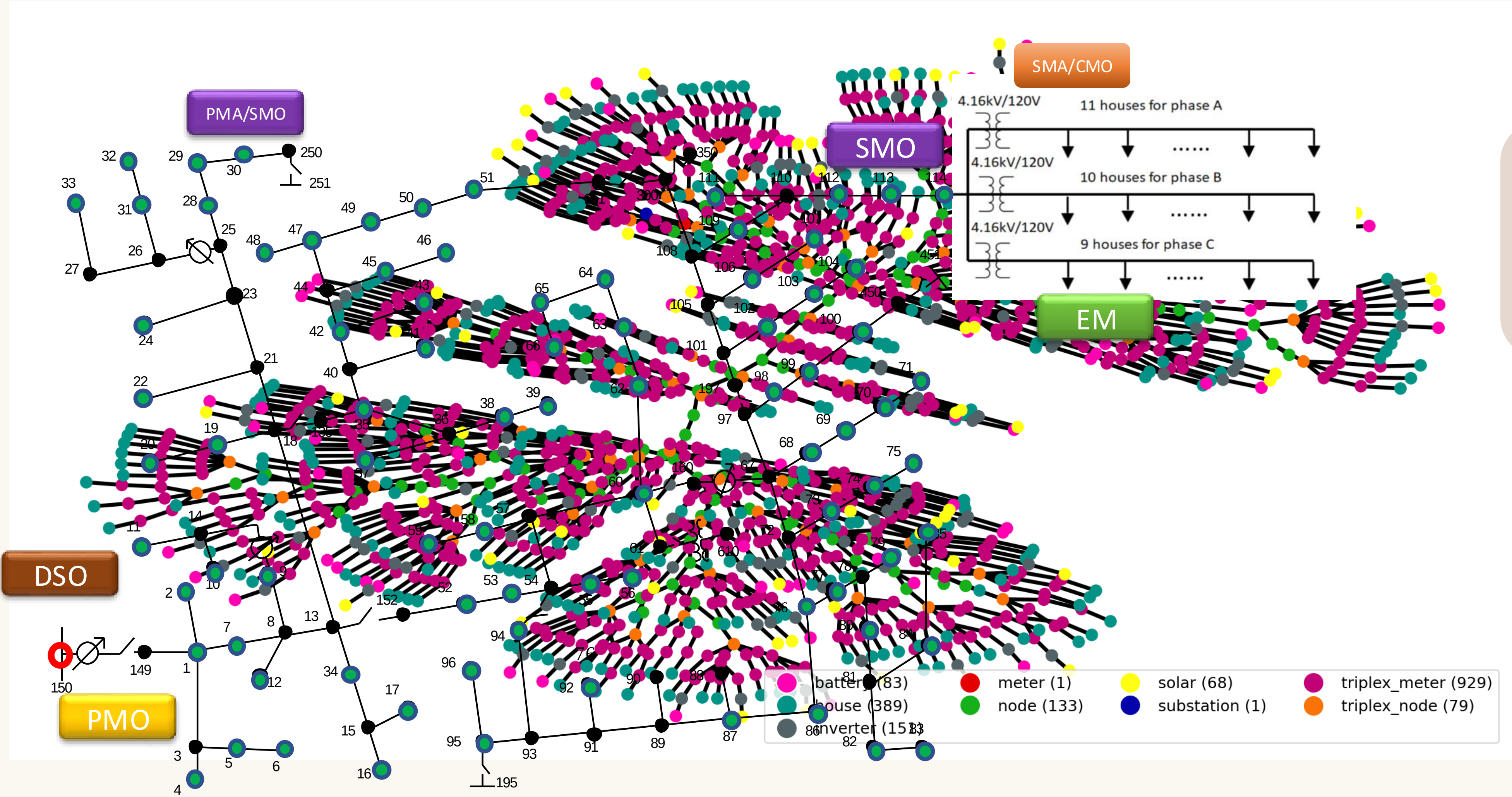
400 Secondary Feeders

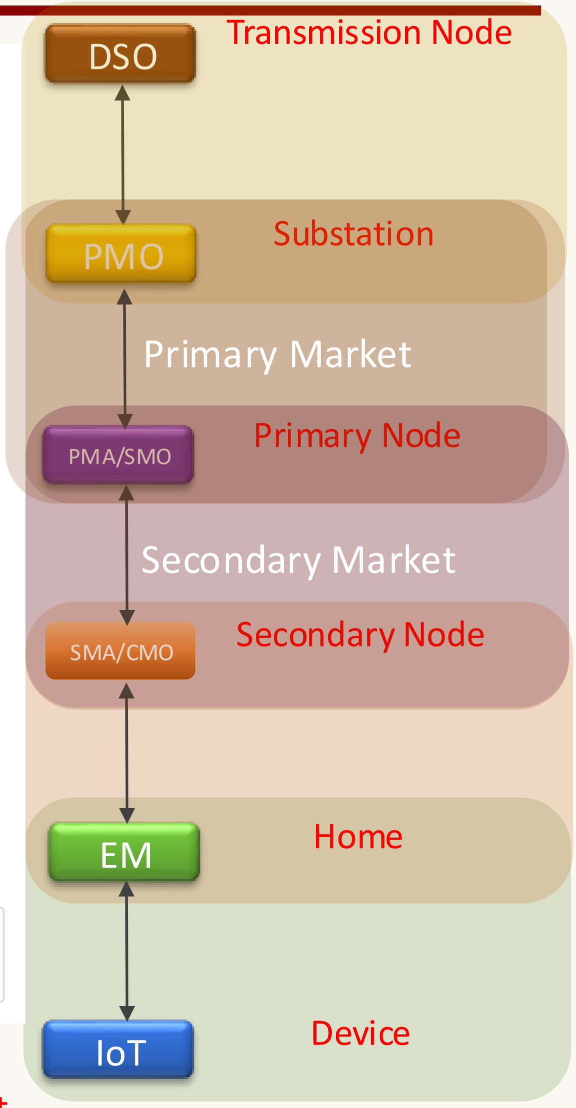
1000 IoT devices
100 PVs (531.5 KW)
200 batteries

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

Source: PNNL Gridlab-D Modeling Team

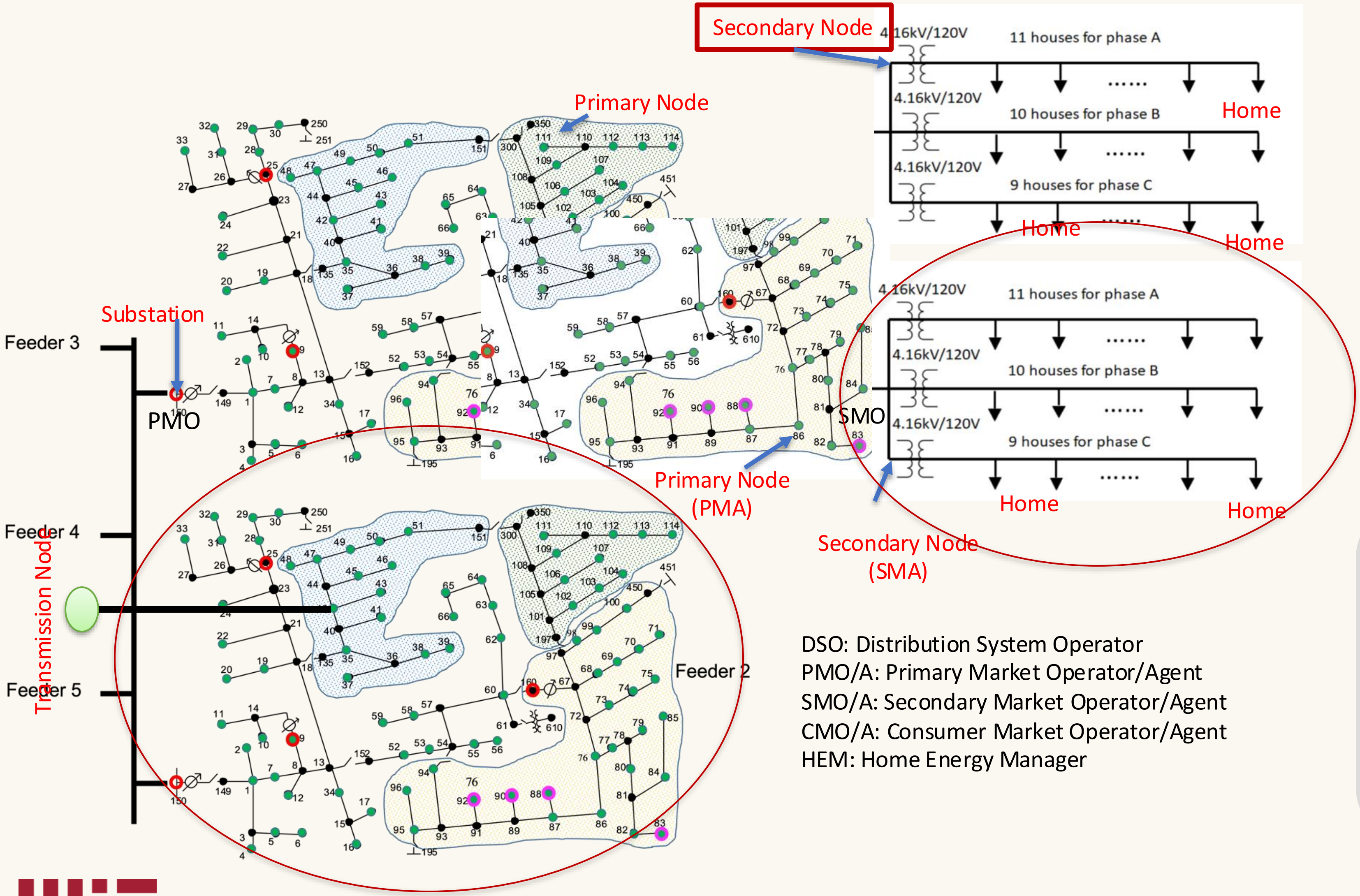
We have a model*



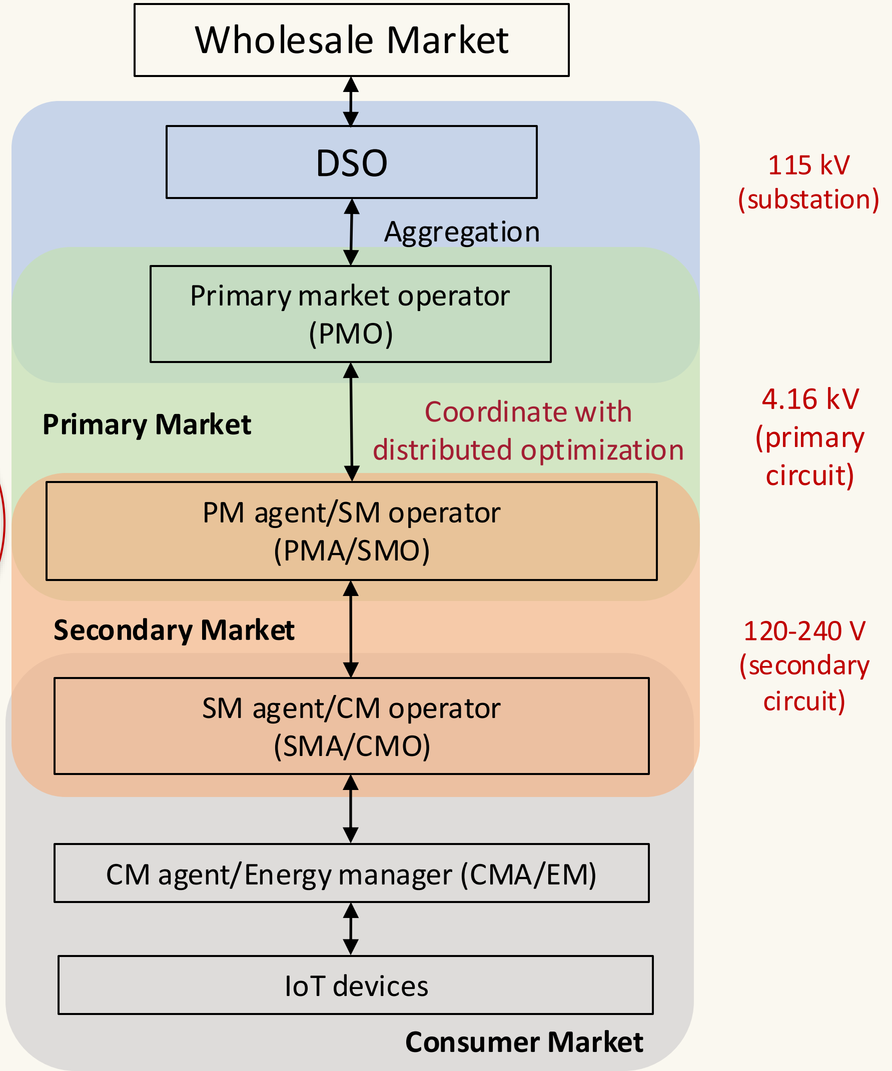


*100,000 nodes, Efficient UltRa Endpoint IoT-enabled Coordinated Architecture (EUREICA), DoE project

Proposed hierarchical local electricity market (LEM)

