Supporting Information for

Resilience of the Electric Grid through Trustable IoT-Coordinated Assets

Vineet J. Nair, Priyank Srivastava, Venkatesh Venkataramanan, Partha S. Sarker, Anurag Srivastava, Laurentiu D. Marinovici, Jun Zha, Christopher Irwin, Prateek Mittal, John Williams, Jayant Kumar, H. Vincent Poor, and Anuradha M. Annaswamy

H. Vincent Poor, Vineet J. Nair.
E-mail: poor@princeton.edu, jvineet9@mit.edu

This PDF file includes:

Supporting text
Figs. S1 to S43
Tables S1 to S4
SI References

Supporting Information Text

Nomenclature

ACOPF Alternating Current OPF

ADMS Advanced Distributed Management System

ADP Anomalous Data Point

AHP Analytic Hierarchy Process

AR Anomaly Ratio

ARIES Advanced Research on Integrated Energy Systems

CAR Cumulative Anomaly Ratio

CI Current Injection

CMO Consumer Market Operator

CS Commitment Score

DCVS Device and Communication Vulnerabilities present at the Secondary

DER Distributed Energy Resources

DERIM DER Integration Middleware

DG Distributed Generator

DoS Denial of Service

DOTS Distribution Operations Training Simulator

DPVs Distributed Photovoltaics

DRTS Digital Real-Time Simulation

DSO Distribution System Operator

DSR Distribution System Resiliency

EUREICA Efficient, Ultra-REsilient, IoT-Coordinated Assets

EV Electric Vehicle

FL Federated Learning

GE General Electric

HELICS Hierarchical Engine for Large-scale Infrastructure Co-simulation

HIL Hardware-in-the-Loop

HVAC Heating, Ventilation, and Air Conditioning

ICAs IoT-Coordinated Assets

ICS Industrial Control Systems

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

LEM Local Electricity Market

LMP Locational Marginal Price

MadIoT Manipulation of Demand via IoT

MCDM Multiple-Criteria Decision-Making

NREL National Renewable Energy Lab

NVD National Vulnerability Database

OPF Optimal Power Flow

OT Operational Technology

PAC Proximal Atomic Coordination

PCC Point of Common Coupling

PM Primary Market

PMA Primary Market Agent

PMO Primary Market Operator

PNNL Pacific Northwest National Lab

PNR Primary Node Resiliency

PRM Primary Resilience Manager

RS Resilience Score

RTDS Real-Time Digital Simulator

SA Situational Awareness

SM Secondary Market

SMA Secondary Market Agent

SMO Secondary Market Operator

SOCP Second-Order Conic Program

SRM Secondary Resilience Manager

STNR Secondary Transformer Node Resiliency

TS Trustability Score

WH Water Heater

Common Vulnerability Scoring System CVSS

1. IEEE 123-NODE DISTRIBUTION NETWORK

Fig. S1 shows the IEEE 123-node test feeder (1), which is the distribution network model used to simulate and validate all our attack scenarios.

2. EXAMPLE INSTANCE OF LEM

Here, we sketch out a possible (hypothetical) instantiation of our LEM for the city of Boston, MA, which is located in the New England (NE) region in the US. Fig. S2 shows the IEEE 39-bus transmission system (2) which is a synthetic representation of the entire NE region, with a peak load of 6254 MW and a total of around 7 million homes. This corresponds to $\approx$ 162 MW and 180,000 homes per bus. Given that the IEEE 123-node distribution feeder has a peak load of roughly 3.6 MW, we can estimate that there will be 44 such primary feeders per transmission bus and 4100 homes per feeder. Thus, the city of Boston with a total of 300,000 homes (3), will be served by 73 primary feeders across 2 transmission buses.

Fig. S3 shows a breakdown of different entities to form a hierarchical LEM for Boston. Note that the main market operators and agents that are relevant for this work are marked in green.

3. DETAILS OF THE LOCAL ELECTRICITY MARKET

Fig. S4 shows the inputs and outputs for different levels of the hierarchical LEM. For both the SM and the PM, the inputs consist of the baseline power injections and flexibility bids, while the outputs are the market schedules (setpoints for power injections) and their associated flexibility ranges, along with the corresponding electricity prices of tariffs.

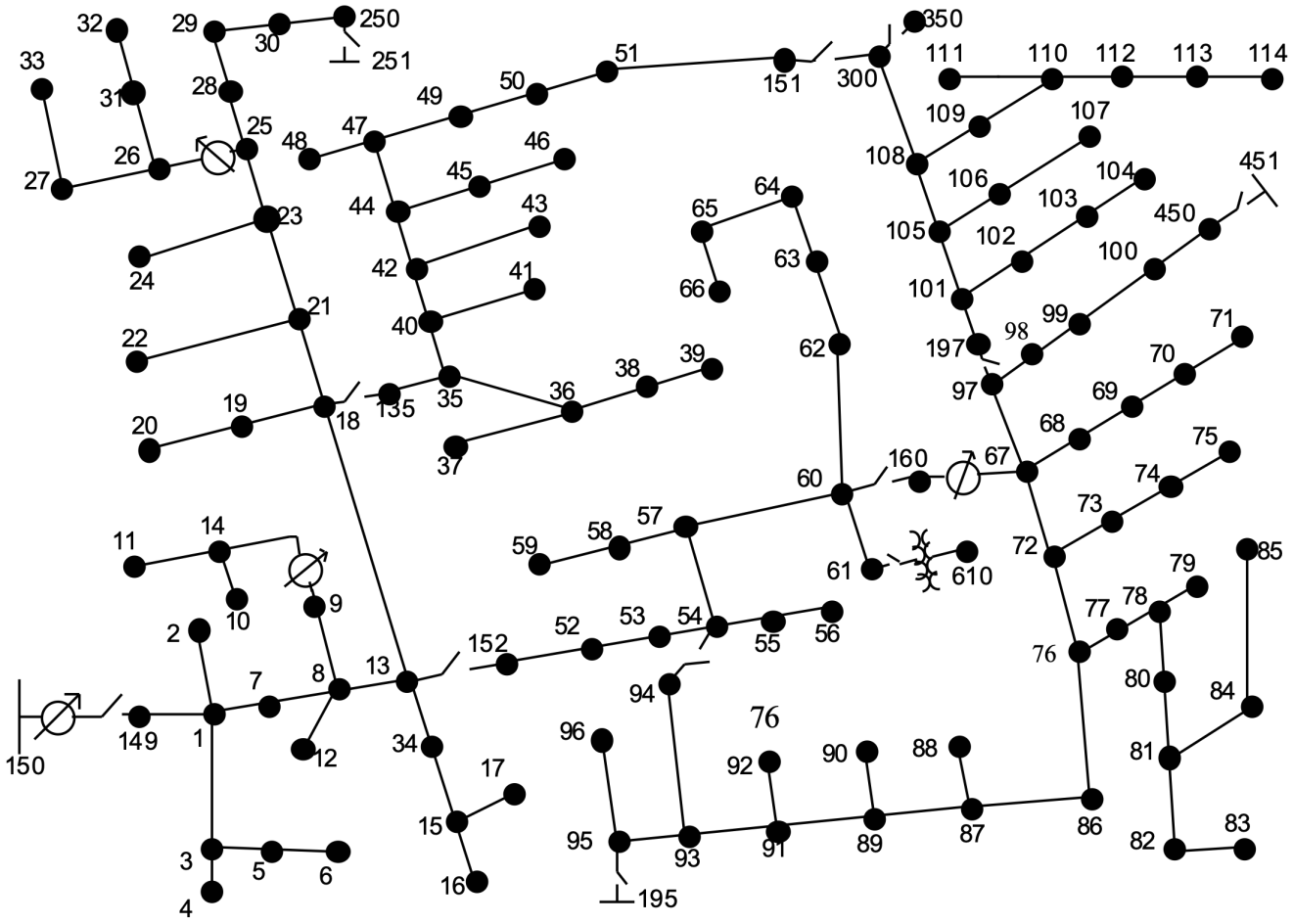


Fig. S1. IEEE 123-node test feeder network.

A. Objective functions for optimization in the Secondary Market. The four objective functions considered in the SM clearing are defined as:

O1. Maximization of aggregate resilience, f_i^1, given by the following, where RS_j^i denotes the resilience score of SMA j under SMO i

$$f_i^1 = -\sum_{j=1}^{n} RS_j^i((P_j^i - P_j^{i0})^2 + (Q_j^i - Q_j^{i0})^2)$$

O2. Minimization of net cost, f_i^2 to the SMO for running the SM

$$f_i^2 = \sum_{j=1}^{n} \mu_j^{iP} P_j^i + \mu_j^{iQ} Q_j^i$$

O3. Maximization of total flexibility, f_i^3 that the SMO can extract from all its SMAs

$$f_i^3 = -\sum_{j=1}^{n} (\delta P_j^i + \delta Q_j^i)$$

O4. Minimization of disutility of the SMAs, f_i^4 arising from flexibility provision

$$f_i^4 = \sum_{j=1}^{n} \beta_j^{iP} (P_j^i - P_j^{i0})^2 + \beta_j^{iQ} (Q_j^i - Q_j^{i0})^2.$$

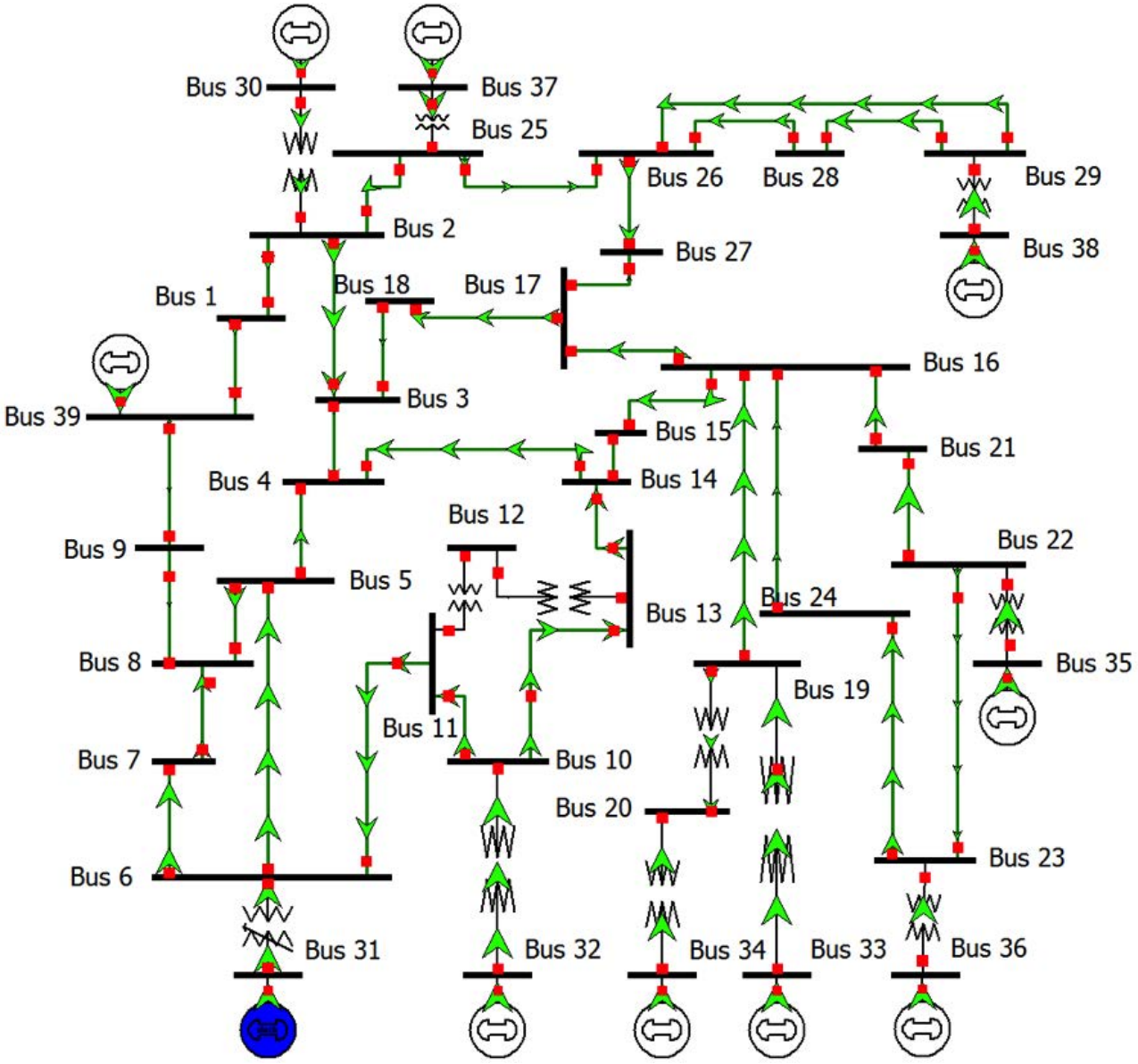


Fig. S2. IEEE 39-bus transmission system.