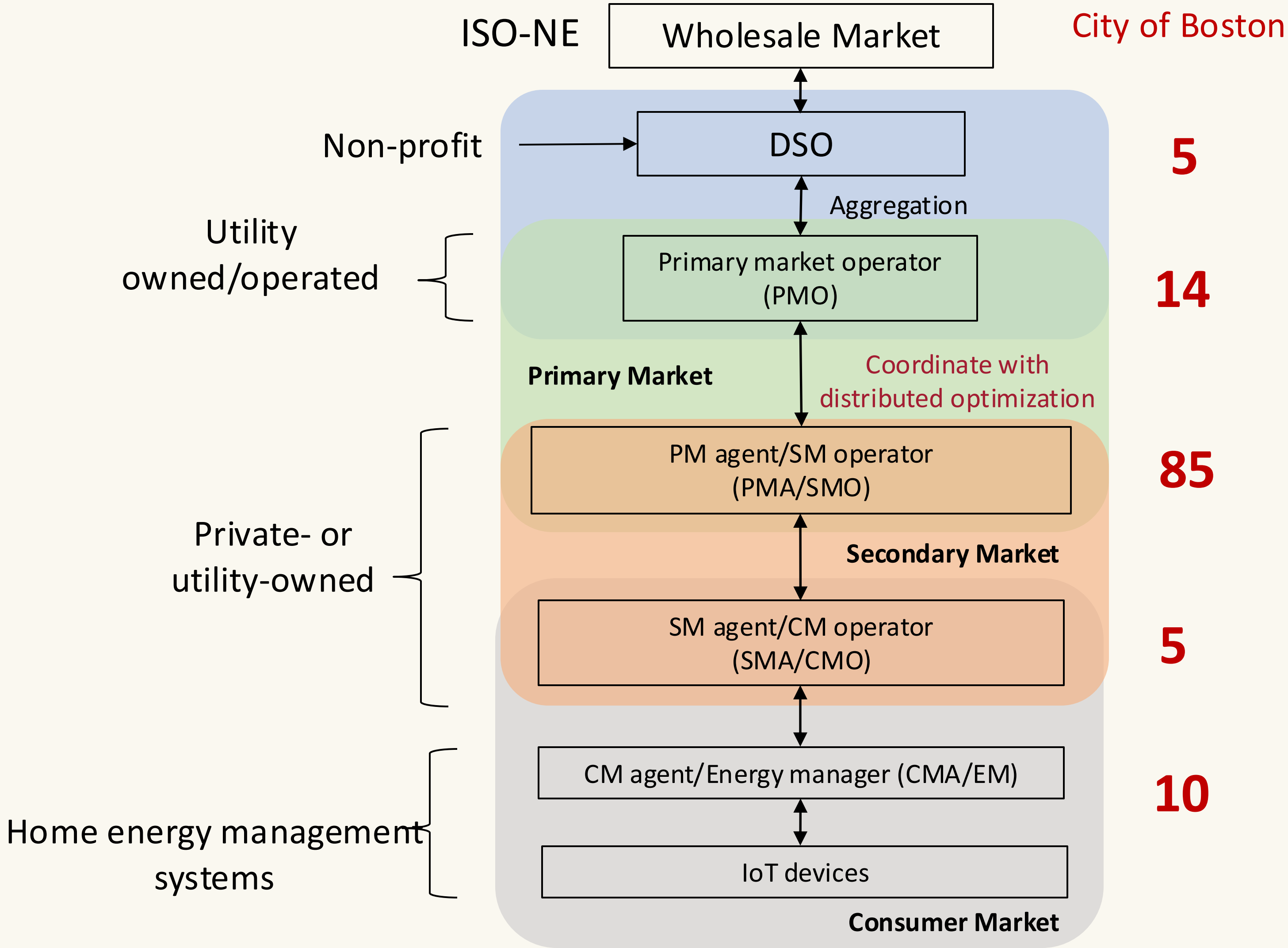


DSO: Distribution System Operator
PMO/A: Primary Market Operator/Agent
SMO/A: Secondary Market Operator/Agent
CMO/A: Consumer Market Operator/Agent
HEM: Home Energy Manager

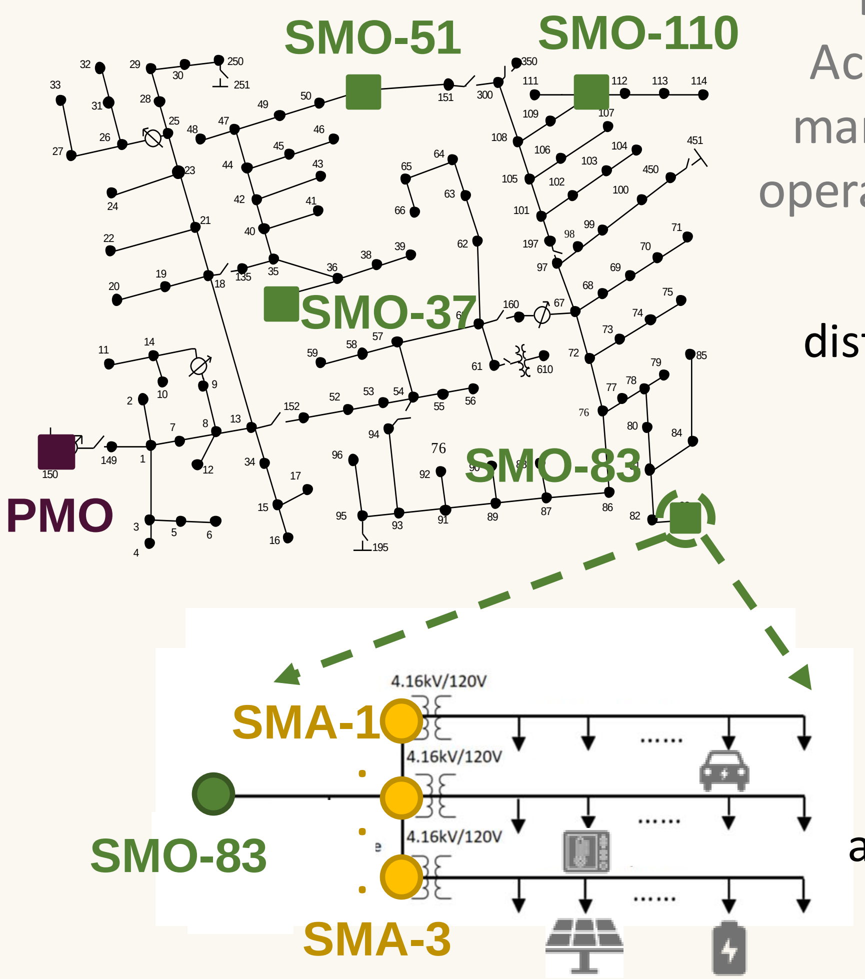


Different players in the LEM

- 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



Hierarchical local electricity markets (LEM)



Hierarchical paradigm:
Accommodate concerns for market stakeholders and grid operators at all levels of the grid

115 kV

Power physics and distribution-level constraints (unbalanced network)

Distributed Optimization

4.16 kV

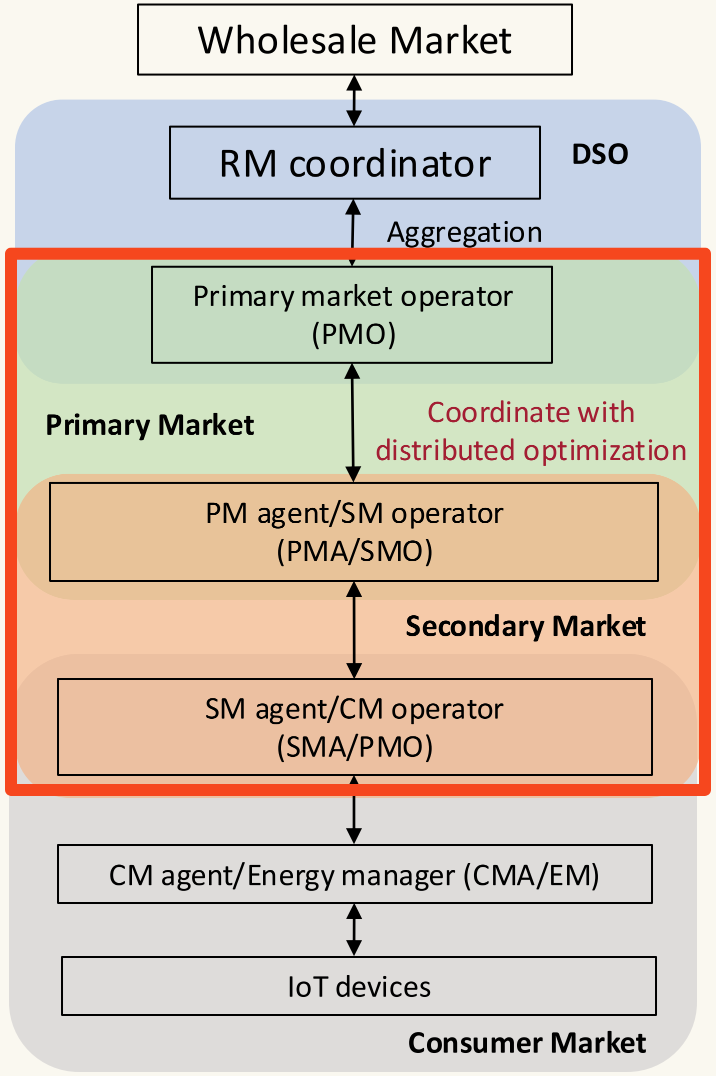
Commitment reliability and Budget constraints

Multi-objective Optimization

120-240 V

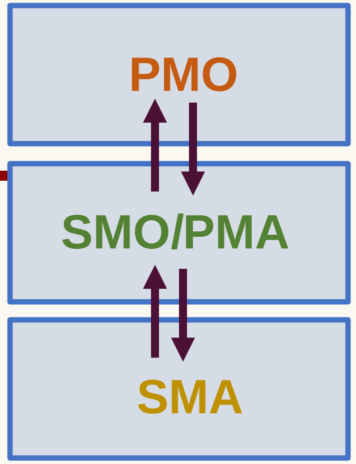
Consumer preferences and end-use data privacy

Game theory, Federated Learning



* Haider et al., Advances in Applied Energy, 2022; Nair et al., TSG 2022; Nair et al., CCTA 2023, Nair et al., ICCPS 2024.

Primary market (PM) operation*



- Primary market clearing: Solve **optimal power flow (OPF)** problem
- Can accommodate different types of distribution networks:
  - Branch flow model → Radial, balanced systems
  - Current injection model → Meshed, unbalanced networks
- Satisfy **grid physics**: Ohm's & Kirchhoff's law, power balance with losses, voltage/current bounds, capacity limits
- Solve PM using **privacy-preserving distributed optimization** algorithm → SMOs only communicate with their neighbors

* Haider et al., Advances in Applied Energy, 2022; Romvary et al. IEEE TAC, 2021, Haider et al., TSG 2021

Distributed optimization: Proximal atomic coordination (PAC)*

$$\min_{x \in \mathbb{R}^n} \sum_{i=1}^{n} f_i(x_i) \quad s.t. \quad Gx = b, \; Hx \le d$$

Atomization

$$\min_{a_j} \sum_{j=1}^{k} f_j(a_j) \quad s.t. \quad G_j a_j = b_j, \; H_j a_j \le d_j, \; B_j a = 0 \quad \forall j \in k$$

Lagrangian

$$\mathcal{L}(a, \mu, \nu) = \sum_{j \in K} \left[f_j(a_j) + \mu_j^T (G_j a_j - b_j) + \nu_j^T B_j a \right] \triangleq \sum_{j \in K} \mathcal{L}_j(a_j, \mu_j, \nu).$$

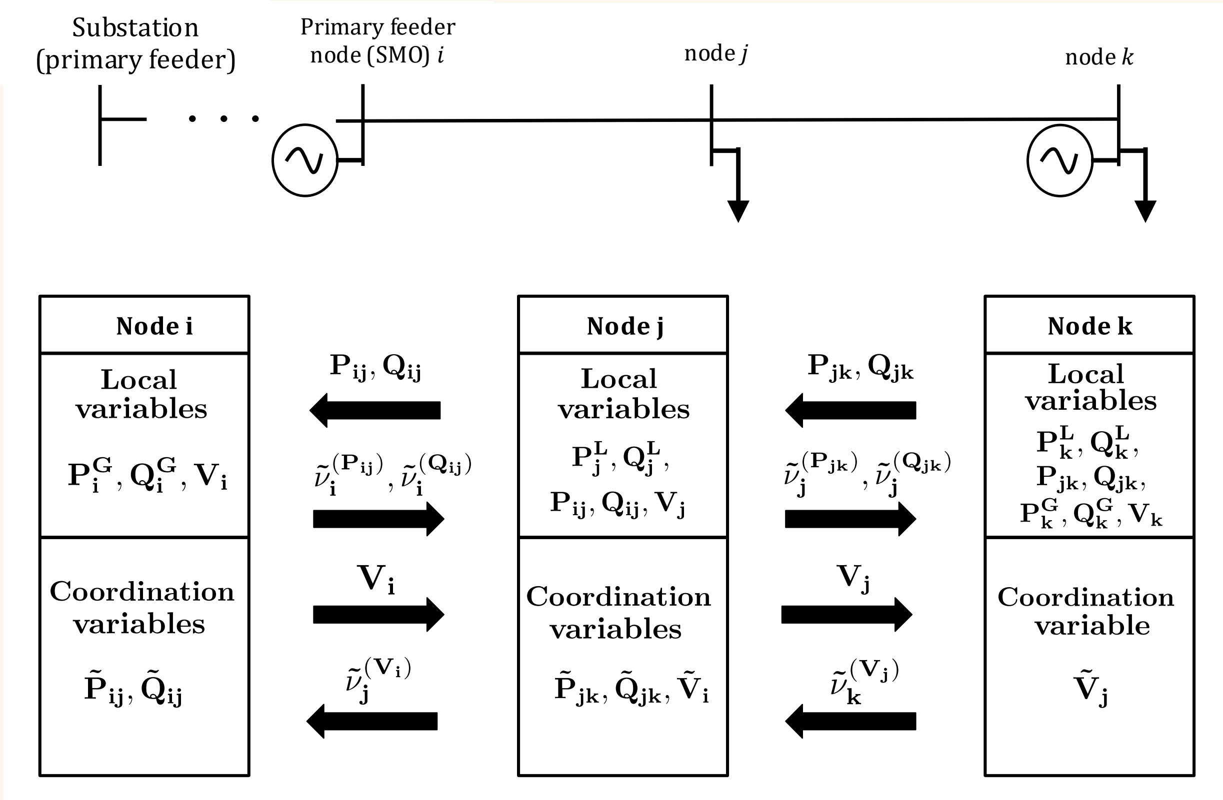
$$a_j[\tau+1] = \underset{a_j}{\operatorname{argmin}} \left\{ \mathcal{L}_j(a_j, \hat{\mu}_j[\tau], \hat{\nu}[\tau]) + \frac{1}{2\rho} \|a_j - a_j[\tau]\|_2^2 \right\}$$

$$\mu_j[\tau+1] = \mu_j[\tau] + \rho \gamma_j \tilde{G}_j a_j[\tau+1] \text{ and } \hat{\mu}_j[\tau+1] = \mu_j[\tau+1] + \rho \hat{\gamma}_j[\tau+1] \tilde{G}_j a_j[\tau+1]$$

Communicate $\{a_j[\tau+1]\}$ with neighbours, for all j

$$\nu_j[\tau+1] = \nu_j[\tau] + \rho \gamma_j [B]_j a[\tau+1] \text{ and } \hat{\nu}_j[\tau+1] = \nu_j[\tau+1] + \rho \hat{\gamma}_j[\tau+1] [B]_j a[\tau+1]$$

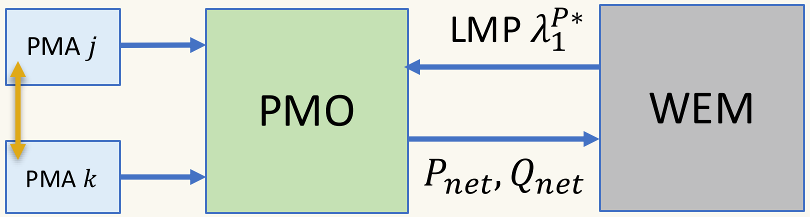
Communicate $\{\hat{\nu}_j[\tau+1]\}$ with neighbours, for all j



* Romvary et al. IEEE TAC, 2021, Haider et al., TSG 2021

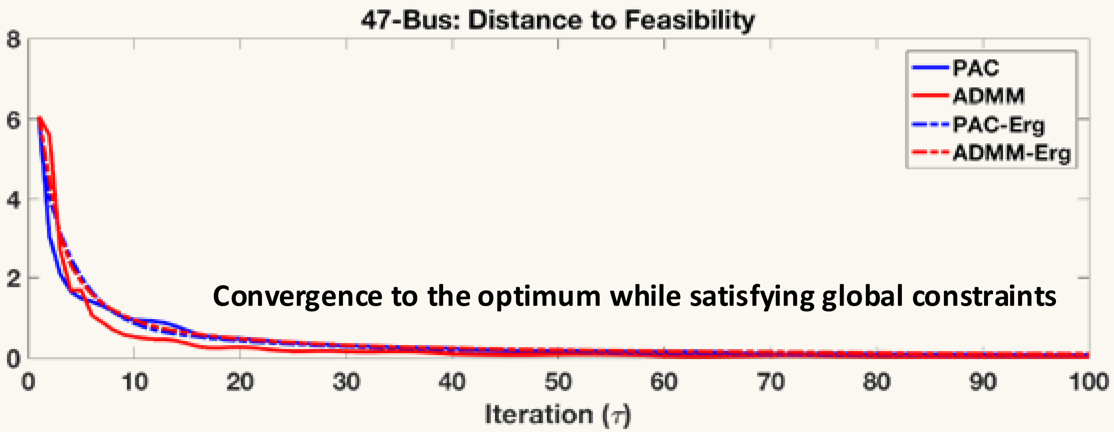
Primary retail market clearing using SMO bids & PAC

Every 1 min   average during 5min

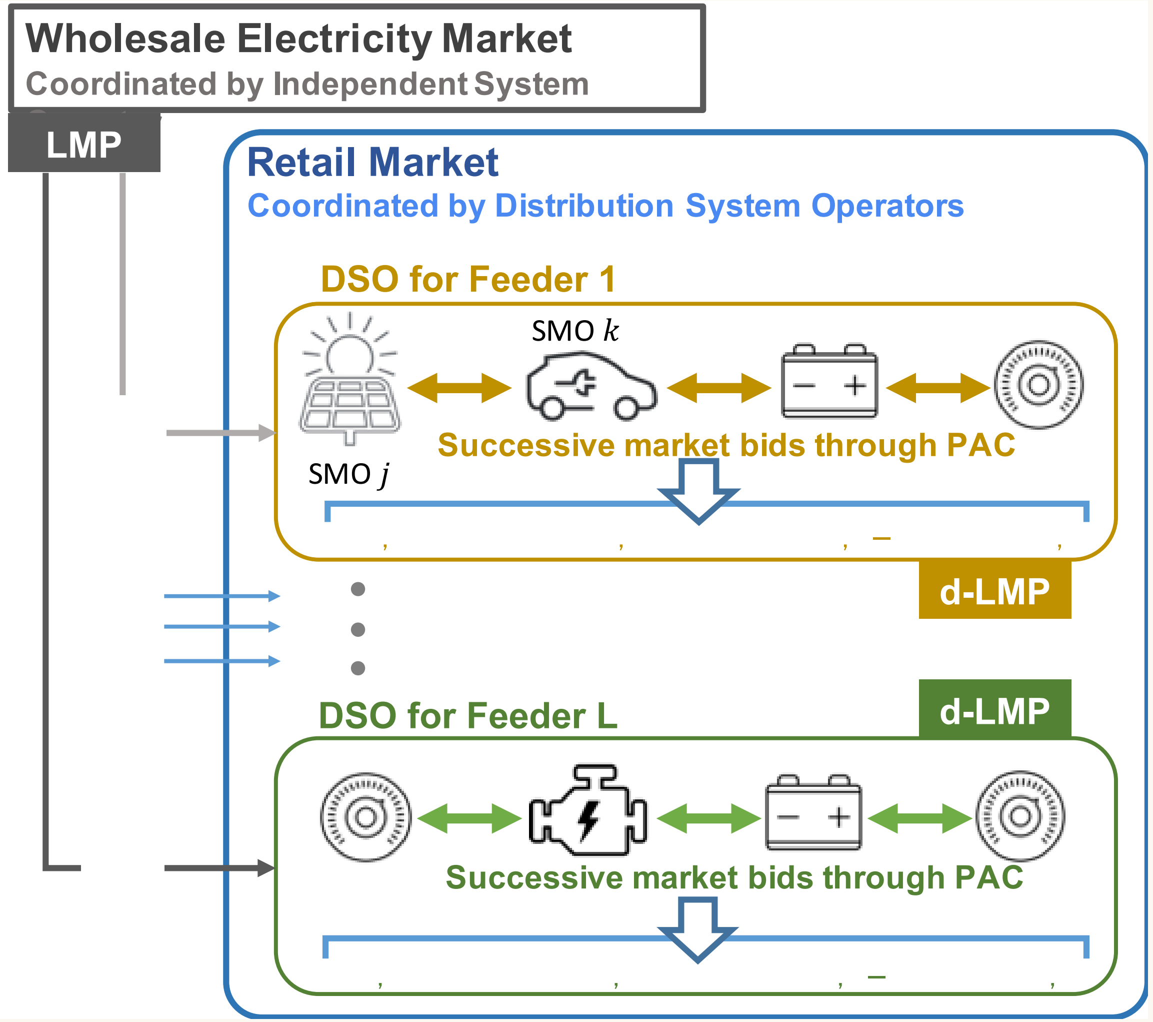


$P_j^{G^*}, Q_j^{G^*}, P_j^{L^*}, Q_j^{L^*}, j \in \mathcal{B} = 1, \dots, 123$

d-LMPs $\mu_j^{P^{G^*}}, \mu_j^{Q^{G^*}}, \mu_j^{P^{L^*}}, \mu_j^{Q^{L^*}}, j \in \mathcal{B} = 1, \dots, 123$



- Fully distributed
- Computationally tractable
- Reduced communication requirements
- Preserve data privacy



* Haider et al., Advances in Applied Energy, 2022; Romvary et al. IEEE TAC, 2021, Haider et al., TSG 2021

Secondary market (SM) operation*

SMOs aggregate schedules of all their SMAs → Provide flexibility bids into primary market

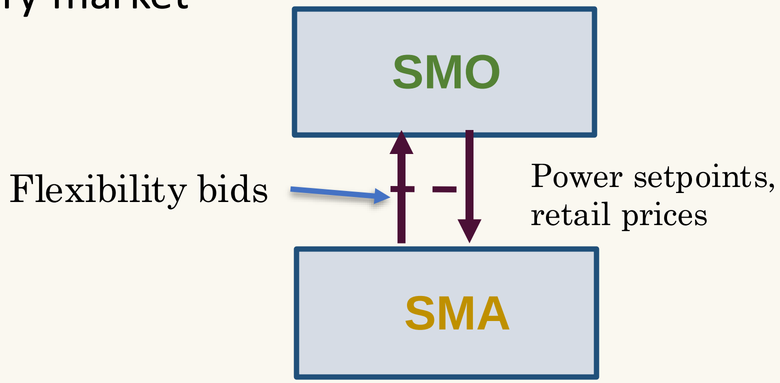
$$\min_{\vec{s_j}} \sum_j w_1\left(\beta_j^P\left(P_j-P_j^0\right)^2+\beta_j^Q\left(Q_j-Q_j^0\right)^2\right) + w_2\left(\mu_j^P P_j+\mu_j^Q Q_j\right) - w_3\left(\delta P_j+\delta Q_j\right) - w_4 RS_j(t)\left(\left(P_j\right)^2+\left(Q_j\right)^2\right)$$

Resilience score

Min: disutility to SMA_j

Min: net cost to SMO

Max: aggregate flexibility & reliability



Subject to:

- Device operating and flexibility limits (P and Q limits)
- Budget balance: revenue exceeds payments
- Price cap for retail prices
- Lossless power balance

Solve multi-objective optimization via hierarchical approach

$$w_1+w_2+w_3+w_4=1$$

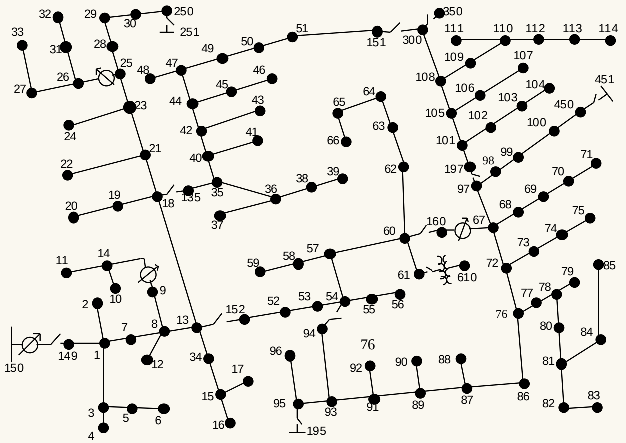
- **Trustability score (TS)**: Captures possibly of agents (& their IoT devices) being compromised due to cyber anomalies or vulnerabilities
- **Commitment score (CS)**: Measures how reliably agents will follow through & meet their contractual commitments
- **Resilience score (RS)** combines both to provide overall situational awareness

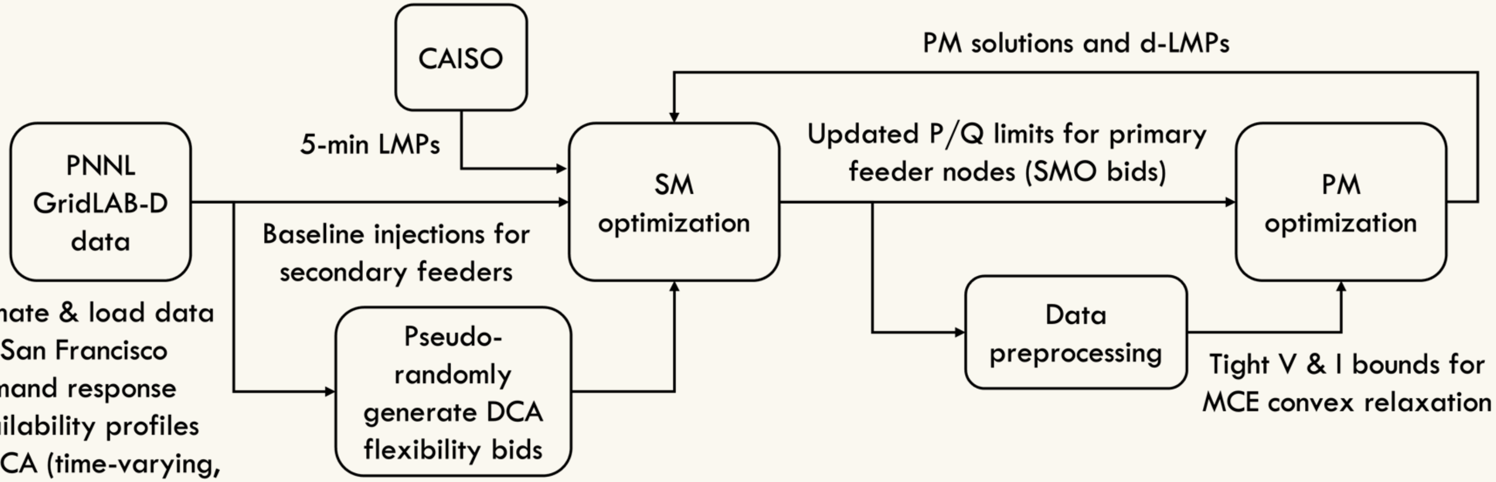
$$RS_j = CS_j + (1-\alpha)TS_j, 0 \le \alpha \le 1$$

Nair et al., TSG 2022; Nair et al., CCTA 2023, Nair et al., ICCPS 2024.