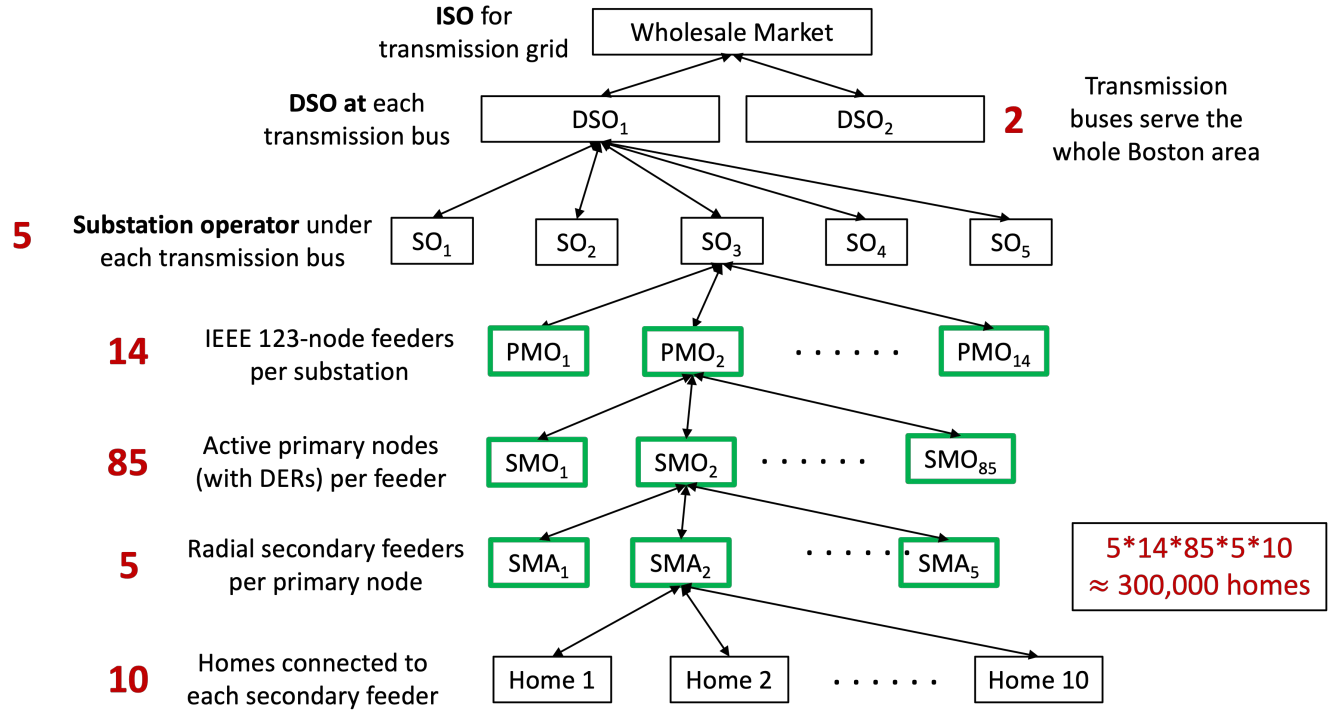


Fig. S3. Example of hypothetical LEM for the city of Boston, MA.

B. Three-phase SM optimization problem.

$$\min \sum_{j\in\mathcal{N}_{J,i}} \{f^i_{j,1}, f^i_{j,2}, f^i_{j,3}, f^i_{j,4}\} \tag{1a}$$

$$f^i_{1,j} \succ f^i_{2,j} \succ f^i_{3,j} \succ f^i_{4,j}, \quad \Phi = \{a, b, c\} \tag{1b}$$

$$f^i_{j,1} = -C^i_j \left(\sum_{\phi\in\Phi} (P^{i,\phi}_j - P^{i0,\phi}_j)^2 + (Q^{i,\phi}_j - Q^{i0,\phi}_j)^2 \right)$$

$$f^i_{j,2} = \sum_{\phi\in\Phi} \mu^{iP,\phi}_j P^{i,\phi}_j + \mu^{iQ,\phi}_j Q^{i,\phi}_j$$

$$f^i_{j,3} = -\sum_{\phi\in\Phi} (\delta P^{i,\phi}_j + \delta Q^{i,\phi}_j)$$

$$f^i_{j,4} = \beta^{iP}_j \sum_{\phi\in\Phi} \left(P^i_j - P^{i0}_j\right)^2 + \beta^{iQ}_j \sum_{\phi\in\Phi} \left(Q^i_j - Q^{i0}_j\right)^2$$

subject to:

$$P^{i,\phi}_j - \delta P^{i,\phi}_j \geq \underline{P}^{i,\phi}_j \; Q^{i,\phi}_j - \delta Q^{i,\phi}_j \geq \underline{Q}^{i,\phi}_j \tag{1c}$$

$$P^{i,\phi}_j + \delta P^{i,\phi}_j \leq \overline{P}^{i,\phi}_j, \; Q^{i,\phi}_j + \delta Q^{i,\phi}_j \leq \overline{Q}^{i,\phi}_j \tag{1d}$$

$$\delta P^{i,\phi}_j, \; \delta Q^{i,\phi}_j \geq 0, \; 0 \leq \mu^{iP}_j \leq \overline{\mu}^{iP}, 0 \leq \mu^{iP}_j \leq \overline{\mu}^{iQ} \tag{1e}$$

$$\sum_{t_s}^{t_s+\Delta t_p} \sum_{j\in\mathcal{N}_{J,i}} \sum_{\phi\in\Phi} \left(\mu^{iP,\phi}_j(t) P^{i,\phi}_j(t) + \mu^{iQ,\phi}_j(t) Q^{i,\phi}_j(t)\right) \Delta t_s$$

$$\leq \sum_{\phi\in\Phi} \left(\mu^{P^*,\phi}_i(\hat{t}_p) P^{\phi^*}_i(\hat{t}_p) + \mu^{Q^*,\phi}_i(\hat{t}_p) Q^{\phi^*}_i(\hat{t}_p)\right) \Delta t_p \tag{1f}$$

$$\sum_{j\in\mathcal{N}_{J,i}} P^{i,\phi}_j(t_s) = P^{\phi^*}_i(\hat{t}_p), \quad \sum_{j\in\mathcal{N}_{J,i}} Q^{i,\phi}_j(t_s) = Q^{\phi^*}_i(\hat{t}_p) \tag{1g}$$

C. Bidding in the Primary Market. The bid submitted by each SMO $j \in \mathcal{N}$ into the PM $\mathcal{B}^P_i$ defined as:

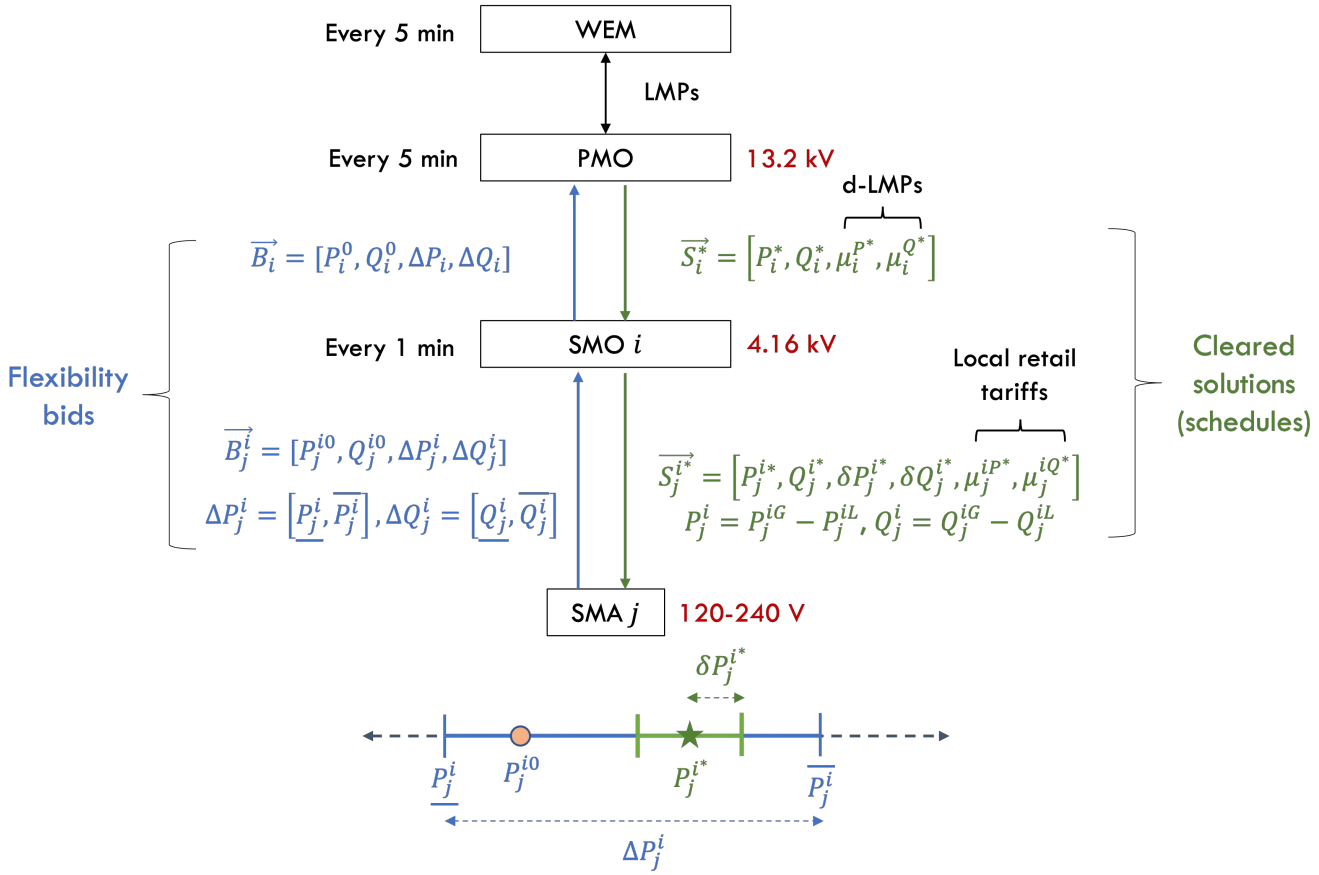


Fig. S4. Overall inputs and outputs in the LEM. Image Credit: Adapted with permission from (4).

$$\mathcal{B}_i^S = \{P_i^0, Q_i^0, \underline{P}_i, \underline{Q}_i, \overline{P}_i, \overline{Q}_i, \alpha_i^P, \alpha_i^Q, \beta_i^P, \beta_i^Q\}. \quad [2]$$

$$P_i^0(t_p) = \sum_{j\in\mathcal{N}_i} P_j^{i*}(t_p),\ Q_i^0(t_p) = \sum_{j\in\mathcal{N}_i} Q_j^{i*}(t_p) \quad [3]$$
$$\underline{P}_i = \sum_{j\in\mathcal{N}_i} P_j^i - \delta P_j^{i*}, \overline{P}_i = \sum_{j\in\mathcal{N}_i} P_j^{i*} + \delta P_j^{i*}$$
$$\underline{Q}_i = \sum_{j\in\mathcal{N}_i} Q_j^{i*} - \delta Q_j^{i*}, \overline{Q}_i = \sum_{j\in\mathcal{N}_i} Q_j^{i*} + \delta Q_j^{i*}$$

In the above, (i) P_i^0, Q_i^0 denote the baseline active and reactive power injection bids of the SMOs, (ii) $(\underline{P}_i, \underline{Q}_i)$ and $(\overline{P}_i, \overline{Q}_i)$ denote the downward and upward flexibilities (around their nominal values) in active and reactive power, respectively, (iii) α_i^P, α_i^Q are the local net generation costs, and (iv) β_i^P, β_i^Q are the flexibility disutility parameters of SMO i for P and Q, respectively. The SMO computes (iii) and (iv) as weighted averages of all their SMA retail tariffs, and SMA disutility parameters, respectively, as follows:

$$\alpha_i^P = \frac{\sum_{j\in\mathcal{N}_i} \mu_j^{iP*} |P_j^{i*}|}{\sum_{j\in\mathcal{N}_i} |P_j^{i*}|}, \beta_i^P = \frac{\sum_{j\in\mathcal{N}_i} \beta_j^{iP*} |P_j^{i*}|}{\sum_{j\in\mathcal{N}_i} |P_j^{i*}|}$$

D. Objective functions for optimization in the Primary Market. We define the following functions

$$f^P(\mathbf{y}^P) = \sum_{i\in\mathcal{N}} f_i^P(\mathbf{y}_i^P) = \sum_{i\in\mathcal{N}} \Big[f_i^{\text{Load-Disutil}}(\mathbf{y}_i^P) + f_i^{\text{Gen-Cost}}(\mathbf{y}_i^P) \Big] + \xi \Big[\sum_{(ki)\in\mathcal{E}} f_{ki}^{\text{Loss}}(\mathbf{y}_i^P) \Big] \quad [4]$$

$$f_i^{\text{Load-Disutil}}(\mathbf{y}_i^P) = \beta_i^P (P_i^L - P_i^{L0})^2 + \beta_i^Q (Q_i^L - Q_i^{L0})^2 \quad [5]$$

$$f_i^{\text{Gen-Cost}}(\mathbf{y}_i^P) = \begin{cases} \alpha_i^P (P_i^G)^2 + \alpha_i^Q (Q_i^G)^2, \\ \lambda_i^P P_i^G + \lambda_i^Q Q_i^G, \text{if } i \qquad \text{is PCC} \end{cases} \quad [6]$$

$$f_{ki}^{\text{Loss}}(\mathbf{y}_i^P) = R_{ki} |I_{ki}|^2 \quad [7]$$

The objective function used in Eq. (4) used is a weighted linear combination of (i) maximizing social welfare in Eq. (5), (ii) minimizing total generation costs in Eq. (6) and (iii) minimizing electrical line losses in Eq. (7). The total cost includes paying the locational marginal price (LMP) λ for importing power from the transmission grid at the point of common coupling (PCC), as well as the payments to local generator PMAs that provide net positive injections into the PM. We divide by suitable base values to convert all quantities to per unit (between 0 and 1 p.u.). Thus, it is reasonable to combine all the terms into a single objective function using a simple weighted sum. The hyperparameter ξ controls the tradeoff between penalizing line losses versus optimizing for other objectives. The coefficients α_i, β_i, are communicated by each PMA i as part of their bids, while ξ is a global hyperparameter common to all PMAs, and determined by the PMO. Here, R denotes the network resistance matrix and $\mathcal{E}$ denotes the set of all edges in the network.

E. Computation of commitment scores. We describe here the details of computing the commitment reliability score, mentioned in Section A.3. From the SM clearing, the SMAs j are directed by their SMO i to keep their net injections within the intervals $[P_j^{i*} - \delta P_j^{i*}, P_j^{i*} + \delta P_j^{i*}]$. We first compute the deviations (if any) in their actual responses $\hat{P}_j^i$ from this range, where $[\![\cdot]\!]$ denotes the indicator function:

$$e_j^{iP}(t_s) = [\![\hat{P}_j^i > \overline{P}_j^{i*}]\!](\hat{P}_j^i - \overline{P}_j^{i*}) + [\![\hat{P}_j^i < \underline{P}_j^{i*}]\!](\underline{P}_j^{i*} - \hat{P}_j^i) + [\![\underline{P}_j^{i*} \le \hat{P}_j^i \le \overline{P}_j^{i*}]\!] \max(\hat{P}_j^i - \overline{P}_j^{i*}, \underline{P}_j^{i*} - \hat{P}_j^i) \quad [8]$$

We then obtain relative deviations by comparing these with the magnitudes of their corresponding baseline setpoints:

$$\overline{e_j^{iP}}(t_s) = \frac{e_j^{iP}(t_s)}{|P_j^{i*}(t_s)|}, \quad \overline{e_j^{iQ}}(t_s) = \frac{e_j^{iQ}(t_s)}{|Q_j^{i*}(t_s)|} \quad [9]$$

These are then normalized to unit vectors to compare the deviations among all SMAs overseen by the SMO. This allows the SMO to assess their relative performance across all its SMAs.

$$\widetilde{\mathbf{e^{iP}}}(t_s) = \frac{\overline{\mathbf{e^{iP}}}(t_s)}{\|\overline{\mathbf{e^{iP}}}(t_s)\|}, \ \widetilde{\mathbf{e^{iQ}}}(t_s) = \frac{\overline{\mathbf{e^{iQ}}}(t_s)}{\|\overline{\mathbf{e^{iQ}}}(t_s)\|} \quad [10]$$

The scores are then updated, with the score being increased when the SMAs follow their contracts and decreased otherwise:

$$C_j^i(t_s) = \begin{cases} 1 & \text{if } t_s = 0 \\ C_j^i(t_s - 1) - \frac{\widetilde{e_j^{iP}}(t_s) + \widetilde{e_j^{iQ}}(t_s)}{2} & \text{if } t_s > 0 \end{cases} \quad [11]$$

Finally, we perform min-max normalization across all the SMAs' scores to ensure that $0 \le C_j \le 1 \ \forall$ SMAs j.

$$\overline{C}_j^i = \frac{C_j^i - \max_j C_j^i}{\max_j C_j^i - \min_j C_j^i}$$

4. TRUSTABILITY SCORES AND RESILIENCY METRICS

A. Computation of IoT trustability scores. The IoT trustability score (TS) is computed utilizing the federated self-learning concept (5). Anomalies in IoT data are the key factor in the formulation of the IoT TS. Another contributing factor is the IoT device's market commitment history. More details of the features are shown in Table S1.

To detect anomalies, we learn the IoT data's expected behavior and prediction for the short time steps. Predicted data is compared with measured data for anomaly detection. For prediction, we are using an autoencoder neural network for federated unsupervised learning. There will be one autoencoder model for each IoT device to train on its physical data and one more autoencoder model to train only on IoT network packet data. For each type of data, there is a tolerance value T_{err} for the

Table S1. Features considered for each type of data. Image Credit: Adapted with permission from (5).

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

relative error (RE). If any data point (DP) crosses T_{err}, then that is flagged as an anomalous data point (ADP). So, for any reporting time period Δt, non-anomaly ratio (NAR) is calculated using,

$$NAR = 1 - \frac{\text{Total ADP number over } \Delta t}{\text{Total DP number over } \Delta t} \quad [12]$$

Next, the cumulative non-anomaly ratio ($CNAR$) is computed, where T is the fixed total time period and is always divisible by Δt.

$$CNAR_t = \sum_{j=1}^{\frac{T}{\Delta t}} \frac{T}{j\Delta t} NAR_{t-j\Delta t} \quad [13]$$

IoT Trustability Score (TS) for time t and building/house i is calculated:

$$TS_{t,i} = w_t \times NAR_t + w_{t-} \times \frac{CNAR_t}{CNAR_{max}} \quad [14]$$

where

$$(I)\ w_t \geq w_{t-} \qquad (II)\ w_t + w_{t-} = 1 \quad [15]$$

Here, $CNAR_{max}$ is calculated using Eq. (13) with the maximum NAR being $NAR = 1$ for the whole time period T. Finally, to get the overall TS_t of any observation node with IoTs at time t, we average the $TS_{t,i}$ of all the clients i of that observation node to calculate TS_t:

$$TS = \frac{\sum_{i=1}^{M} TS_{t,i}}{M} \quad [16]$$

where M is the total number of clients or buildings/houses at that observation node.

B. Secondary Transformer and Primary Node Resiliency Metric (STNR and PNR). Secondary transformer node resiliency (STNR) is computed using multiple resiliency factors and TS.

$$STNR_j = \prod_{i=1}^{n_c} F_i^{W_i} \quad [17]$$

where n_c is the total number of factors for the category of the secondary level node, F_i is the value for each factor, and W_i is the normalized weight for each factor. These factors f influencing resiliency are determined and assigned weights to aggregate into the PNR score. Factors that can be determined directly from the secondary level configuration are described in Fig. S5. All the device and communication vulnerabilities present at the secondary (DCVS) level of a primary node are identified using the national vulnerability database (NVD) (6). Then DCVS factor is calculated as,

$$DCVS = \frac{1}{\sum_{i=1}^{N_s} CVSS_i} \quad [18]$$

where N_s is the number of total vulnerabilities present at the secondary level. Here, the common vulnerability scoring system (CVSS) is one of several methods to measure the impact of vulnerabilities in devices known as Common Vulnerabilities and Exposures (CVE). It is an open set of standards used to assess the vulnerability of software and assign severity along a scale of 0-10. The National Institute of Standards and Technology (NIST) analyzes all identified vulnerabilities and enlists these in the NVD. In case of the absence of any vulnerability, DCVS will be equal to 1.

Weight assignment and aggregation are managed by fuzzy multiple-criteria decision-making (MCDM), specifically the fuzzy analytic hierarchy process (Fuzzy AHP). A weighted average of the STNR results in the primary node resiliency (PNR):

$$PNR_k = \frac{\sum_{j=1}^{n} (STNR_j \times W_j)}{\sum_{j=1}^{n} W_j} \quad [19]$$

where W_i is the weighted coefficient for the i^{th} secondary feeder node.

C. Distribution System Resiliency (DSR). Let $F = (f_{ij}) \in R_+^{m \times n}$ be the factors value matrix, where f_{ij} is value of factor i of primary node j. The higher the value of f_{ij}, the more the node will contribute to the resiliency metric in regard to that factor. Now, following the data envelopment analysis (DEA) method, each node p can choose a set of weights $w^p = (w_1^p, ...w_m^p)$, where, $\sum_{i=1}^{m} w_i^p = 1$. Now the relative contribution (RC) of the node p to the total contribution of all the nodes towards DSR, as measured by node p's weight selection can be evaluated as,

$$RC^p = \frac{\sum_{i=1}^{m} w_i^p f_{ip}}{\sum_{i=1}^{m} w_i^p \sum_{j=1}^{n} (f_{ij})} \quad [20]$$

Now, each node wants to maximize this ratio in Eq. (20) to have the best set of weights so that they can contribute to the maximum possible value in DSR. Using the weight vector for each node, a combination of multiplicative and additive methods are used to get the DSR.

$$DSR = \sum_{j=1}^{n} \left(\prod_{i=1}^{m} (f_{ij})^{w_i^j} \right) \quad [21]$$

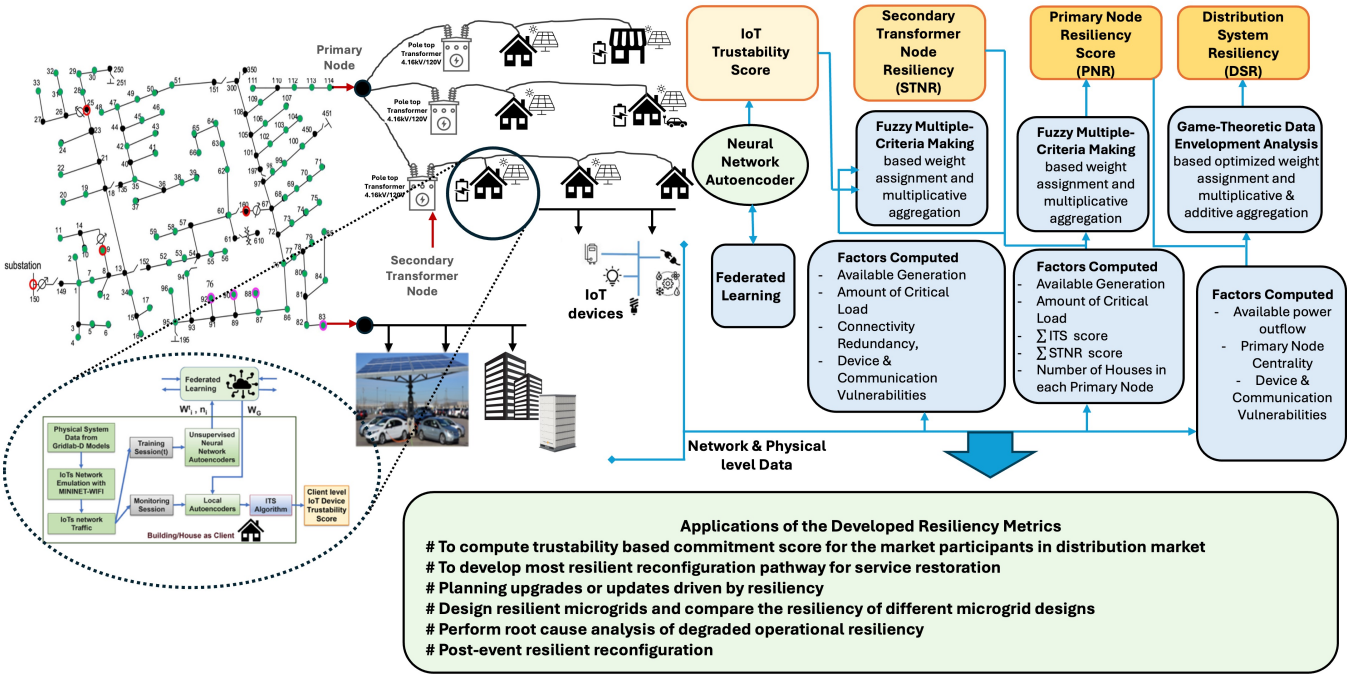


Fig. S5. Overview of the developed resilience score for the distribution system with IoTs. Image Credit: Adapted with permission from (5).