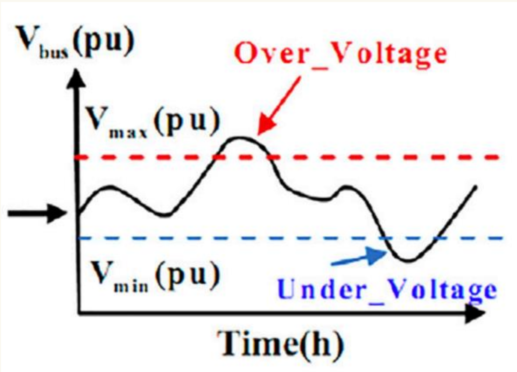
Co-simulation of primary + secondary markets*

Data from modified
IEEE-123 GridLAB-D model





- Climate & load data for San Francisco
- Demand response availability profiles for CA (time-varying, up to 50%)

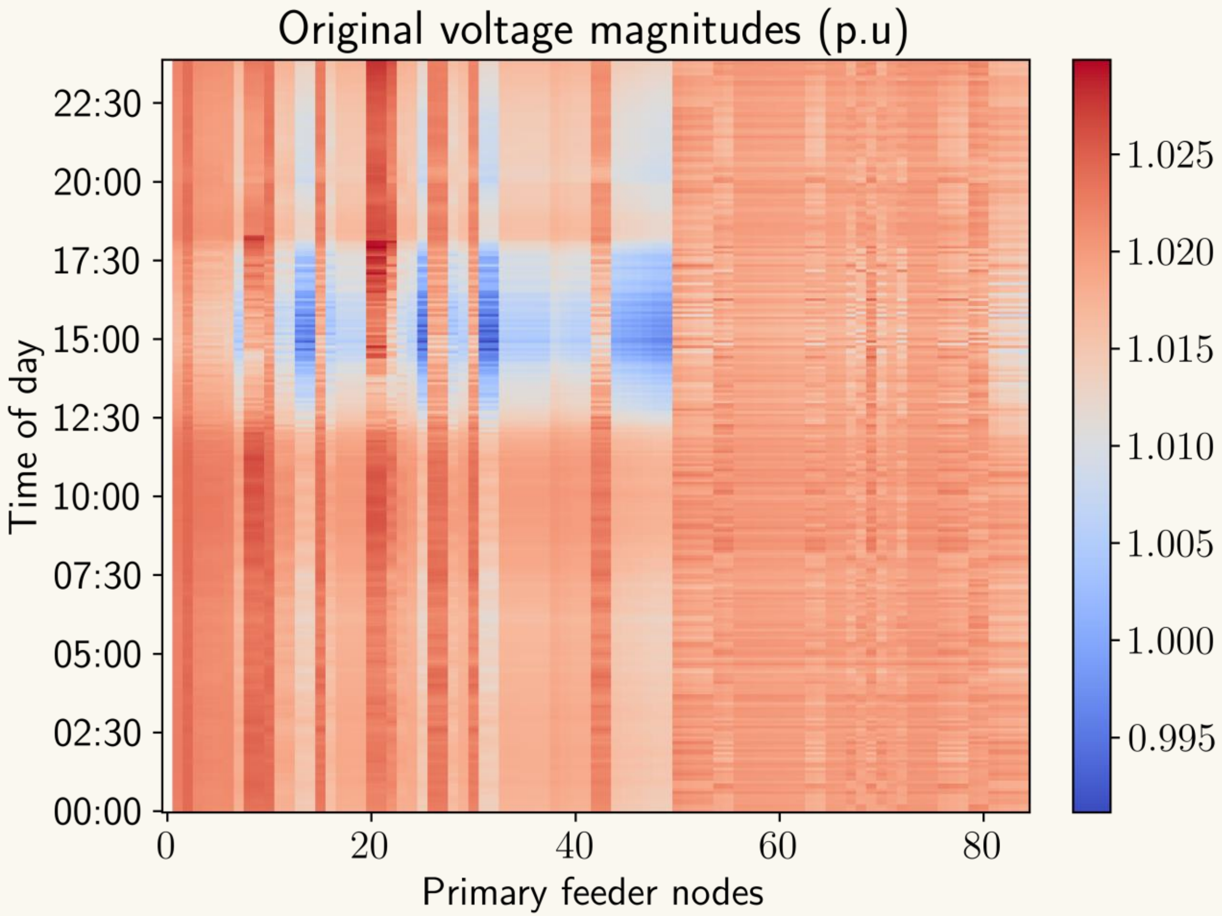


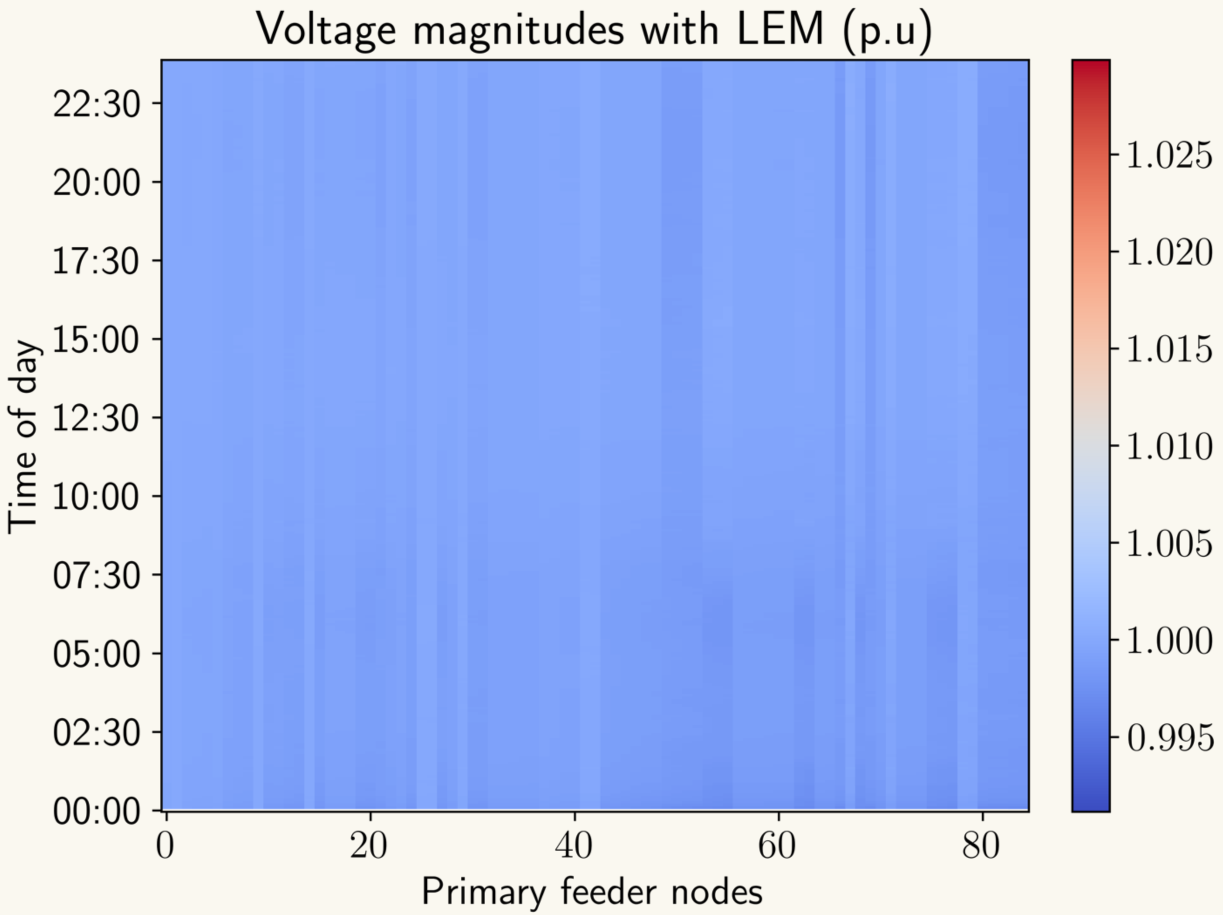
- Accelerated by parallelizing independent SM clearings
- Mitigate voltage issues common in low-medium voltage distribution grids, e.g.
  - High PV output → Over-voltage
  - Demand spikes from HVAC → Under-voltage

Type	Number	Capacity
DERs	380	1,745.8 kVA (~**44%**)
PVs	207	880.84 kVA
Batteries	173	865 kVA
Spot loads	85	3,985.7 kVA
Houses	1008	4-10 kW (variable)
Flexible loads	1-2 per house	10-50% flexibility (variable)

* Nair and Annaswamy, Local retail electricity markets for distribution grid services, CCTA 2023

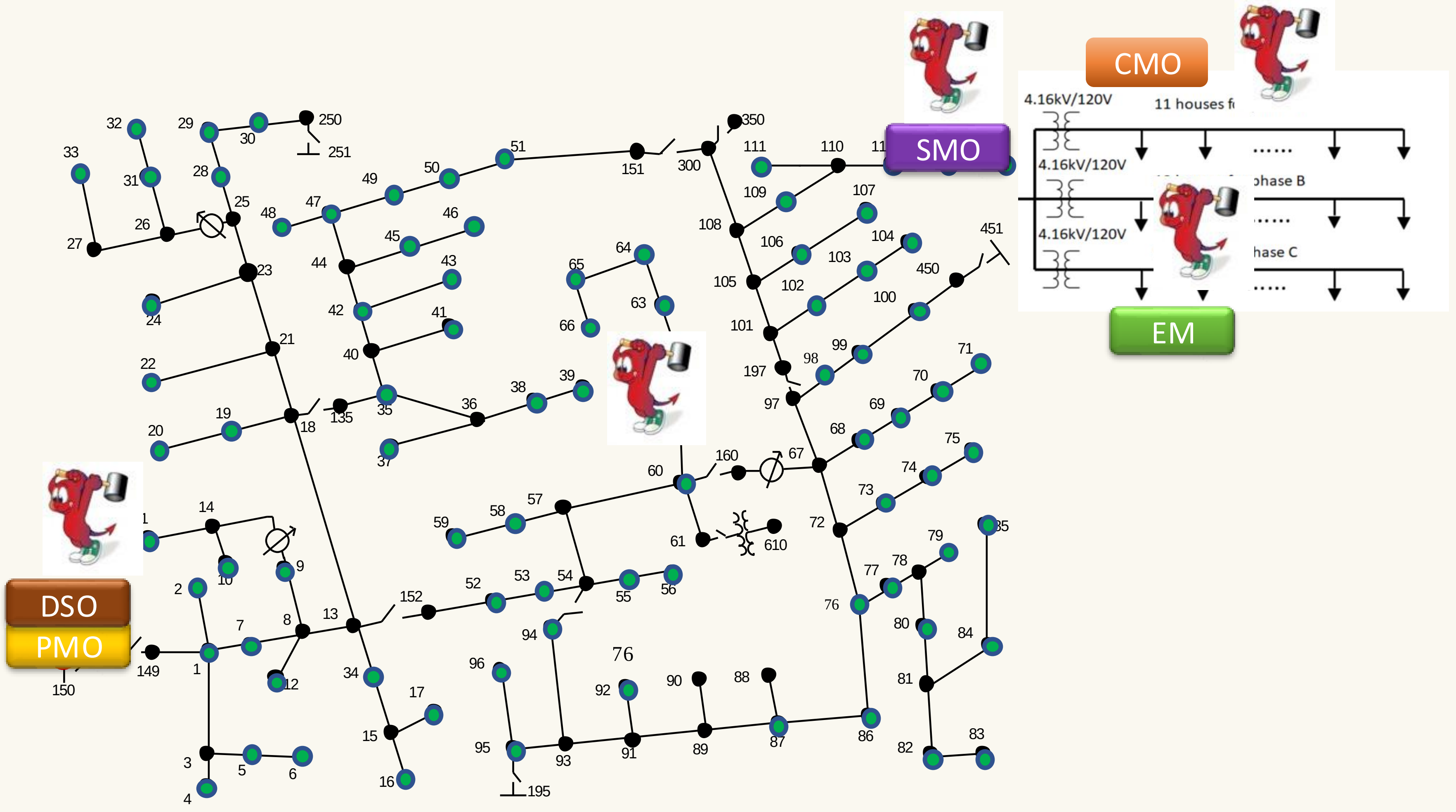
Numerical simulation results: Improved voltage profiles

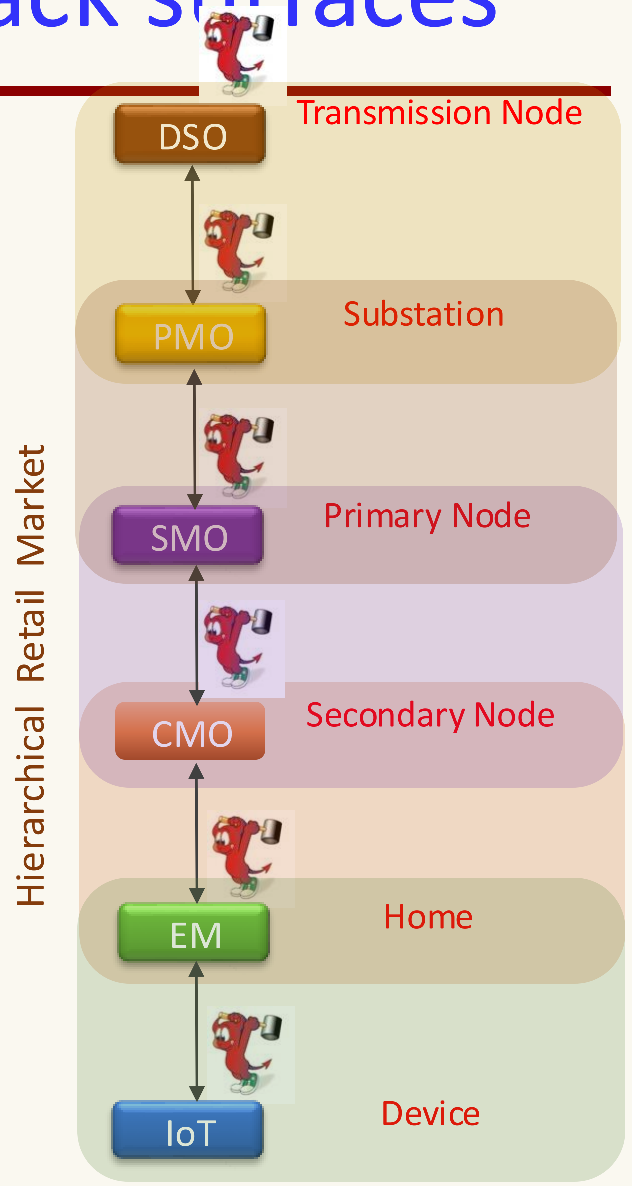




LEM (SM + PM) improves overall voltage profile → More uniform + closer to 1 p.u.