Details related to the computation of DSR are shown in Fig. S5.

5. POWER SYSTEM MODELS

A. Branch flow model. The branch flow OPF problem is formally stated as follows, where R and X denote the network resistance and reactance matrices respectively, v and I denote the nodal voltage magnitudes and branch currents respectively, and $\mathcal{E}$ denotes the set of all edges in the network. The primal decision variables here for each PMA i are $\mathbf{y}_i^{P,BF} = [P_i^G, Q_i^G, P_i^L, Q_i^L, v_i, I_{ki}] \; \forall i \in$

$\mathbf{N}$, $(ik) \in \mathcal{E}$, where $\mathcal{E}$ is the set of all network edges or branches.

$$\min_{\mathbf{y}^P} \; f^{S-W}(\mathbf{y}^P) \tag{22}$$

subject to:

$$\begin{aligned}
&v_i - v_k = \left(R_{ki}^2 + X_{ki}^2\right)|I_{ki}|^2 - 2\left(R_{ki}P_{ki} + X_{ki}Q_{ki}\right) \\
&P_i^G - P_i^L = -P_{ki} + R_{ki}|I_{ki}|^2 + \sum_{k:(i,k)\in\mathcal{E}} P_{ik} \\
&Q_i^G - Q_i^L = -Q_{ki} + X_{ki}|I_{ki}|^2 + \sum_{k:(ik)\in\mathcal{E}} Q_{ik} \\
&P_{ki}^2 + Q_{ki}^2 \le \overline{S}_{ki}^2,\; P_{ki}^2 + Q_{ki}^2 \le v_i|I_{ki}|^2,\; \underline{v}_i \le v_i \le \overline{v}_i \\
&\underline{P}_i^G \le P_i^G \le \overline{P}_i^G,\; \underline{P}_i^L \le P_i^L \le \overline{P}_i^L \\
&\underline{Q}_i^G \le Q_i^G \le \overline{Q}_i^G,\; \underline{Q}_i^L \le Q_i^L \le \overline{Q}_i^L
\end{aligned} \tag{23}$$

B. Current injection model. The decision vector for the CI model is given by $\mathbf{y}_i^{P,CI} = [P_i^\phi, Q_i^\phi, V_i^{\phi,R}, V_i^{\phi,I}, I_i^{\phi,R}, I_i^{\phi,I}, I_{ik}^{\phi,R}, I_{ik}^{\phi,I}]$, where $\phi \in \{a,b,c\}$ are the phases and $\mathcal{E}$ is the set of all network edges or branches. The primal decision variables for each SMO i obtained by solving the optimization problem consist of (i) active ($P_i^{\phi*}$) and reactive ($Q_i^{\phi*}$) power setpoints (ii) real and imaginary components of nodal voltages ($V_i^{\phi,R*}, V_i^{\phi,I*}$) and current injections ($I_i^{\phi,R*}, I_i^{\phi,I*}$). Note that these are solved for each non-zero phase $\phi \in \mathcal{P} = \{a,b,c\}$. The CI-OPF problem formulation is given by:

$$\min_x f^{obj}(x) \tag{24a}$$

$$I^R = \mathrm{Re}(\mathrm{Y}V),\; I^I = \mathrm{Im}(\mathrm{YV}) \tag{24b}$$

$$P_i^\phi = V_i^{\phi,R}I_i^{\phi,R} + V_i^{\phi,I}I_i^{\phi,I} \quad \forall i \in \mathcal{N}, \phi \in \mathcal{P} \tag{24c}$$

$$Q_i^\phi = -V_i^{\phi,R}I_i^{\phi,I} + V_i^{\phi,I}I_i^{\phi,R} \quad \forall i \in \mathcal{N}, \phi \in \mathcal{P} \tag{24d}$$

$$(I_{ik}^{\phi,R})^2 + (I_{ik}^{\phi,I})^2 \le \overline{I_{ik}^\phi}^2 \quad \forall i \in \mathcal{N}, \phi \in \mathcal{P}, (ik) \in \mathcal{E} \tag{24e}$$

$$\underline{V_i^\phi}^2 \le (V_i^{\phi,R})^2 + (V_i^{\phi,I})^2 \le \overline{V_i^\phi}^2 \quad \forall i \in \mathcal{N}, \phi \in \mathcal{P} \tag{24f}$$

$$\underline{P_i^\phi} \le P_i^\phi \le \overline{P_i^\phi},\; \underline{Q_i^\phi} \le Q_i^\phi \le \overline{Q_i^\phi} \tag{24g}$$

where Y is the 3-phase bus admittance matrix for the network, and V and I are matrices of nodal voltages and currents respectively. Problem Eq. (24) is nonconvex due to bilinear constraints Eqs. (24c) and (24d), and the ring constraint Eq. (24f) on voltage magnitudes. We obtain a convex relaxation by using McCormick envelopes (MCE), which represent the convex hull of a bilinear product $w = xy$ by using upper and lower limits on x, y. Thus, we replace the bilinear equality with a series of linear inequalities, denoted as $\mathrm{MCE}(w) = \{w = xy : x \in [\underline{x}, \overline{x}], y \in [\underline{y}, \overline{y}]\}$:

$$MCE(w, \underline{x}, \overline{x}, \underline{y}, \overline{y}) = \begin{cases} w \ge \underline{x}y + x\underline{y} - \underline{x}\underline{y} \\ w \ge \overline{x}y + x\overline{y} - \overline{x}\overline{y} \\ w \le \underline{x}y + x\overline{y} - \overline{x}\underline{y} \\ w \le \overline{x}y + x\underline{y} - \underline{x}\overline{y} \end{cases} \tag{25}$$

We introduce auxiliary variables for each of the four bilinear terms $\{a_i^\phi, b_i^\phi, c_i^\phi, d_i^\phi\} = \{V_i^{\phi,R}I_i^{\phi,R}, V_i^{\phi,I}I_i^{\phi,I}, V_i^{\phi,R}I_i^{\phi,I}, V_i^{\phi,I}I_i^{\phi,R}\}$ allowing us to convert constraints Eqs. (24c) and (24d) to linear constraints with MCE constraints on each of the auxiliary variables. We also need additional constraints on the nodal current injections and nodal voltages in order to define the MCE constraints. These voltage and current bounds can be determined by applying a suitable preprocessing method using the nodal P and Q limits from the SMO bids (7). The resulting bounds will also implicitly satisfy constraints Eq. (24e) and Eq. (24f). Thus, we can replace constraints Eqs. (24c) to (24f) with the following set of constraints in order to obtain the relaxed CI-OPF problem, which reduces to a linear program that can be solved easily. However, we do incur the overhead of computing the tightest possible V and I bounds to obtain a good convex relaxation, which in turn ensures that the relaxed solutions are

feasible for the original problem.

$$P_i^\phi = a_i^\phi + b_i^\phi, \;\; Q_i^\phi = -c_i^\phi + d_i^\phi \quad \forall i \in \mathcal{N}, \phi \in \mathcal{P} \tag{26a}$$

$$\underline{I_i^{\phi,R}} \leq I_i^{\phi,R} \leq \overline{I_i^{\phi,R}}, \; \underline{I_i^{\phi,I}} \leq I_i^{\phi,I} \leq \overline{i^{\phi,I}} \tag{26b}$$

$$\underline{V_i^{\phi,R}} \leq V_i^{\phi,R} \leq \overline{V_i^{\phi,R}}, \; \underline{V_i^{\phi,I}} \leq V_i^{\phi,I} \leq \overline{V_i^{\phi,I}} \tag{26c}$$

$$a_i^\phi \in MCE(V_i^{\phi,R} I_i^{\phi,R}, \underline{V_i^{\phi,R}}, \overline{V_i^{\phi,R}}, \underline{I_i^{\phi,R}}, \overline{I_i^{\phi,R}}) \tag{26d}$$

$$b_i^\phi \in MCE(V_i^{\phi,I} I_i^{\phi,I}, \underline{V_i^{\phi,I}}, \overline{V_i^{\phi,I}}, \underline{I_i^{\phi,I}}, \overline{I_i^{\phi,I}}) \tag{26e}$$

$$c_i^\phi \in MCE(V_i^{\phi,R} I_i^{\phi,I}, \underline{V_i^{\phi,R}}, \overline{V_i^{\phi,R}}, \underline{I_i^{\phi,I}}, \overline{I_i^{\phi,I}}) \tag{26f}$$

$$d_i^\phi \in MCE(V_i^{\phi,I} I_i^{\phi,R}, \underline{V_i^{\phi,I}}, \overline{V_i^{\phi,I}}, \underline{I_i^{\phi,R}}, \overline{I_i^{\phi,R}}) \tag{26g}$$

6. DISTRIBUTED OPTIMIZATION

For a given global optimization (primal) problem with equality and inequality constraints for K number of nodes (or agents):

$$\min_x \sum_{i=1}^{K} f_i(x) \text{ s.t. } Gx = b, \quad Hx \leq d \tag{27}$$

We can decompose this into $\mathcal{S} = \{S_1, S_2, \dots S_K\}$ coupled optimization problems, known as atoms (representing each SMO i). We separate the vector of all decision variables x into two sets: $\mathcal{L} = \{L_i, \forall i \in [K]\}$ and $\mathcal{O} = \{O_i, \forall i \in [K]\}$ which is a partition of decision variables into those that are owned and copied by atom i, respectively. We can similarly also decompose the constraints into sets owned by each atom $\mathcal{C} = \{C_i, \forall i \in [K]\}$. These variable copies across multiple atoms can then be used to satisfy coupled constraints and global objectives. Note that for a number K, $[K] = \{1, 2, \dots K\}$.

The decomposed (or atomized) optimization problem is shown in Eq. (28), where a_j and $f_j(a_j)$ are the primal decision variables (both owned and copies) and individual objective functions corresponding to each SMO atom, respectively. G_j and H_j are the atomic constraint submatrices of G and H, while b_j and d_j are subvectors of b and d of the right hand side constraint vectors b and d, respectively. B is the directed graph incidence matrix defining the owned and copied atomic variables. This incidence matrix allows us to fully parallelize the distributed optimization by defining coordination or consensus constraints, which enforce that all the copied variables for each atom j must equal the values of their corresponding owned values in every other atom $i \neq j$. B_j and B^j denote the incoming and outgoing edges for atom j respectively. Here

$$\min_{a_j} \sum_{j \in K} f_j(a_j) \tag{28}$$

$$\text{s.t. } G_j a_j = b_j, \; H_j a_j \leq d_j, \; B_j a = 0 \; \forall j \in [K]$$

$$B_{im} \triangleq \begin{cases} -1, & \text{if } i \text{ is 'owned" and } m \text{ a related "copy"} \\ 1, & \text{if } m \text{ is "owned" and } i \text{ a related "copy"} \\ 0, & \text{otherwise} \end{cases}$$

The augmented Lagrangian is first atomized or decomposed for each node or SMO, introducing dual variables μ and ν corresponding to primal equality and coordination constraints respectively. Note that the inequality constraints are handled directly during the primal minimization step by appropriately defining the feasible set.

$$\begin{aligned} \mathcal{L}(a, \mu, \nu) &= \sum_{j \in K} \left[f_j(a_j) + \mu_j^T (G_j a_j - b_j) + \nu_j^T B_j a \right] \\ &= \sum_{j \in K} \left[f_j(a_j) + \mu_j^T (G_j a_j - b_j) + \nu^T B^j a_j \right] \\ &\triangleq \sum_{j \in K} \mathcal{L}_j(a_j, \mu_j, \nu) \end{aligned} \tag{29}$$

A. PAC algorithm. We can then apply the prox-linear approach of (8) to Eq. (29) and obtain the proximal atomic coordination (PAC) algorithm (9, 10):

$$a_j[\tau+1] = \underset{a_j \in \mathbb{R}^{|\tau_j|}}{\text{argmin}} \left\{ \begin{array}{l} \mathcal{L}_j(a_j, \bar{\mu}_j[\tau], \bar{\nu}[\tau]) \\ + \frac{1}{2\rho} \|a_j - a_j[\tau]\|_2^2 \end{array} \right\}$$

$$\mu_j[\tau+1] = \mu_j[\tau] + \rho \gamma_j \tilde{G}_j a_j[\tau+1]$$

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

Communicate a_j for all $j \in [K]$ with neighbors

$$\nu_j[\tau+1] = \nu_j[\tau] + \rho\gamma_j [B]^{O_j} a[\tau+1]$$
$$\bar{\nu}_j[\tau+1] = \nu_j[\tau+1] + \rho\hat{\gamma}_j[\tau+1][B]^{O_j} a[\tau+1]$$

Communicate $\bar{\nu}_j$ for all $j \in [K]$ with neighbors.

The primal and dual variables are initialized as follows, $\forall j \in [K]$:

$$a_j[0] \in \mathbb{R}^{||T_j|}$$
$$\mu_j[0] = \rho\gamma_j \tilde{G}_j a_j[0]$$
$$\bar{\mu}_j[0] = \mu_j[0] + \rho\hat{\gamma}_j[0]\tilde{G}_j a_j[0]$$
$$\nu_j[0] = \rho\gamma_j [B]^{O_j} a[0]$$
$$\bar{\nu}_j[0] = \nu_j[0] + \rho\hat{\gamma}_j[0][B]^{O_j} a[0]$$

B. NST-PAC algorithm. This work employs an enhanced, accelerated version called NST-PAC developed in (11). It is a primal-dual method incorporating both $L2$ and proximal regularization terms. The convergence speed is increased by using time-varying gains and Nesterov-accelerated gradient updates for both the primal and dual variables. The iterative NST-PAC algorithm consists of the following steps at each iteration τ:

$$\begin{aligned} a_j[\tau+1] = \underset{a_j}{\operatorname{argmin}} \Big\{ & \mathcal{L}_j\left(a_j, \hat{\mu}_j[\tau], \hat{\nu}[\tau]\right) \\ & + \frac{\rho_j\gamma_j}{2}\left\|G_j a_j - b_j\right\|_2^2 + \frac{\rho_j\gamma_j}{2}\left\|B_j a_j\right\|_2^2 \\ & + \frac{1}{2\rho_j}\left\|a_j - a_j[\tau]\right\|_2^2 \Big\} \end{aligned} \quad [30]$$
$$\hat{a}_j[\tau+1] = a_j[\tau+1] + \alpha_j[\tau+1]\left(a_j[\tau+1] - a_j[\tau]\right)$$
$$\mu_j[\tau+1] = \hat{\mu}_j[\tau] + \rho_j\gamma_j\left(G_j\hat{a}_j[\tau+1] - b_j\right)$$
$$\hat{\mu}_j[\tau+1] = \mu_j[\tau+1] + \phi_j[\tau+1]\left(\mu_j[\tau+1] - \mu_j[\tau]\right)$$

Communicate $\hat{a}_j$ for all $j \in [K]$ with neighbors

$$\nu_j[\tau+1] = \hat{\nu}_j[\tau] + \rho_j\gamma_j B_j\hat{a}_j[\tau+1]$$
$$\hat{\nu}_j[\tau+1] = \nu_j[\tau+1] + \theta_j[\tau+1]\left(\nu_j[\tau+1] - \nu_j[\tau]\right)$$

Communicate $\hat{\nu}_j$ for all $j \in [K]$ with neighbors

The algorithm further protects privacy by masking both the primal and dual variables. Masking is implemented by using iteration-varying and atom-specific parameters $\alpha_j[\tau]$, $\phi_j[\tau]$ and $\theta_j[\tau]$. Masking the dual variables (or shadow prices), in particular, is desirable since these may reveal sensitive data related to costs, operating constraints, or other preferences of SMOs. Instead, masked variables $\hat{a}$ and $\hat{\nu}$ are exchanged between atoms. By iteratively solving the local, decomposed optimization problems across all SMOs, NST-PAC (and PAC) provably converge to the globally optimal ACOPF (relaxed) solutions for the whole primary feeder (9, 11).

7. FEDERATED LEARNING

When it comes to DER forecasting, the challenges of privacy as well as the requirement of large training data sets, can be met using a distributed machine learning paradigm, federated learning (FL) (12–15). FL is a machine learning framework where each device participates in training a central model without sending actual data, but only exchanges gradient information in the training phase and sends prediction estimates during deployment. A general overview of the proposed DER prediction process is shown in Fig. S6. In the figure, various IoT devices including those at a house level such as smart thermostats and smart washers, and energy-producing devices such as PV and EVs are considered. The future smart grid will include a wider range of devices that will be capable of computation and communication. The house-level devices are grouped under a home energy manager H_i to enable aggregation at a house level while energy-producing devices such as EV and PV (grouped under E_i) are assumed to directly participate in a transactive environment. Both H_i and E_i can be considered typical IoT-based DERs connected to a power grid, whose energy consumption needs to be predicted. Using a communication infrastructure, our goal is to exchange information between the DERs in the bottom local layer and the global decision makers at the top layer in a private and secure manner so as to lead to an accurate prediction of the DER consumption/generation. The DER prediction is then utilized to formulate a grid service, to mitigate the load swings and "peaks" that occur in the distribution grid due to a lack of situational awareness. The FL-based DER prediction is used to anticipate the load swings and mitigate them by proactively controlling the DERs (16).

A typical process of DER-forecast can occur in the following manner. Collect the input-output pair $[x_t, \hat{P}^t(T)]$ for a federate F_i for several samples n. The features used in this work are $x_t = [P^t(T-15), P^t(T-30), P^t(T-60), P^t(T-120)]$, where $P^t(T-m)$ denotes the actual power consumption, and m denotes the minutes prior to time T. The number of samples n=2880,

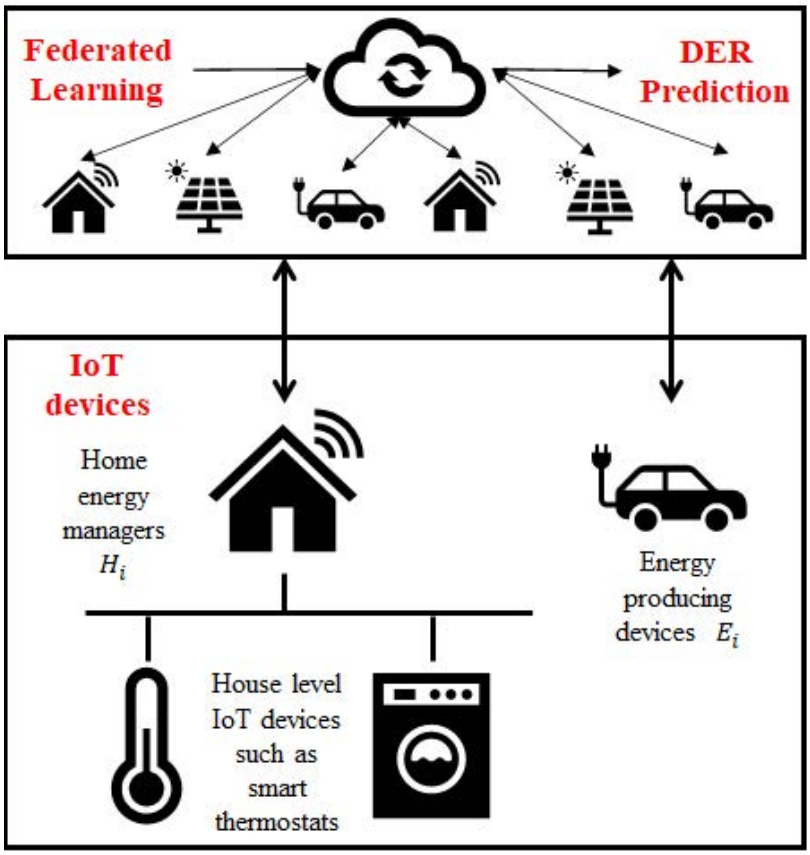


Fig. S6. An overview of the DER prediction process using federated learning. Image Credit: Reprinted with permission from (16).

was obtained by collecting data every 15 minutes over a period of 30 days. The overall training schematic of the FL-based neural network is shown in Fig. S7.

8. DETAILED COMMUNICATION STEPS AND TIMELINE

See Fig. S8 for more details on the communication among different market agents, operators, and resilience managers.

9. MITIGATION USING THE MARKET OPERATORS AND RESILIENCE MANAGERS

Our market framework consisting of the SM and PM provides situational awareness (SA) in the form of available power injections at various nodes at the primary and secondary levels. Once the market is cleared, during execution, the actual injections from the SMA and PMA are monitored by the SRM and PRM, respectively (see Fig. 3). These injections are then utilized by these managers to compute commitment scores, trustability scores, and resilience scores (RS), as shown in Section E and Section A. In what follows, we will show how the SA from the market operators and the RS from the resilience managers can be utilized to mitigate all the attacks described in Section 3.

As a result of continuous monitoring, any unexpected deviation from the agents' nominal performance in the form of change in the net injection at the PCC, raises a flag. Any such flag makes the operators shift from the nominal operating mode to the resilience mode. Minimal visibility regarding actual injections from all PMA is assumed to be available. Rather, we assume that each SRM only locally observes the actual injection from the corresponding SMA, and each SRM communicates that information to the PRM. More importantly, the attack scenarios considered also assume that this important communication to the PRM from all SRMs is completely sabotaged (as was the case in the Ukraine 2015-16 attacks). Despite this loss of communication, the PRM is able to step in and mitigate the attack as the flag raised is independent of this communication loss and is due to a physical impact of the agents' deviation from nominal performance. Subsequently, the PMO redispatches trustworthy PMAs so as to bring the power import from the bulk grid down to pre-attack levels. The new setpoints for the PMAs/SMOs are in turn suitably disaggregated to compute new setpoints for the SMAs through a re-dispatch by the SM. Before proceeding to the results, we propose a specific mitigation strategy that leverages the SA provided by our approach.

A. Algorithm (A) for redispatch by the PMO in a balanced network . We first consider a balanced, equivalent single-phase network using the BF model. The starting point for the overall mitigation sequence is the awareness that an attack has occurred. This is realized by the PRM in the form of a change in the net load from P_{PCC} to $\overline{P}_{PCC}$, which denotes the net

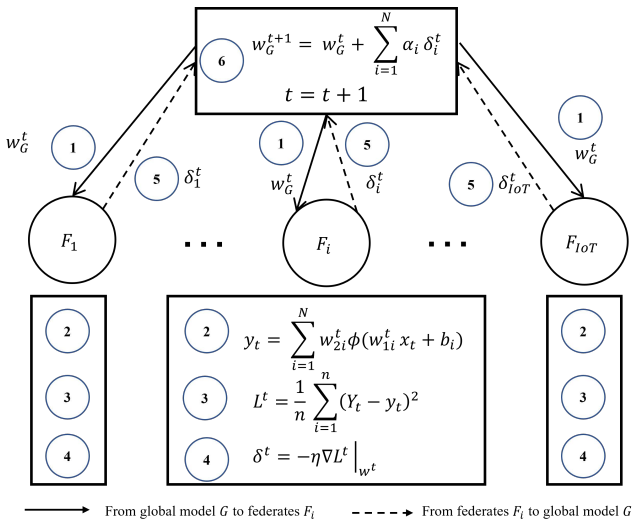


Fig. S7. The schematic of neural network training using federated learning is shown here. The steps (1)-(6) are repeated until $L^t \leq \epsilon$. Image Credit: Reprinted with permission from (16).

load from the entire primary feeder at the substation before and after the attack, respectively. This can be detected by the PRM at the substation or point of common coupling (PCC) since this is the power it imports from the main transmission grid. We propose a redispatch algorithm that the corresponding SMOs can carry out based on the ratio between these two values. To describe this redispatch algorithm, we begin with the cost function in Eq. (4) for the PM ACOPF problem. For ease of exposition, this can be rewritten in a simplified manner as:

$$\sum_{i=1}^{n} \left(\frac{1}{2} \alpha_i P_i^{G^2} + \beta_i \left(P_i^L - P_i^{L0} \right)^2 \right) + \xi \cdot losses \quad [31]$$

$$\overline{\alpha}_i = \Delta_\alpha \alpha_i,\ \overline{\beta}_i = \Delta_\beta \beta_i,\ \overline{\xi} = \Delta_\xi \xi;\ \alpha, \beta, \xi, \Delta > 0 \quad [32]$$

$$\Delta_\alpha = \Delta_\beta = \frac{|P_{PCC}|}{|\overline{P}_{PCC}|},\ \Delta_\xi = \frac{|\overline{P}_{PCC}|}{|P_{PCC}|} \quad [33]$$

We note that a change in the power import from the main grid causes $\Delta_\alpha, \Delta_\beta, \Delta_\xi$ to deviate from unity. Suppose that several distributed local generator SMOs are attacked, as in Attack 1(a). This would increase net feeder load, i.e. $|\overline{P}_{PCC}| > |P_{PCC}|$ (note that both $P_{PCC}, \overline{P}_{PCC} < 0$ since net loads are negative injections), thus causing $\Delta_\alpha < 1$. Applying this cost coefficient update would lower the cost coefficients from α_i to α_i'. This results in dispatching more local generation from remaining online SMOs instead of importing power from the bulk grid. As the SMOs also have information about the flexibility in their corresponding SMAs in the form of $\delta P^*, \delta Q^*$ (see Section A.2), the overall hierarchical PM-SM market structure automatically provides the solutions of the new dispatch. Similarly, a value of $\Delta_\beta < 1$ reduces the disutility coefficients to encourage more demand response via load shifting and/or curtailment, by utilizing the downward flexibility provided by the SMOs bidding into the PM, and subsequently also by the SMAs bidding into the SM. In contrast to these two values, when the net import from the main grid increases, then $\Delta_\xi > 1$ penalizes electrical line losses more heavily in the objective function. As a result, the redispatch discourages imports from the transmission grid in favor of dispatching more local DERs. This is because distribution grids are more lossy (have higher resistance to reactance ratios), and hence prioritizing the loss minimization makes it more efficient to utilize local generation closer to the loads being served.