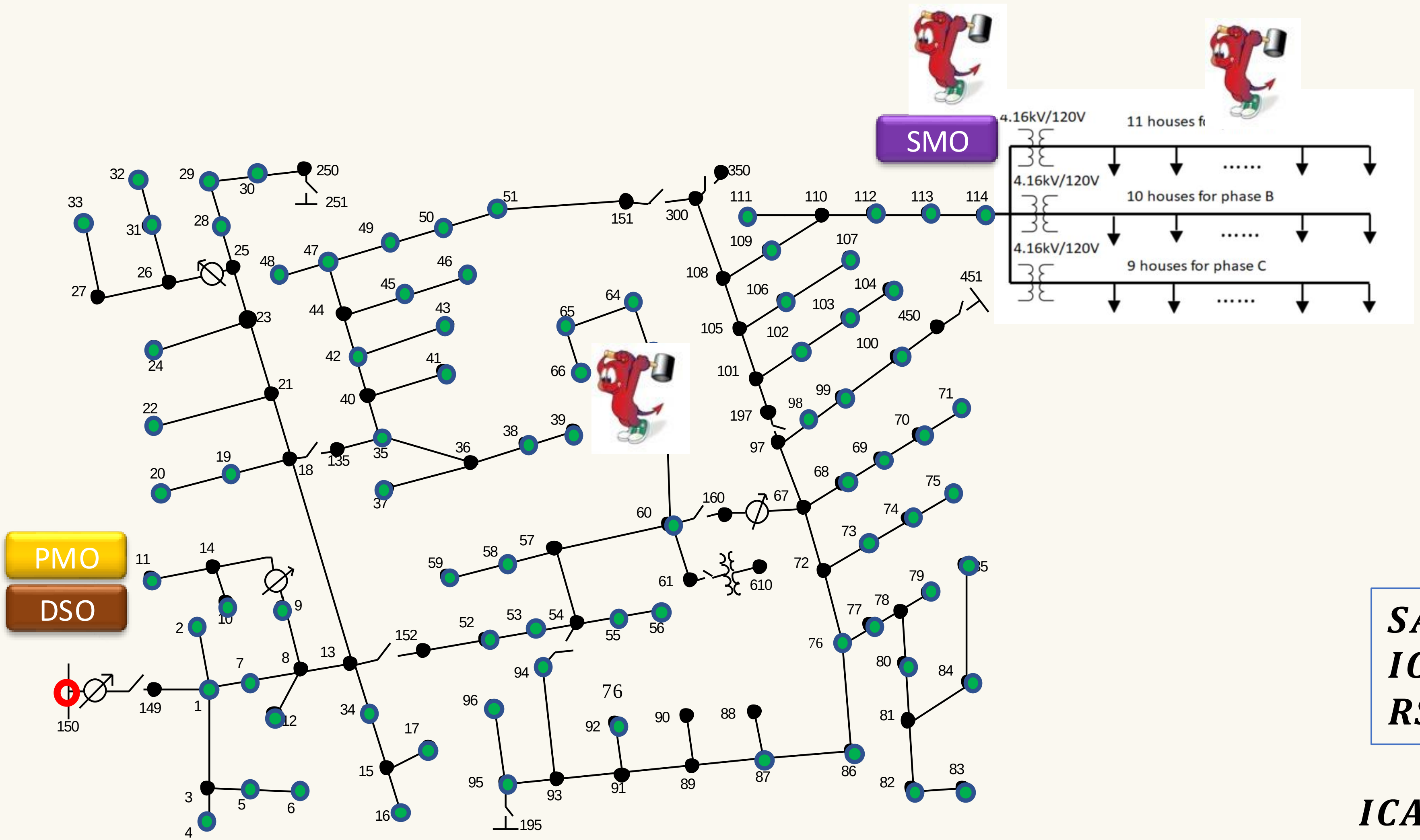
Leverage the Market Structure: Build attack surfaces

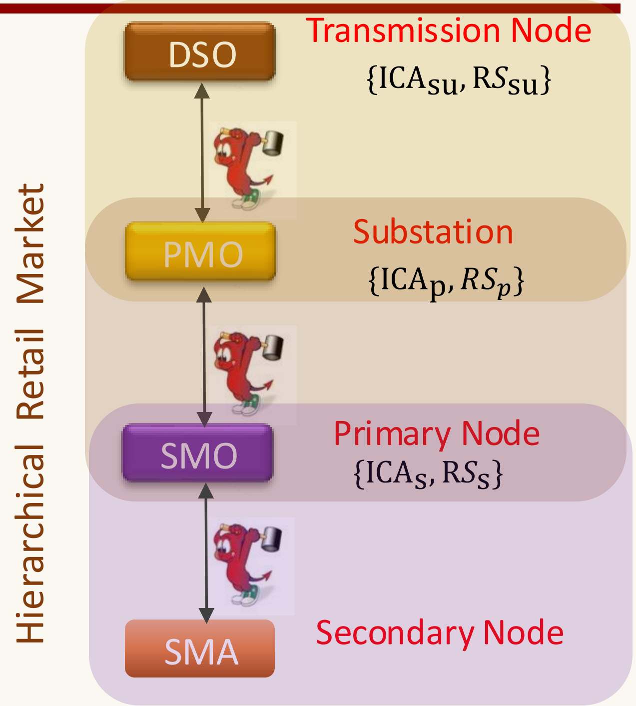




Emulate several large-scale attacks

Second step: Develop Situational Awareness (SA)



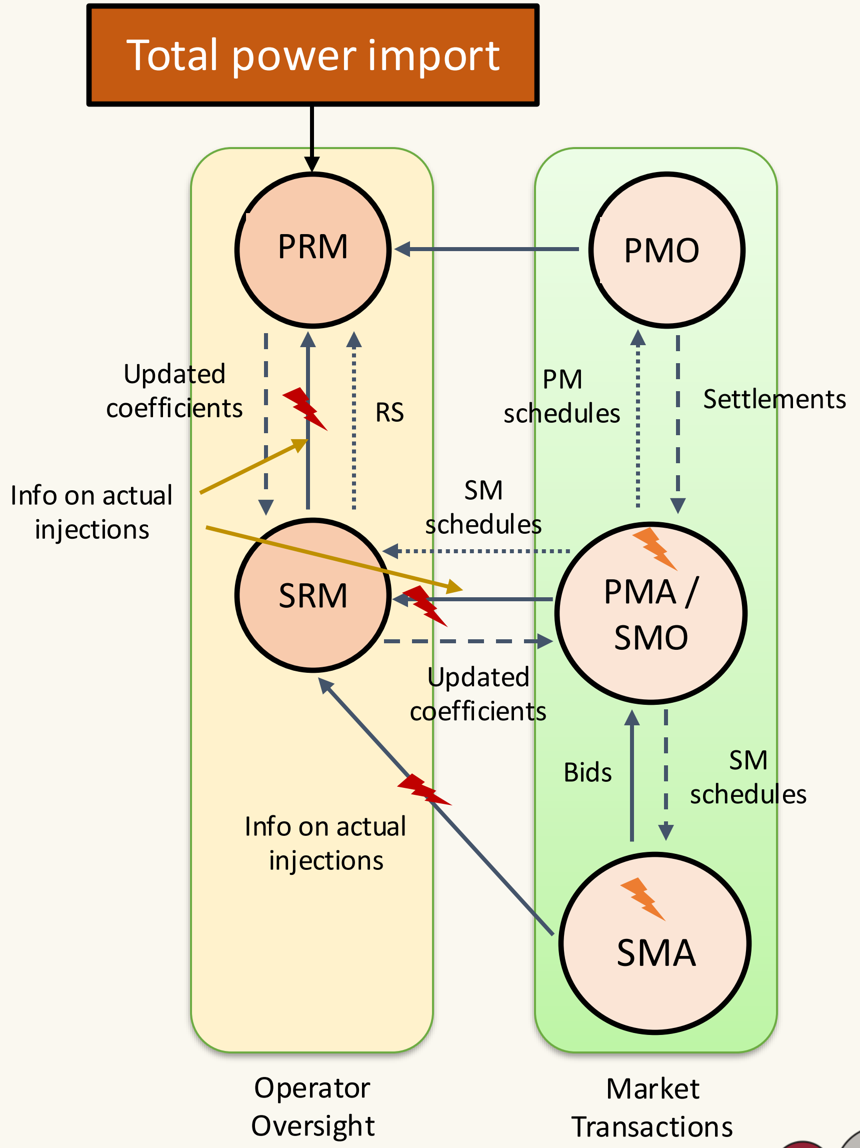


$SA_x = \{ICA_x, RS_x\}$ at node x
$ICA_x = \{P_x, Q_x\}$ at node x
RS_x = Resilience Score of node x

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



Attack detection & mitigation

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

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

$$\Delta = \mathbf{P}_{cc} - \overline{\mathbf{P}}_{cc} \tag{2}$$

$$Z_i(\delta_i) = 1 + \frac{RS_i \Delta^\top \delta_i}{\mu \sum_i RS_i} \implies \gamma_{i\delta} = \frac{1}{Z_i(\delta_i)} \tag{3}$$

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

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

Intuition behind coefficient updates

Suppose several local DGs are attacked → Increases net feeder load i.e. $|\overline{\boldsymbol{P}}_{cc}| > |\boldsymbol{P}_{cc}|$
This would result in the following coefficient updates:

1. $\gamma_{i\alpha} < 1$: Lowers cost coefficients to dispatch more local generation from remaining online SMOs instead of importing power from WEM

2. $\gamma_{i\beta} < 1$: Reduces disutility coefficients to encourage demand response via load shifting/curtailment

3. $\bar{\xi} > \xi$: Penalizes electrical line losses more heavily → Discourages imports from transmission grid in favor of dispatching more local DERs closer to the loads being served.

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

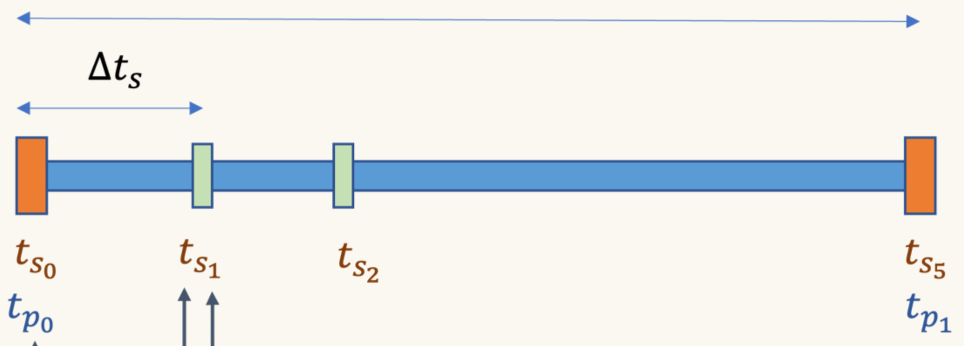
$$\Delta = \mathbf{P}_{cc} - \overline{\mathbf{P}}_{cc} \quad (2)$$

Assets with higher RS are used to a greater extent for attack mitigation

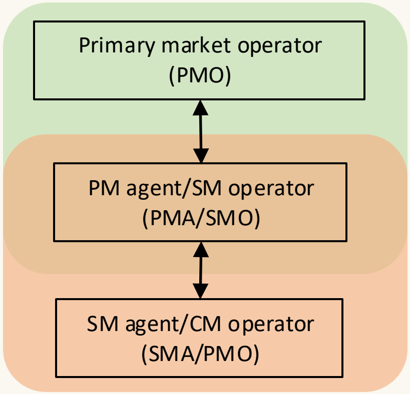
$$Z_i(\delta_i) = 1 + \frac{RS_i \Delta^\top \delta_i}{\mu \sum_i RS_i} \implies \gamma_{i\delta} = \frac{1}{Z_i(\delta_i)} \quad (3)$$

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

Timeline of attack & mitigation steps



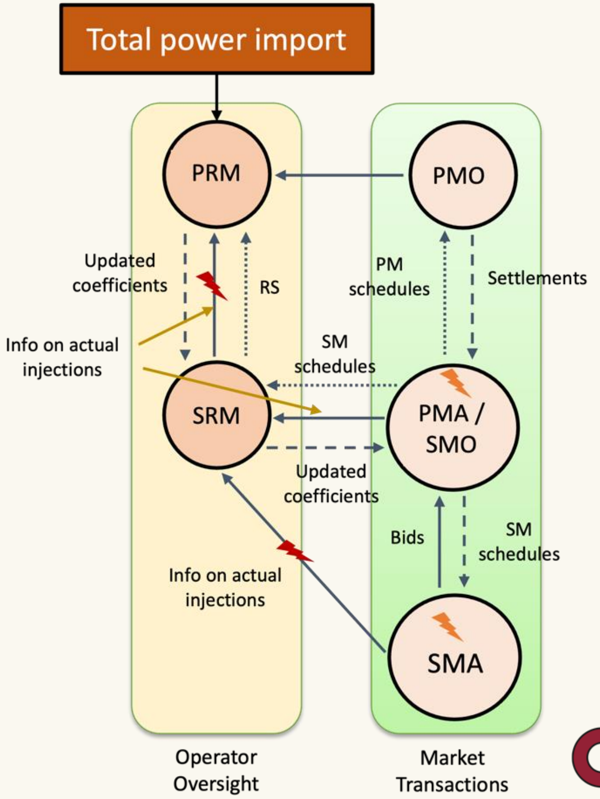
Mitigation involves PM redispatch followed by SM redispatch



6. SM redispatch with new PM solution: SMOs disaggregate new setpoints amongst their SMAs within their flex bids for $[t_{s_1}, t_{s_2}]$