After deriving the multiplicative coefficient update factors $\Delta_\alpha, \Delta_\beta, \Delta_\xi$, the PRM can broadcast these common values to all the SRMs simultaneously, who in turn send them to their corresponding SMOs. The SMOs update each of their objective function coefficients using these factors and then perform distributed optimization to redispatch the PM, resulting in new P and Q setpoints for SMOs, along with new nodal distribution LMPs (d-LMPs). This is followed by each SMO also re-dispatching their SM, in order to disaggregate the new setpoints among their SMAs. A timeline of the key events is shown in Fig. S9.

B. Algorithm (B) for redispatch in an unbalanced, 3-phase network. For the unbalanced 3-phase case, we use a modified algorithm for the coefficient update. The update rule here is more sophisticated since in this case, the variables are now 3-phase

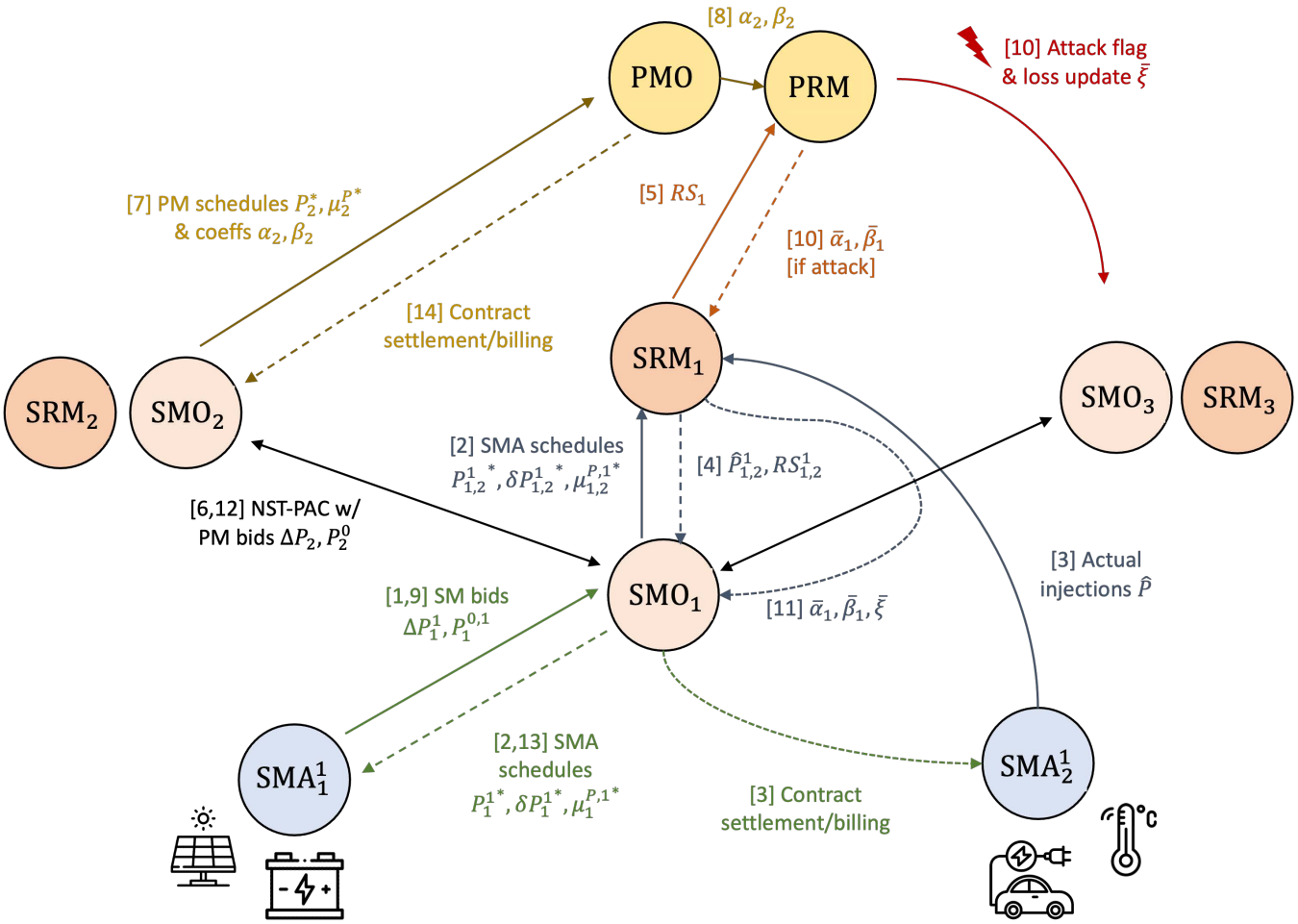


Fig. S8. Diagram showing a more detailed communication scheme and steps for information exchange between the various market operators, agents, and resilience managers at the secondary and primary levels.

vectors rather than scalars.

$$\Delta = \mathbf{P}_{PCC} - \overline{\mathbf{P}}_{PCC} \quad [34]$$

$$Z_i(\delta_i) = 1 + \frac{RS_i \Delta^\top \delta_i}{\mu \sum_i RS_i} \Longrightarrow \gamma_{i\delta} = \frac{1}{Z_i(\delta_i)} \quad [35]$$

$$\overline{\boldsymbol{\alpha}}_i = \gamma_{i\alpha} \boldsymbol{\alpha}_i, \quad \overline{\boldsymbol{\beta}}_i = \gamma_{i\beta} \boldsymbol{\beta}_i, \quad \overline{\boldsymbol{\xi}} = \left(\frac{\sum_i \gamma_{i\alpha} + \gamma_{i\beta}}{2n} \right)^{-1} \boldsymbol{\xi} \quad [36]$$

Note here that $\mathbf{P}_{PCC}, \overline{\mathbf{P}}_{PCC}$ are the 3-phase power imports from the tie line before and after the attack. $\boldsymbol{\alpha}_i, \boldsymbol{\beta}_i$ are 3×1 vectors representing cost and disutility coefficient for each phase at SMO node i, and $\boldsymbol{\xi}$ is a 3-phase hyperparameter that penalizes line losses in the objective function. A DG attack that increases net load would result in $\gamma_{i\alpha}, \gamma_{i\beta} < 1$ and $\overline{\boldsymbol{\xi}} < \boldsymbol{\xi}$. Thus, these coefficient updates work using a similar intuition to algorithm (A) in that it favors local DER generation and load flexibility over transmission imports. A key difference here is that the PRM also takes into account the RS of each SMO during the redispatch so that it relies more heavily on resilient SMOs for attack mitigation. The PRM updates the coefficients α_i, β_i and ξ to α_i', β_i' and ξ', and sends the new coefficient values to all SRMs. The SRMs send these new objective functions to the corresponding SMOs, and the rest of the mitigation procedure follows in the same manner as in the previous section.

10. RESILIENCE-DRIVEN RECONFIGURATION ALGORITHM

All possible shortest paths are computed between each generation source and critical load pairs present within the system using the graph network. If the generation is not enough to supply the total critical load, then the algorithm searches for the next available generation. This will continue until the critical load demand is met. As the generation sources are assigned to critical loads, if any source's capacity is more than the assigned load, the source's partial remaining capacity will be utilized for other loads. Once we have all the feasible paths for reconfiguration, we will compute the resiliency metric for each path (see

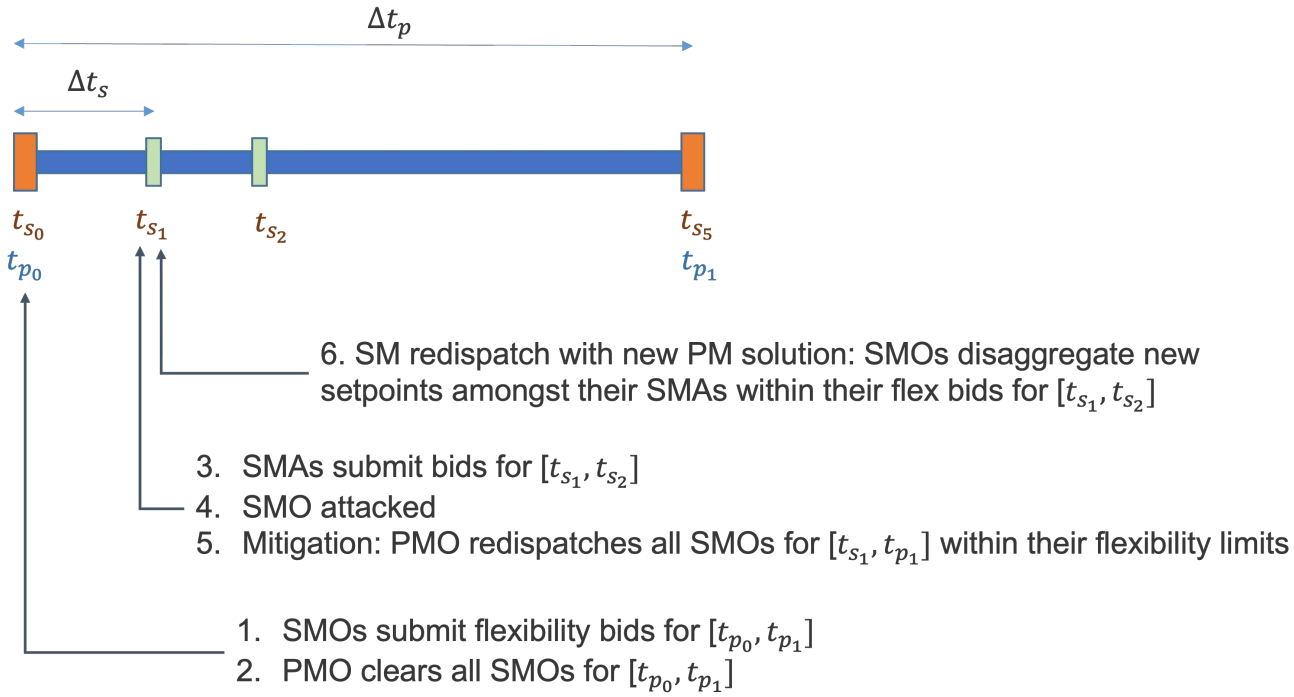


Fig. S9. Timeline of attack detection and mitigation. Image Credit: Reprinted with permission from (17).

Section B for how to compute the resiliency metrics and PNR), which will support the operator in finding the most resilient path to restore. The reconfiguration paths will be determined based on the stress levels of the grid and the corresponding degree of the failed SMA node, the tolerance bands and flexibility of the ICA, and the security levels and privacy needs of the SMA. This process is outlined in Fig. S10.

11. VALIDATION PLATFORMS

A. PNNL. Since the proposed framework is intended to be deployed in a large-scale distribution system with a high penetration of renewables, we choose our first validation platform to be driven by HELICS (Hierarchical Engine for Large-scale Infrastructure Co-simulation), an open-source cyber-physical energy co-simulation framework for energy systems (18). As the core engine of the platform, HELICS provides time management and data exchanges between the simulators, also known as federates. Moreover, through standard procedures and application programming interfaces (APIs), data exchange between federates is performed either as values or messages. Within this platform, GridLAB-D is the distribution system simulator used to simulate all of the use cases we discussed above. GridLAB-D is versatile, with the capability of simulating large 3-phase unbalanced distribution systems, with agent-based and information-based modeling tools and extensive data collection tools for end-use technologies and interface APIs for co-simulation (19). Thus, it allows us to modify the standard IEEE 123-node system to include (1) residential (either single or multi-family) and commercial buildings with or without heating, ventilation, and air conditioning (HVAC) systems, (2) edge devices with IoT connectivity including HVAC type appliances, small electronics and lighting, (3) distributed generators (DGs) such as photovoltaic (PV) panels, battery energy storage systems (BESSs), and diesel generators. The distribution model is also assumed to have all its loads connected via smart meters with load-shedding capability to regulate energy demand according to a distribution system operator's command. Specifically, the IoT-enhanced version of the IEEE 123-node system consists of the assets detailed in Table S2.

B. NREL. The objective of validating the EUREICA framework at NREL is to evaluate the feasibility of implementing the framework in *real-time*. Since electrons flow in the grid in real-time, it is critical that the operations proposed should also function in real-time, and be in compliance with operational requirements. The Advanced Research on Integrated Energy Systems (ARIES) at NREL is a cutting-edge virtual emulation platform that encompasses actual Distributed Energy Resource (DER) hardware systems, such as wind turbines, photovoltaic (PV) arrays with controllers, batteries, and storage systems (20). The digital real-time simulation (DRTS) cluster of ARIES is used for validating the performance of the EUREICA modules. The overall validation platform is shown in Fig. S11. It constitutes 5 components - (i) IoT device virtualization (using Raspberry Pis and Typhoon HIL to characterize IoT devices), (ii) Communication emulation (using analog and network connections to emulate communication at the speed of actual communication in the field) (iii) hardware-in-the-loop interface (to provide increased fidelity for components under study) (iv) digital real-time simulation (using RTDS and Typhoon HIL to emulate the power grid in real-time) (v) Time synchronization (to bring together the hardware components using a time server

Table S2. GridLAB-D IEEE 123-node test feeder features with IoT-enhanced model.

		Number	Capacity
Standard IEEE 123-node test feeder	Spot loads	85	3,985.7 kVA
EUREICA IEEE 123-node test feeder	Houses - Demand response (HVACs in all, WHs in 348)	1,008	variable (4 KW avg/house) (20% to 30% critical)
	Distributed generators (DGs)	380	1,745.8 kVA (≈ 44% system penetration)
	PVs	207	880.84 kVA
	BESSs	173	865 kVA
	Community PVs	12	96 kVA

to ensure accuracy of simulation). This validation platform is used to determine the performance of the EUREICA framework for all the modules.

C. LTDES. A training simulator-based platform was also used to validate the EUREICA framework. In particular, the General Electric (GE) ADMS DOTS (Advanced Distribution Management System-Distribution Operations Training Simulator), used for training operators and dispatchers, was used as the validation platform. Rather than users waiting to experience challenging events on the job, dispatchers are able to familiarize themselves with advanced application functionality and gain an understanding of how they interact with other subsystems of the ADMS. Into this ADMS-DOTS we introduce DERIM, a Distributed Energy Resource Integration Middleware, an interface that allows integration of various DERs with the ability to communicate as dictated by the EUREICA framework (see Fig. S12). This integrated system uses the same software components, programmatic and user interfaces as the real-time ADMS, and creates an effective training and testing environment to operate with the actual network model, data, and functions in a controlled and safe environment. Fig. S13 shows an example of what the validation process looks like for attack 1a.

12. Kundur 2-area system

Fig. S14 is a diagram of the Kundur 2-area transmission system commonly used as a test case to study dynamic stability, power interchange, oscillation damping, etc. The system contains 11 buses, four generators, and two areas. The two areas are connected with weak tie lines (21).

13. Numerical simulation setup for markets

All use cases considered are based on an IEEE 123 test feeder (see Fig. 2), which is radial, unbalanced, and multi-phase. The feeder was modeled in the GridLAB-D environment (see SI Section A for more details) and augmented to have a high penetration of DERs. For all attacks except attack 3, we assumed that the switch settings are in their nominal positions such that we have one primary feeder, with 85 active nodes with SMOs/PMAs (out of the 123 in total). A PMO was assumed to be at the slack bus (substation), at either 115 or 69kV, with the SMOs at 4.16kV, and each SMA at 120-240V. The flexibility bids for the SMAs and the SMOs were randomly generated, allowing each to offer flexibilities of up to ±30% around their baseline power injections (22). We used 5-minute real-time market LMPs from the California ISO and assumed the Q-LMP to be 10% of the P-LMP. Note that for all attack scenarios except attack 3, we used the CI model to represent the feeder as is.

For attack 2, however, we considered a modified version of the feeder and deployed the BF model instead. Here, we modified the original IEEE-123 feeder to consider a case where we have a few large distributed generators (PV, batteries, diesel generators) concentrated at just five primary feeder (SMO) nodes numbered 25, 40, 67, 81, and 94. This is in contrast to the other attacks where there were instead a larger number of smaller DERs distributed throughout the network. Another distinguishing factor of this scenario is that the originally unbalanced feeder was converted to an equivalent balanced 3-phase model by (i) assuming all switches to be at their normal positions, (ii) converting single-phase spot loads to 3-phase, (iii) assuming cables to be 3-phase transposed, (iv) converting configurations 1 thru 12 to symmetric matrices and (v) modeling shunt capacitors as 3-phase reactive power generators (10). Each SMO was assumed to have between 3-5 SMAs with the number chosen uniformly at random. Since the injection data in the original IEEE-123 model was only available up to the primary feeder node level, we artificially randomly disaggregated the injections at each SMO amongst its SMAs, which could be net loads or generators.

We then performed a co-simulation of both the PM and SM for all attack scenarios. We refer the reader to (4, 23) for the behavior of this market structure for a nominal scenario when there is no attack. In what follows, we only consider the three attack scenarios described above. We also note that our flexibility bids were synthetically created, so the resulting flexible ranges in our simulations may be quite large at times and not realistic in some cases. However, our proposed framework can be generally applied to cases where there is less DER flexibility as well.

14. MARKET SIMULATIONS OF OTHER ATTACKS

A. Mitigation of Attack 1b. We note that in Attack 1b, there is a loss in net generation, and therefore the power imported from the bulk grid increases. It is also assumed that the communication from all SRM to the PRM is disrupted, while the

communication from PRM to SRM remains intact. That is, the PRM loses observability but is still able to communicate the redispatch of the new coefficients to the SRM. We do not consider the case when such observability is not lost, a discussion of which is beyond the scope of this paper. With the redispatch, the PM-SM framework identifies all of the new trustable PMAs through the SA computations described in Section 3 with the overall power balance met at all points in the distribution grid.

The steps in mitigating this attack are as follows. Due to the attack, 45 kW of net-generation compromised as shown in Fig. S15a. The PMO alerts other trustable PMAs/SMOs to redispatch their generation assets in the PM. Trustable PMAs/SMOs will curtail flexible loads to respond and mitigate the attack as in Fig. S17. The redispatch is also influenced by the resilience scores of different SMOs over time shown in Fig. S18. SMOs redispatch the SM which provides correct setpoints to all their SMAs. An example of this in Fig. S16 shows how the SMO at node 35 disaggregates its new setpoint amongst its 3 SMAs. As a result of mitigation, the total import from the main grid stays at the same level as shown in Fig. S15b.

B. Mitigation of Attack 1c. Attack 1c is a more distributed attack where individual SMAs representing secondary feeders are attacked directly. We considered a case where a large number of DGs including solar PV and batteries are attacked. A total of 53 SMA nodes with DGs were compromised and taken offline, resulting in a total loss in generation capacity of 157 kW. This leads to a decrease in the net injections across all the SMOs as seen in Fig. S19a - there are no longer any SMOs with net generation after the attack and the loss of local generation also increases the net load at the SMOs. This leads to an increase in power import from the main transmission grid as in Fig. S19b.

In the case of all other attacks, the mitigation strategy involves the PM redispatch occurring 1st followed by the SM redispatch. There, only the PM is directly involved in attack mitigation while the SM is only used to disaggregate the new SMO setpoints amongst their SMAs. However, in the case of attack 1c, the SM redispatch occurs first at the secondary feeder level and is then followed by the PM redispatch at the primary feeder level. Thus, both the SM and PM are actively involved in attack mitigation here. We see in Fig. S19b that we can partially mitigate the attack by leveraging the flexibility of SMAs in the SM. However, SM mitigation alone is not sufficient. We need to also utilize the inter-SMO flexibility in the PM to fully mitigate and restore the feeder import back down to the pre-attack level. A summary of the attack metrics is shown in Table S3.

Table S3. Attack 1c summary.

	Power import [kW]	Total net load [kW]
Pre-attack	1412	1457
Post-attack	1722	1716
SM mitigation only	1553	1547
SM + PM mitigation	1422	1417

We also compare the flexibility bids of the SMOs before and after the attack in Fig. S20. As expected, the net load of the bids generally increases across all SMOs due to the loss of local DGs at their respective SMAs. However, by leveraging their SMA flexibilities, the SMOs are still able to offer some flexibility to the PM to help mitigate the attack.

C. Mitigation of Attack 2a . This corresponds to a case where there are five large distributed generators in the modified IEEE-123 system, one of which (at SMO node 94) is taken offline. Here, we see that the remaining four SMO nodes (25, 40, 67, 81) have more than enough remaining generation capacity to meet the shortfall caused by the attack. Without mitigation, the attack would have resulted in an additional import of about 261 kW from the main grid. However, by utilizing the upward flexibility of remaining SMOs, we are able to fully resolve the attack and bring the total power imported back to pre-attack levels. The left figure in Fig. S21 shows the results of the PM dispatch before the attack and after attack mitigation for the five key SMO nodes of interest. The plot also shows the SMO's bids into the PM, with the dashed blue line being the baseline injection bid and the blue-shaded region representing the upward/downward flexibility around it. The right figure shows the results of the SM re-dispatch after the attack mitigation and PM re-dispatch for SMO 67 as an example. It disaggregates the new setpoints among its three SMAs, with SMA 1 being a net load while SMAs 2 and 3 are net generators.

D. Effects of Attack 2b on prices and economic implications. We can obtain the electricity prices in the PM from the dual variables associated with the power balance constraints in Eq. (22). We refer to these as distribution-LMPs (d-LMPs) at each node (with an SMO) in the primary feeder. We compared the normalized d-LMPs for active power before and after the attack, as well as post-attack mitigation, shown in Fig. S22. As intuitively expected, we see that nodal prices increase throughout the grid after the attack and rise even further after implementing the attack mitigation steps, indicating that the loss of some local generation makes it more expensive to satisfy network constraints and results in sub-optimal solutions. The pre-attack and post-attack prices have nearly the same spatial profile across all the SMO nodes, with the post-attack values essentially being higher by an offset. This makes sense because the d-LMP variations between nodes are influenced by congestion on lines. In the attack case without mitigation, the shortfall caused by the attack would've been compensated for entirely by importing extra power from the grid, and thus the relative congestion variation over the rest of the network remains largely unchanged. The price trends after attack mitigation look more different since the changes in power flow and congestion (resulting from the PM re-dispatch) are not uniform throughout the network. Notably, we see that the prices are significantly more volatile,

especially around the nodes affected by the attack. The price also peaks at node 67 - this makes sense since it has the highest increase in injection after attack mitigation, which in turn worsens congestion in lines connected to it.

Another important consideration is the impact of our mitigation approach on the different market participants, i.e., the SMOs and SMAs themselves. The objective function update rules from Sections A and B generally imply that these local resources will be compensated less per unit (kW or kVAR) of grid support they provide, either in terms of load flexibility or generation dispatch. It may also lead to significant load shifting and curtailment in order to meet grid objectives, which can reduce the overall utility of end-users. We also need to more carefully study the distributional impacts of such methods since they may end up disproportionately negatively impacting certain groups of customers or prosumers, which could in turn have important implications for energy affordability, equity, and fairness.

15. FURTHER VALIDATION DETAILS OF ALL ATTACK SCENARIOS

A. Validation of Attack 1a by PNNL using HELICS. This attack artificially increases the load at several devices throughout the network. Fig. S23 shows the effects of attack 1a and mitigation on the total feeder load over the course of the 48-hour simulation. This was performed using the HELICS platform and a GridLAB-D model (see Section A for details). Firstly, we notice that the application of the LEM during day 2 generally results in curtailment of net load by leveraging DER flexibility, relative to day 1 (when the market is not used). Secondly, upon zooming in on the attack period (around 13:00 PST), we see that the LA attack increases the total system load. However, attack mitigation is quickly able to reduce the system load using flexibility and help the system recover.