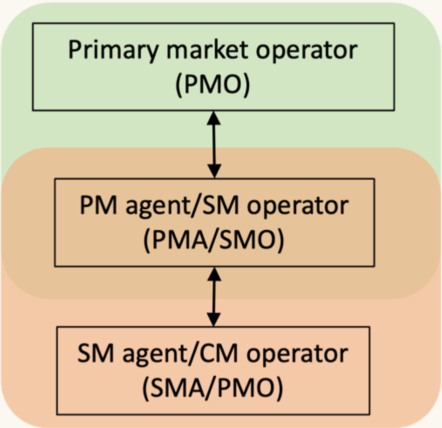
3. SMAs submit bids for $[t_{s_1}, t_{s_2}]$
4. SMO attacked
5. Mitigation:
   - PRM broadcasts cost coefficient updates to all SMOs
   - PMO redispatches all SMOs for $[t_{s_1}, t_{p_1}]$ within their flexibility limits

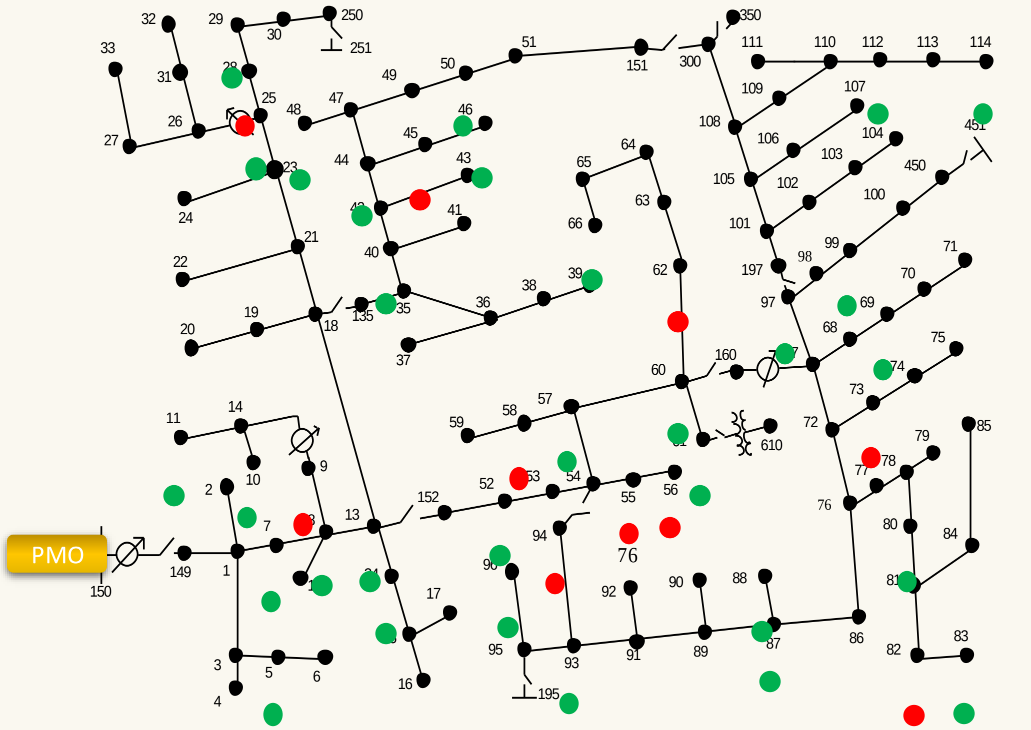
1. SMOs submit flexibility bids for $[t_{p_0}, t_{p_1}]$
2. PMO clears all SMOs for $[t_{p_0}, t_{p_1}]$



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



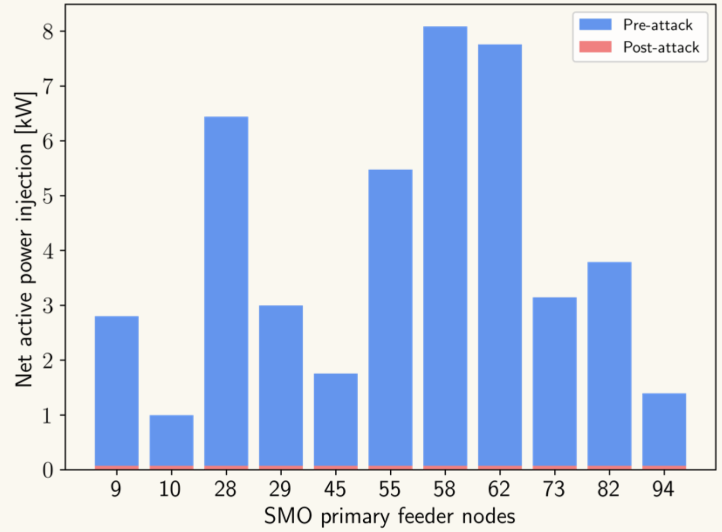


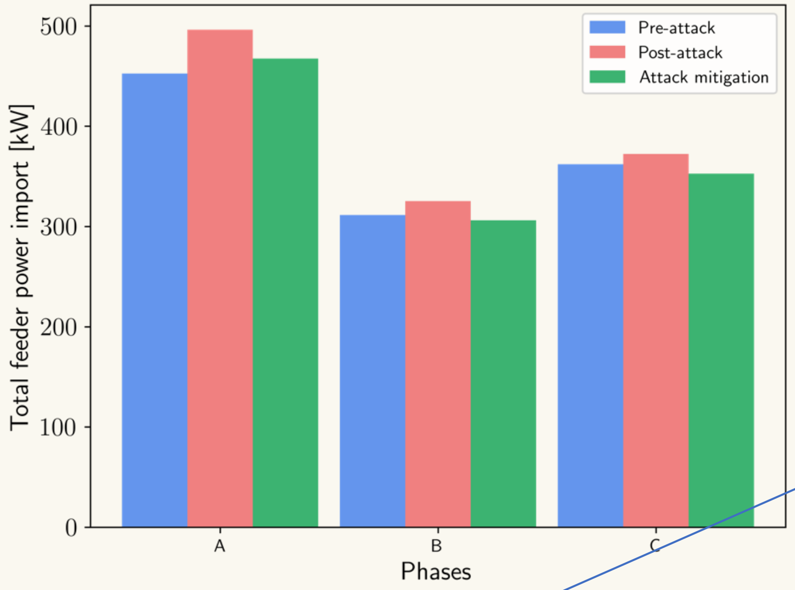
: Attacked Nodes : Trustable EUREICA-Nodes

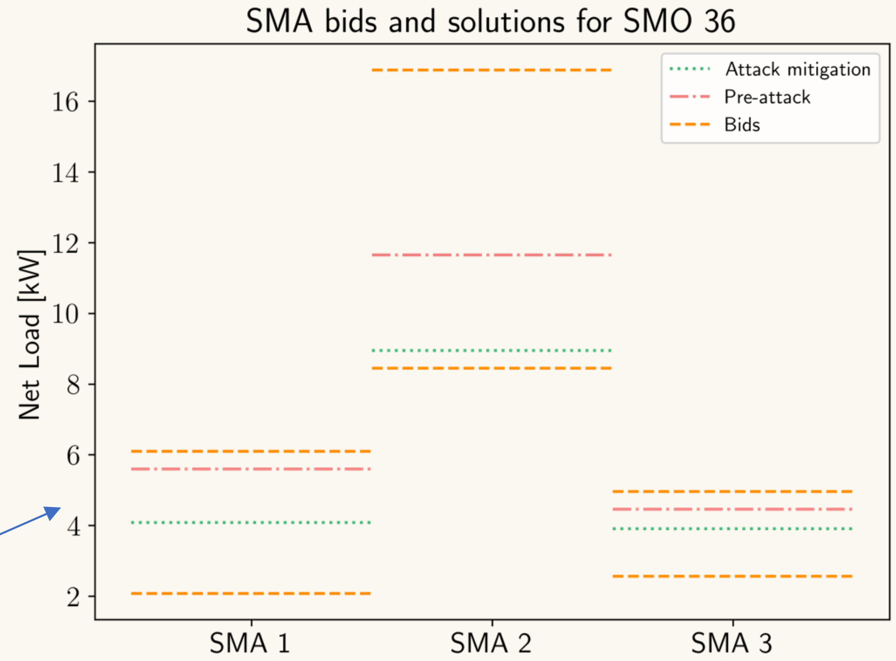
EUREICA: Efficient, Ultra-Resilient IoT-coordinated Assets

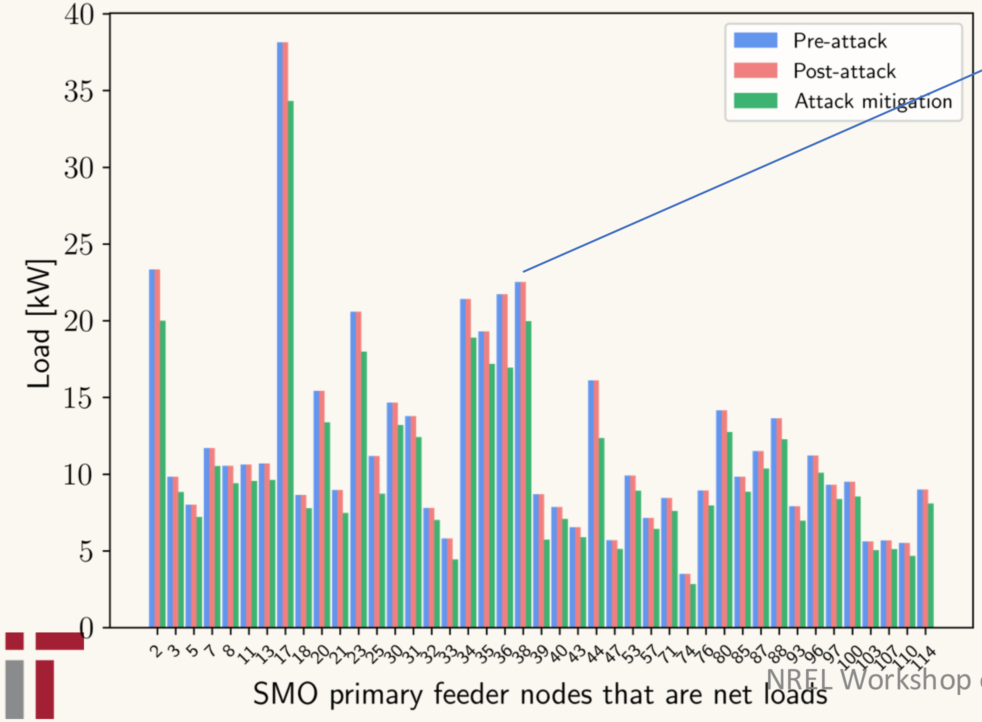
[* https://arxiv.org/abs/2406.14861](https://arxiv.org/abs/2406.14861)

Attack 1: Results*









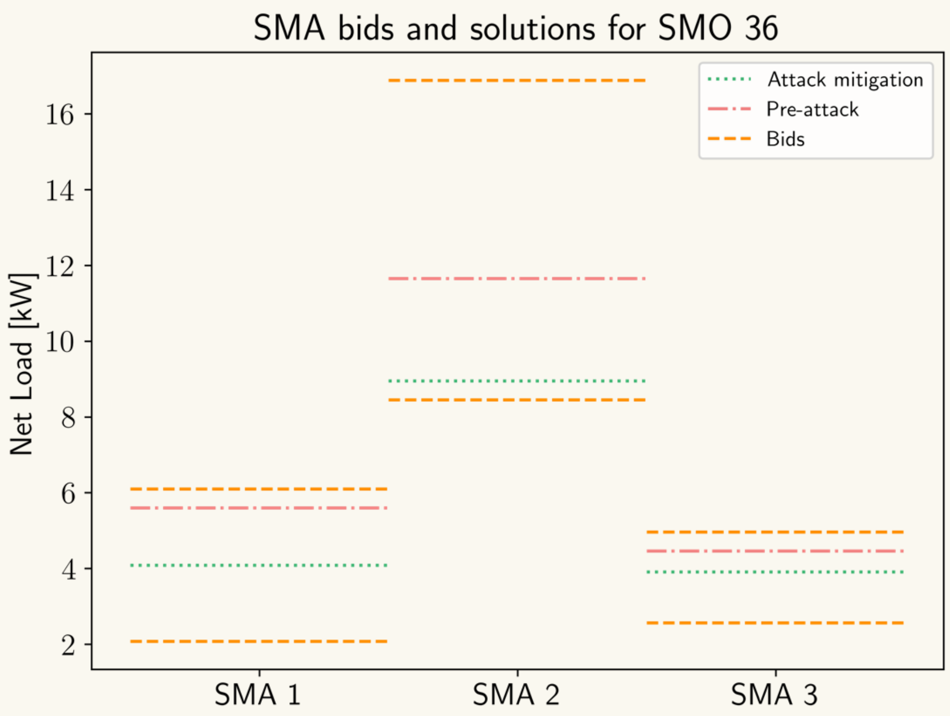
Metric	Value [kW]
Total load without attack	1167.52
Total load with attack	1190.44
Total load after attack mitigation	1123.31
Minimum SMO load curtailment	0.12
Maximum SMO load curtailment	4.77
Total import w/o attack	1125.91
Total import w/ attack	1193.87
Total import w/ attack mitigation	1126.35

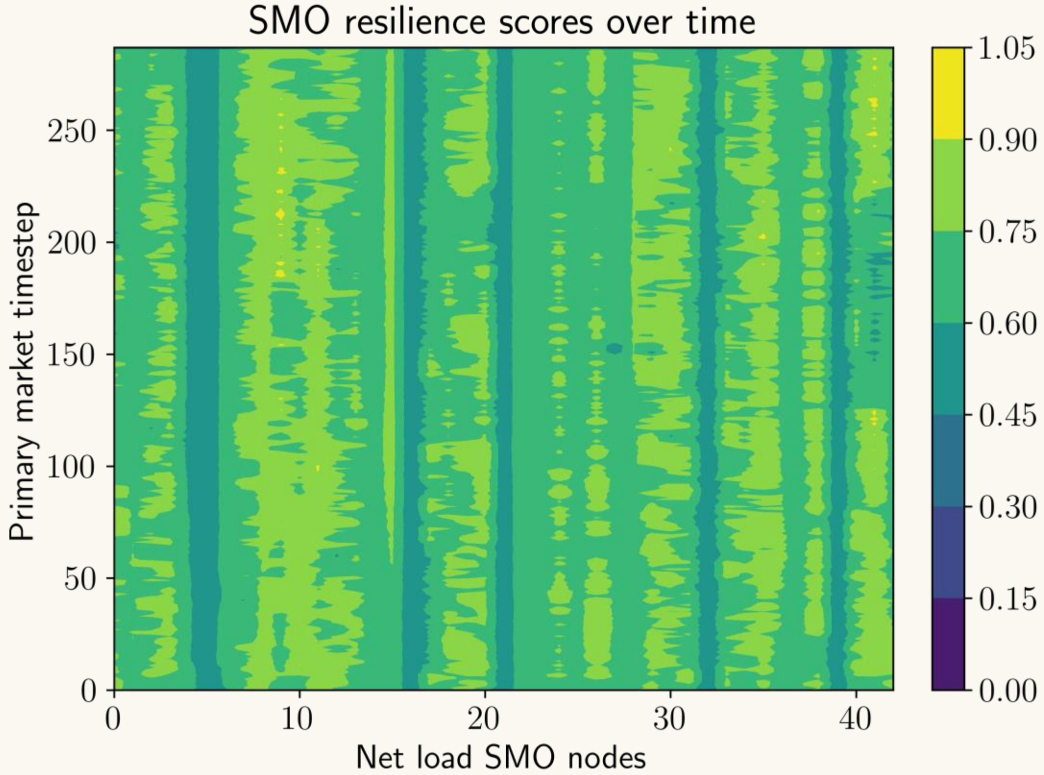
* https://arxiv.org/abs/2406.14861

SMA disaggregation and RS

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

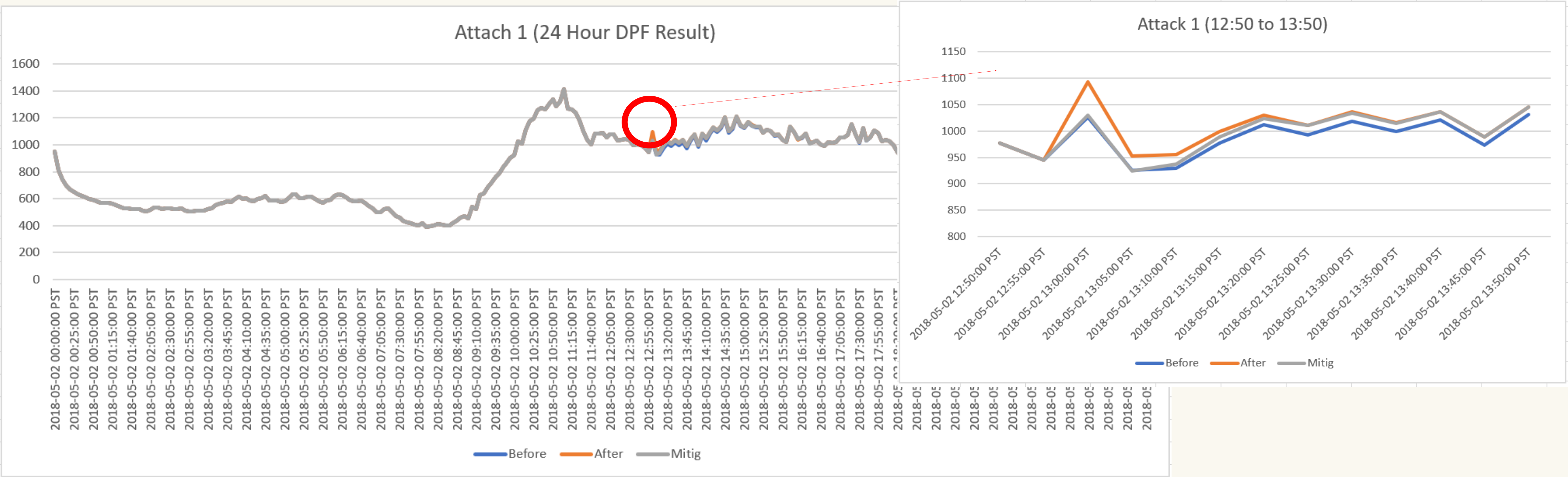
SMA	RS
SMA 1	0.947
SMA 2	0.985
SMA 3	0.493





Attack 1: ADMS Verification Analysis

Power Flow (Active Power) result at Substation



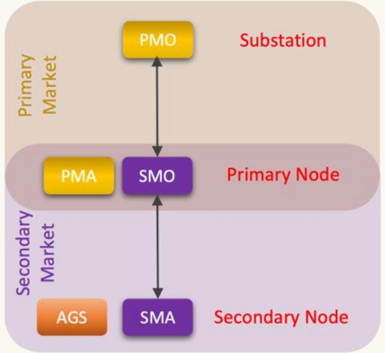
1. Without the Market mitigation

   The feeder demand jumped by 68 kW

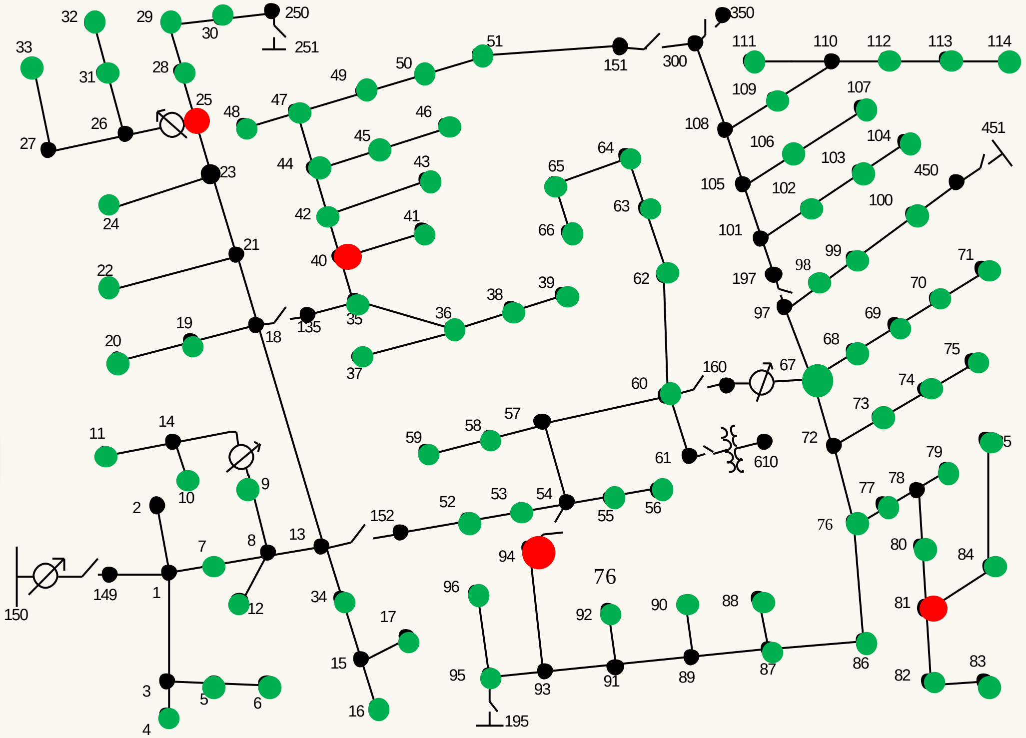
2. With Market mitigation

   Attack does not have any impact on feeder demand (only 4 kW increase)

Attack 2: Large scale attack with mitigation



PMO



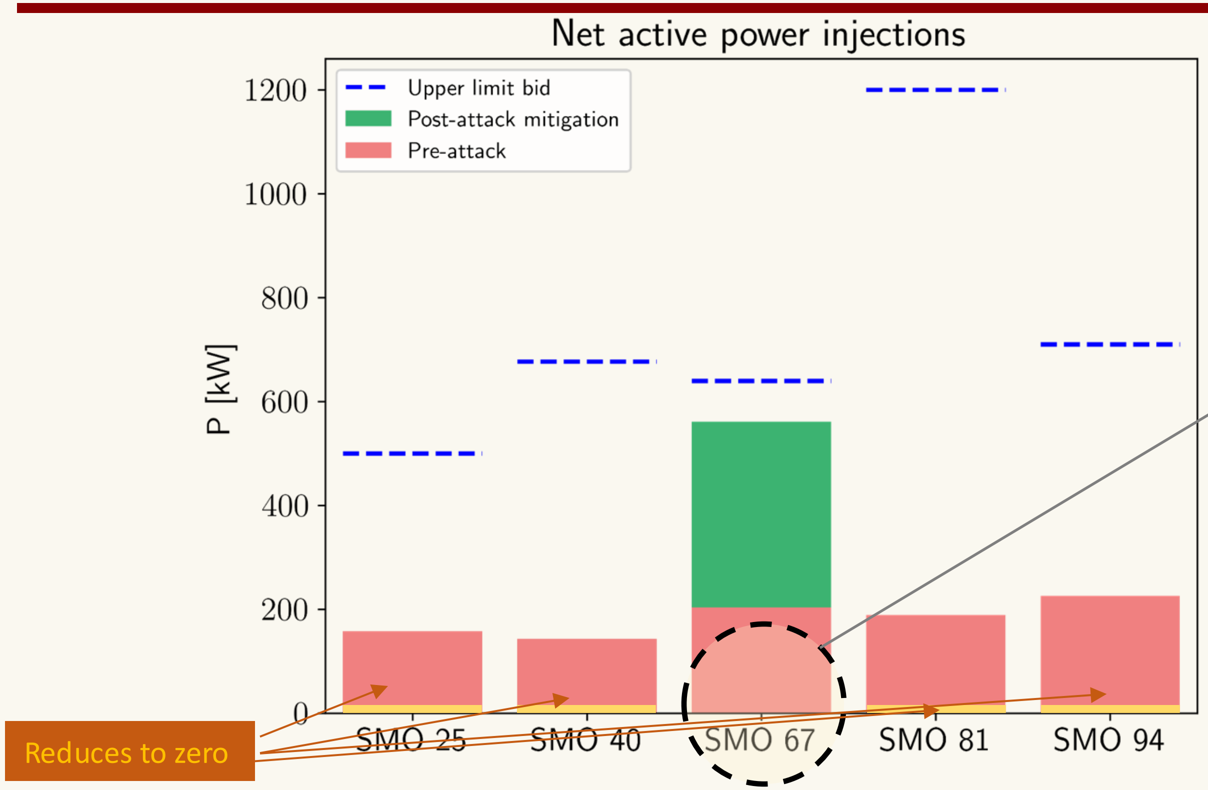
1. A total of 641 kw generation loss
2. PRM alerts other trustable PMAs/SMOs to redispatch their generation assets
3. Trustable PMAs/SMOs will curtail flexible loads to respond & mitigate attack
4. SMOs redispatch SMAs who provide correct setpoints
5. Total import from the main grid stays at the same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

82 flexible load nodes respond

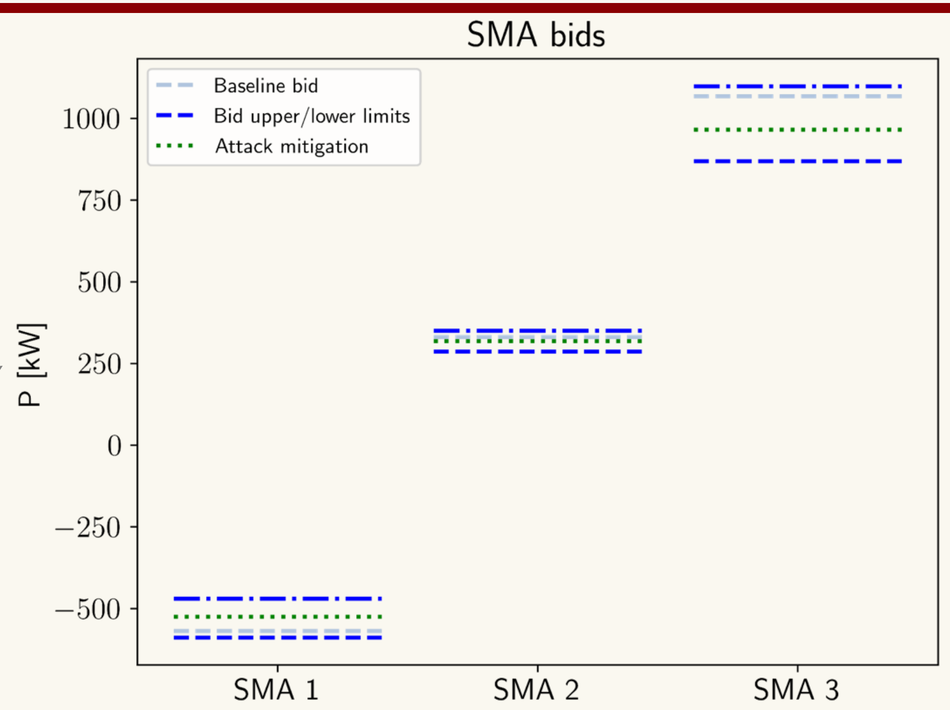
: Attacked Nodes

: Trustable EUREICA-Nodes

Large scale attack 2: Mitigation



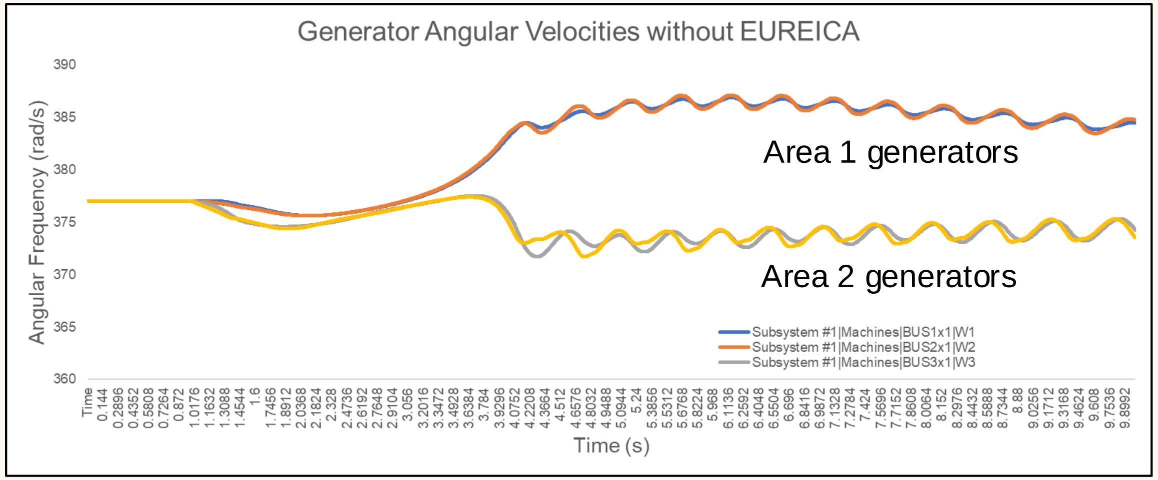
Changes in dispatch at key primary nodes

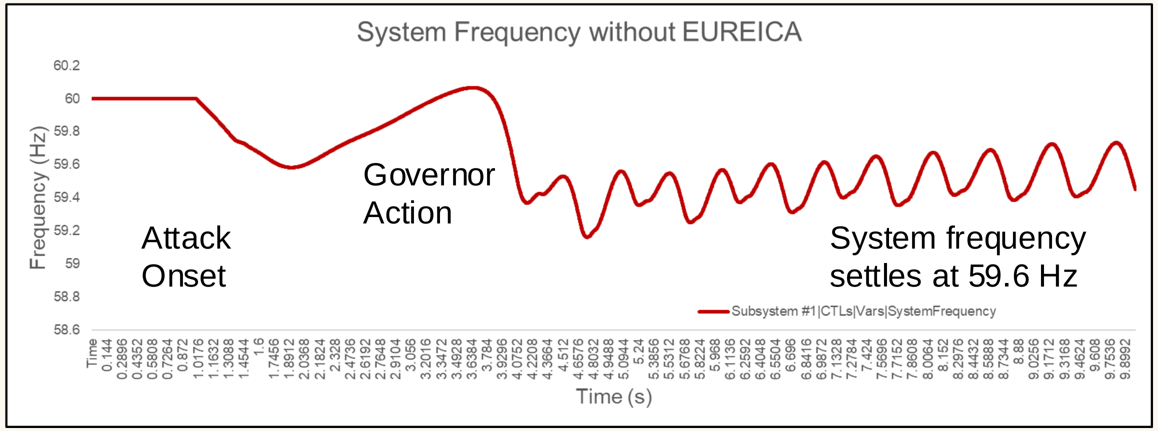


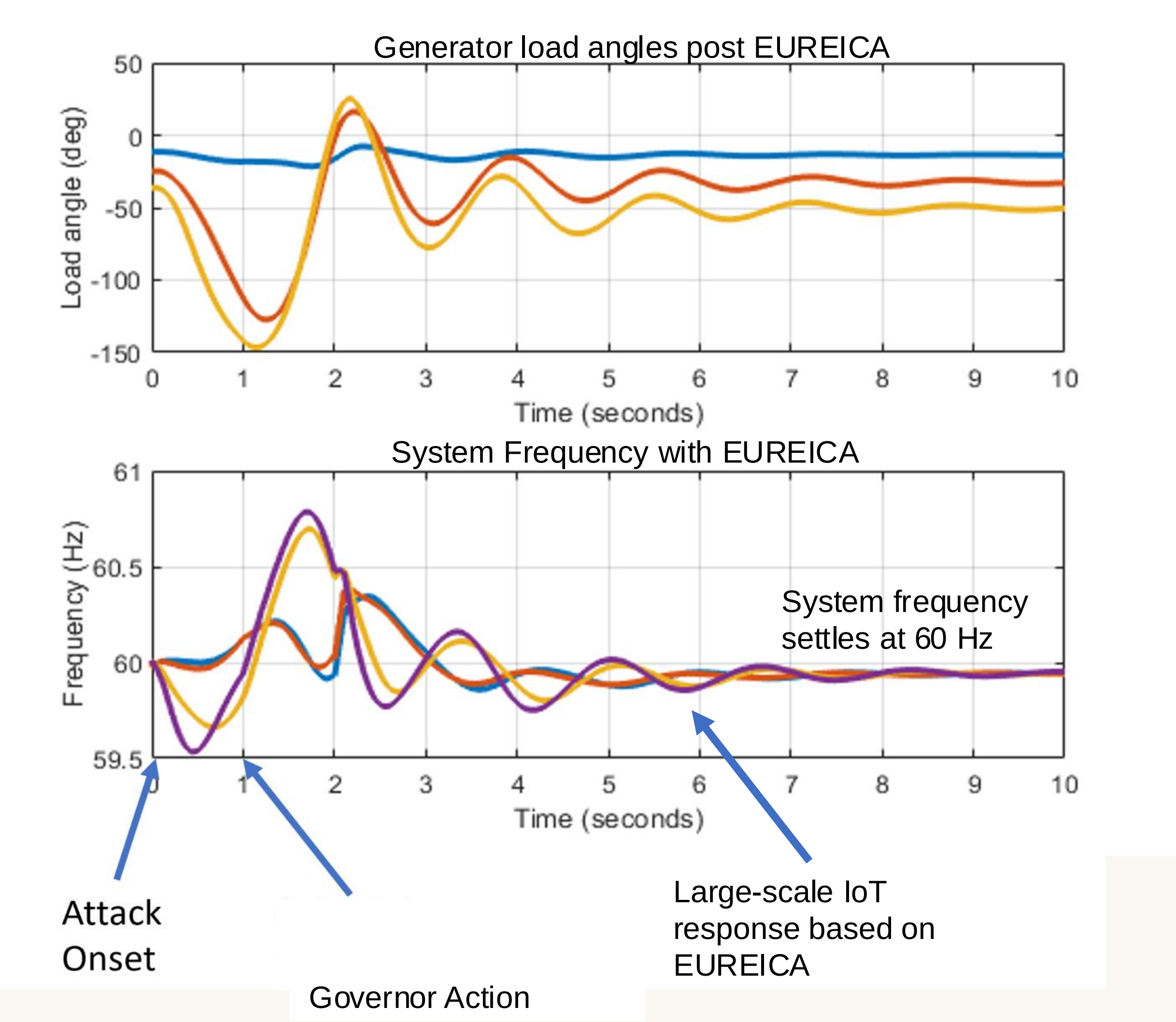
Disaggregation of new primary node setpoints across secondary feeders

- 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





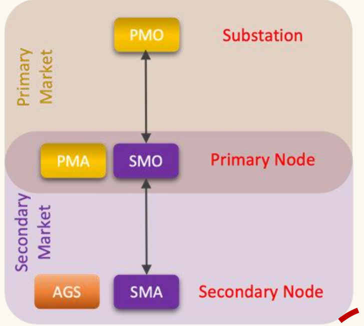


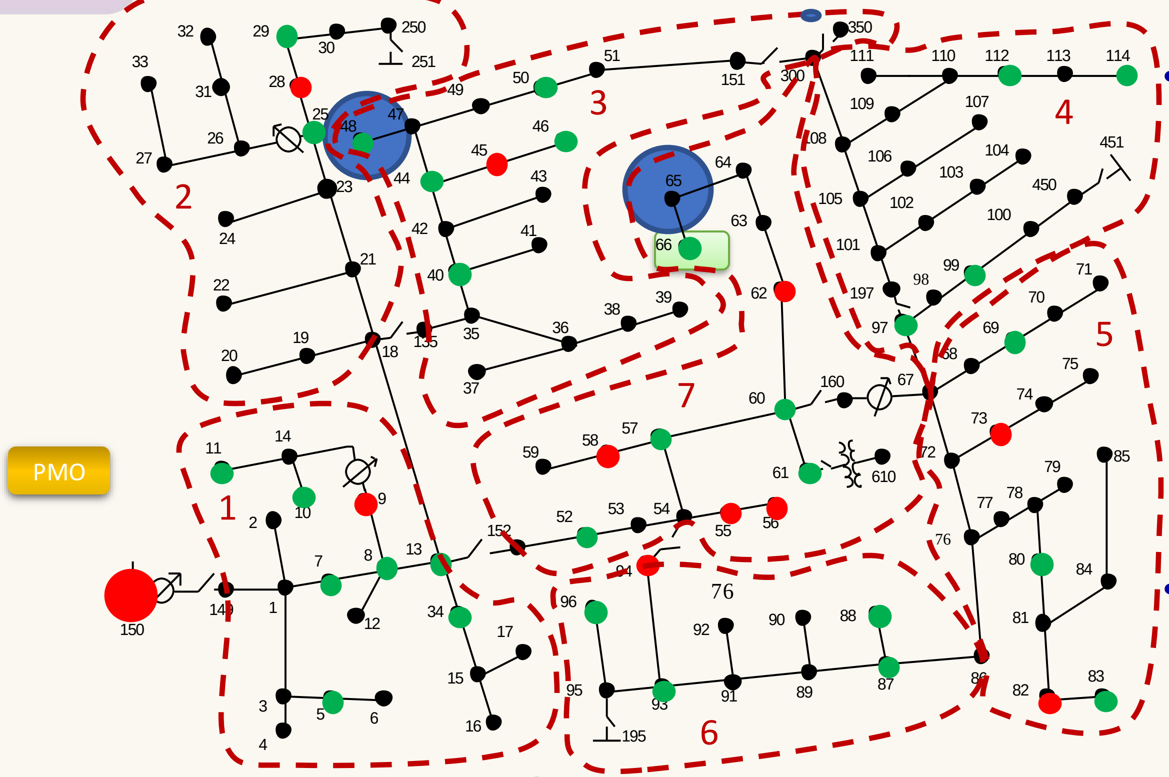
RESPONSE WITHOUT EUREICA

RESPONSE WITH EUREICA

EUREICA: Efficient Ultra-efficient IoT-coordinated Assets

Overall timeline of Attack 3.0





: Attacked Nodes

: Trustable EUREICA-Nodes

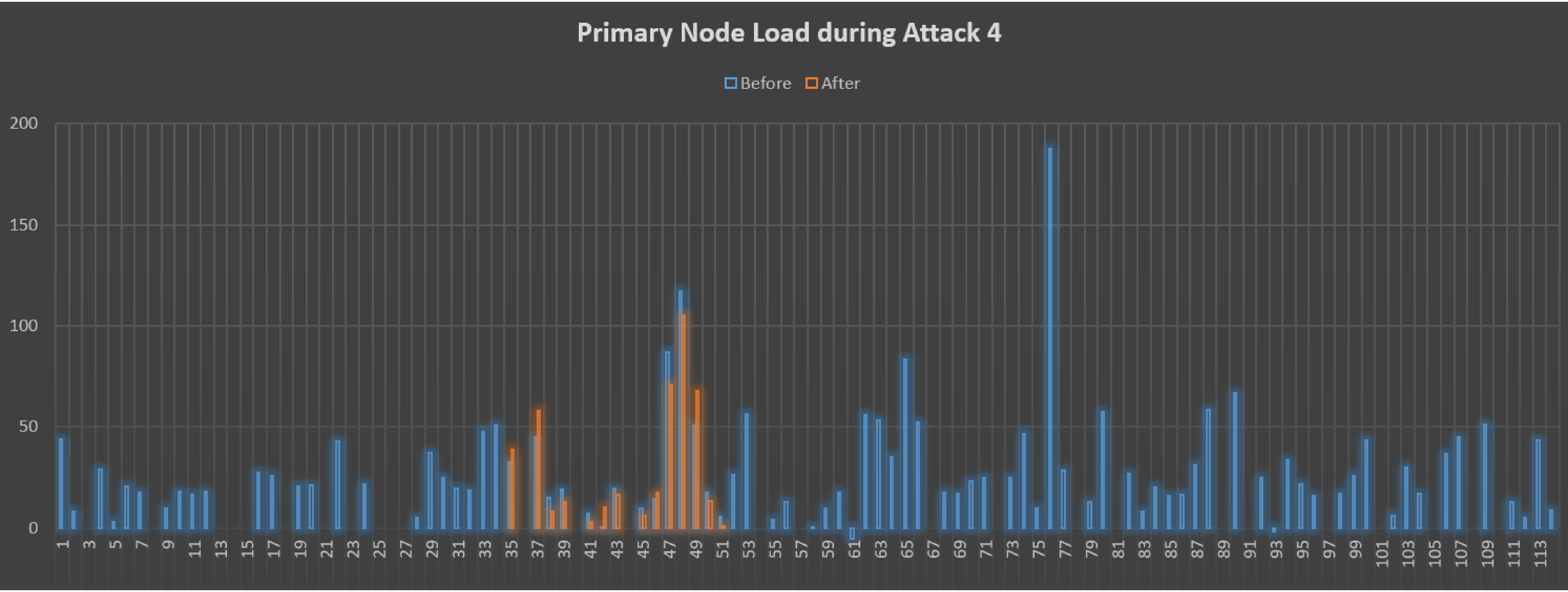
- Fault occurs at Node 150
- SW 150 to 149 is disconnected
- DG at node 48 is connected through reconfiguration

- 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

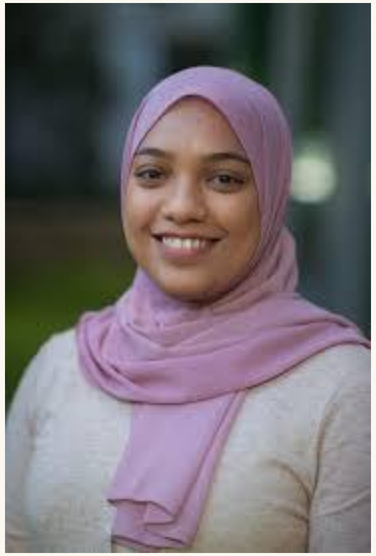
1. Distributed IoT-coordinated Assets can be ascertained
2. They provide opportunities for enhancing resilience
3. Local resilience through trustable DERs

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: Anjan Bose, Anurag Srivastava
- National Renewable Energy Laboratory: Venkatesh Venkataraman
- Pacific Northwest National Laboratory: Laurentiu Maronvici, Karan Kalsi
- Princeton: Vince Poor, Prateek Mittal

Thank you!

Questions?