B. Validation of Attack 1b by PNNL using HELICS. We utilized the HELICS-based co-simulation platform to simulate this use case in which several of the distributed generation resources are being disconnected leading to about a 44 kW loss in generation. That is accomplished in the model simulation by taking offline the PVs at the buses as indicated in Fig. S15a. However, with the SA enabled through the market module, the SM agents are informed about how much they need to adjust their flexible assets, which results in an approximate 36 kW load and local generation alteration after attack mitigation to counterbalance the distributed generation loss, as seen in Fig. S17. The effect of the market integration on the total system load during the second 24-hour period of a 48-hour simulation is depicted in Fig. S24. In particular, the window details the attack that happens around 13:00 on the second day and how the total flexible load is manipulated to mitigate the need for increased generation demand from the main grid. We see that the attack mitigation reduces the impact of the attack by lowering the total feeder load and bringing it back down closer to the values if there wasn't an attack. However, we note that even after mitigation, the load is still slightly higher than the 'without attack' case for some periods but much lower than the 'with attack' case.

C. Validation of Attack 3 by PNNL using HELICS. The enhanced EUREICA IEEE 123-node feeder is covered partially by the local distributed generation resources, that is the PVSs and BESSs, and mainly from the main transmission and generation grid through a connection at node 150, as shown in Fig. 14. Moreover, the system has available 2 large diesel generators at buses 48 (150 kVA rated capacity) and 66 (1 MVA rated capacity), respectively, that could be called upon to serve loads in case of adversarial events. Also, a set of switches between certain nodes of the system configures it into 7 areas that could be isolated in certain scenarios to be able to serve critical loads, as in Fig. 14. The initial configuration of the switches is given in Table S4.

Table S4. Original switch configuration in the EUREICA IEEE 123-node test feeder.

Node A	Node B	Switch status
13	152	CLOSED
18	135	CLOSED
60	160	CLOSED
61	610	CLOSED
97	197	CLOSED
150	149	CLOSED
250	251	OPEN
450	451	OPEN
300	350	OPEN
95	195	OPEN
54	94	OPEN
151	300	OPEN
13	18	CLOSED
86	76	CLOSED
48	48_dg	OPEN
65	65_dg	OPEN

The validation scenario assumes that due to an adversary event, either a cyber attack or a physical phenomenon, the distribution system gets islanded from the main grid, which is simulated by opening the switch between nodes 150 and 149 at 13:00. The system reconnection to the main grid is assumed to happen at 14:00. As expected, at 13:00 the system collapses, which is demonstrated by the sudden drop to 0 for all the spot-load bus voltages, as seen in Fig. S25.

The proposed reconfiguration and load shed approach addresses the situation created at 13:00 hours, creates situational awareness, and decides the switch statuses and loads that might need to be shed. If only the available diesel generators are brought online once the system is disconnected from the grid, by reconfiguring the corresponding switches status, the system would not be in a blackout, as seen in Fig. S26.

However, as seen in Fig. S27, to supply the entire house population load (the total measurements from the house management units in the second graph from the top), even with the support of the PVs and batteries, the diesel generators would still need a total capacity of over 2 MW (as seen in bottom-most graph of Fig. S27), which is more than the maximum capacity of the model diesel generators.

Through the proposed resilience-based IoT load restoration with demand response optimization strategy, a feasible reconfiguration path is computed to open and/or close tie switches and shed either completely/partially grid edge loads to allow the available generation resources to cover the approximately 30% critical load in the system, as identified in Table S2. As seen in Fig. 15, with the almost 70% load shed (second graph from the top) between 13:00 and 14:00 hours, and batteries only allowed to discharge, if possible, to supply extra energy (third graph from the top), the burden on the diesel generators is significantly alleviated as they only need to ramp up to about 230 KW.

For the islanded attack, the power flow redirection through switch reconfiguration as in SI Fig. S10 and load shed also helps with keeping the spot-load buses voltages within the admissible limits during the attack (Fig. S28). Moreover, by bringing the loads back online sequentially after system recovery, under-voltage problems due to load rebound are also avoided.

D. Validation of Attack 1a by LTDES using DERIM-ADMS-DOTS. While Fig. 7 zooms in on the period around the attack timestep, Fig. S29 shows the total feeder head load over the entire 24 h simulation horizon. We can clearly see the blip at 13:00 PST indicating the impact of the attack. Fig. S30 shows the effects of attack and mitigation on the net load at all the SMO primary nodes. This shows that the DERIM-ADMS-DOTS validation produces similar results to our market simulation in Fig. 4a and Fig. 5. The attack increases the load at the following nodes: 12, 17, 21, 36, 65, 75, 95, 105, 112, and 113. The majority of load curtailment for mitigation is contributed by the larger loads at nodes 1, 16, 48, 76, and 88.

E. Validation of Attack 1b by LTDES using DERIM and ADMS-DOTS. Fig. S31 shows the effects of the DG attack 1b on the total system load over the full 24 h simulation while Fig. S32 zooms in on the period around the attack. We see that without the market-based mitigation, the feeder demand would have jumped by 68 kW due to the attack. However, with mitigation, the attack impact is minimal since there's only a 4 kW increase in feeder demand. Fig. S33 shows the changes in net injections at all primary nodes during attack 1b. This essentially shows that we leverage flexibility from several primary nodes across the feeder, producing results similar to those shown in SI Section A and Section B. The attack causes the following DG nodes to lose power and go offline: 9, 28, 45, 55, 56, 58, 62, 73, 82, and 94. The following flexible load nodes contribute a majority of the curtailment needed to mitigate: 1, 48, 76, and 88.

Fig. S34 compares the load setpoints at the SMO level (updated every 5 minutes) for node 76 versus the aggregated setpoints over all the SMAs at this node (cleared every 1 minute). Although these are largely similar, there are some slight differences between the two values. Thus, it may make more sense to utilize the more precise SMA setpoints directly for the ADMS simulation.

We also did some further analysis on the role of the SM and PM in attack mitigation. Fig. S35 compares the contributions of the setpoints of the SMOs (5 minutes) and the SMAs (1 minute). The blue bar shows the 5-minute setpoint changes expected from the SMOs, while the orange bar shows the 1-minute setpoint changes at the SMA level. We see that the SM clearing every minute and the associated SMA setpoint changes contribute more toward the overall primary load adjustment when compared to the SMO-level changes alone.

F. Validation of Attack 3 by LTDES using DERIM and ADMS-DOTS.

F.1. Case 1: Critical loads distributed across the feeder. Fig. S36 shows the new switch settings and updated topology after applying the resilience-based reconfiguration during attack 3. In this case, we assume that there are critical loads distributed throughout the feeder. The system is islanded from the main grid at 13:00 PST and islanding ends at 14:00.

The DG at node 48 can output up to 270 kW while DG 65 outputs a constant 15 kW, and we use node 150 as the swing node (or slack bus) for the simulation. Fig. S37 shows the impact of the attack on the total feeder load and Fig. S38 shows the changes in the net load at all primary nodes without the attack and with the attack (and associated reconfiguration). We see that the DGs at nodes 48 and 65 together pick up about 300 kW of the critical load, which represents about 20% of the total baseline load. The remaining 80% of the feeder load which is non-critical is shed (goes to zero after the attack in Fig. S38) to maintain feasibility.

F.2. Case 2: Critical loads aggregated in a single zone. Fig. S39 shows the new switch settings and updated topology after applying the resilience-based reconfiguration during attack 3. In this case, we assume all the critical loads are concentrated only in zone 3. The system is islanded from the main grid at 13:00 PST and islanding ends at 14:00. During reconfiguration, switch 18-135 is opened so that cluster 3 becomes a microgrid. The DG at node 48 has sufficient capacity to meet all the load in zone 3 alone. Again, node 150 is used as the slack node for the simulation.

Fig. S40 shows the changes in the net load at all primary nodes without the attack and with the attack (and associated reconfiguration), as observed from the simulation results. We see that the DG at node 48 picks up all the expected load in zone 3 with 430 kW of generation output.

Thus the main conclusions from the attack 3 validation using DERIM-ADMS-DOTS are as follows. Under case 1, the reconfiguration algorithm is able to restore all the critical loads throughout the islanded distribution circuit without relying on any power from the external transmission grid. In case 2, all the load in zone 3 (as a microgrid) was completely restored without any loss of load. In both cases, without the SA provided by the EUREICA framework, the control center operator at the substation would not have the necessary means to achieve restoration.

G. Validation of Attack 1a by NREL using ARIES. The market structure is implemented using the same validation platform, with the primary feeders modeled on the RTDS, and secondary feeders, and below on Typhoon HIL and Raspberry Pis. In the implementation, the SMAs receive DER predictions from federated learning. The PMO and SMOs solve for primary and secondary market setpoints at each primary feeder node and secondary feeder, respectively, and then they are distributed to the SMAs, and ultimately to the IoT devices. Under nominal conditions (without an attack), the market operates with the objective of voltage regulation and minimization of power import from the main grid.

In the case of attack 1a, the secondary feeder load increases by 63 kW, which may be driven by various factors, such as weather-related load swings, or a coordinated cyber attack across IoT devices, such as the MadIoT attack. In this case, the mitigation is provided by using 30 flexible load nodes. Curtailment at the IoT device level ranges from a minimum of 0.2 kW reduction and a maximum of 0.5 kW reduction per primary feeder node. In total, approximately 130 kW of power import from the main grid decreases after mitigation. Market clearing happens every minute, and the drop in the load is shown in Fig. S41. The IoT device response, which is the thermostat in this case, has an instantaneous response, with an immediate drop in net load.

H. Validation of Attack 3 by NREL using ARIES. The mitigation of Attack 3 is validated using the RTDS at NREL-ARIES. The implementation of the reconfiguration algorithm in the RunTime environment of RTDS is shown in Fig. S42.

In the case where the EUREICA framework is not used, the frequency of the system becomes unstable, and the distribution feeder is broken into islands and only the loads in Zone 3 are picked by the DG in Node 48. This plot is shown in Fig. S43.

The case with the EUREICA framework, with the contributions from various DGs and the military microgrid connected at Node 66 has already been demonstrated in Section E.3.

References

1. WH Kersting, Radial distribution test feeders in *Proceedings of the 2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 01CH37194)*. (IEEE), Vol. 2, pp. 908–912 (2001).
2. T Athay, R Podmore, S Virmani, A practical method for the direct analysis of transient stability. *IEEE Transactions on Power Apparatus Syst.* pp. 573–584 (1979).
3. UC Bureau, Quick facts: Boston city, massachusetts (2023) available at https://www.census.gov/quickfacts/fact/table/bostoncitymassachusetts/PST120222 (accessed 23 April 2024).
4. VJ Nair, V Venkataramanan, R Haider, AM Annaswamy, A hierarchical local electricity market for a der-rich grid edge. *IEEE Transactions on Smart Grid* **14**, 1353–1366 (2022).
5. PS Sarker, SK Sadanandan, AK Srivastava, Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System With IoTs. *IEEE Internet Things J.* **10**, 7469–7479 (2023).
6. H Booth, D Rike, G Witte, The national vulnerability database (nvd): Overview, Technical report (2013).
7. G Ferro, M Robba, D D'Achiardi, R Haider, AM Annaswamy, A distributed approach to the Optimal Power Flow problem for unbalanced and mesh networks. *IFAC-PapersOnLine* **53**, 13287–13292 (2020).
8. A Aljanaby, E Abuelrub, M Odeh, A survey of distributed query optimization. *Int. Arab. J. Inf. Technol.* **2**, 48–57 (2005).
9. JJ Romvary, G Ferro, R Haider, AM Annaswamy, A Proximal Atomic Coordination Algorithm for Distributed Optimization. *IEEE Transactions on Autom. Control.* **67**, 646–661 (2022).
10. R Haider, et al., Toward a Retail Market for Distribution Grids. *IEEE Transactions on Smart Grid* **11**, 4891–4905 (2020).
11. G Ferro, M Robba, R Haider, AM Annaswamy, A Distributed-Optimization-Based Architecture for Management of Interconnected Energy Hubs. *IEEE Transactions on Control. Netw. Syst.* **9**, 1704–1716 (2022).
12. Q Yang, Y Liu, T Chen, Y Tong, Federated machine learning: Concept and applications. *ACM Transactions on Intell. Syst. Technol. (TIST)* **10**, 1–19 (2019).
13. T Li, AK Sahu, A Talwalkar, V Smith, Federated learning: Challenges, methods, and future directions. *IEEE Signal Process. Mag.* **37**, 50–60 (2020).
14. WYB Lim, et al., Federated learning in mobile edge networks: A comprehensive survey. *IEEE Commun. Surv. & Tutorials* **22**, 2031–2063 (2020).
15. Y Guo, D Wang, A Vishwanath, C Xu, Q Li, Towards federated learning for HVAC analytics: A measurement study in *Proceedings of the Eleventh ACM International Conference on Future Energy Systems*. pp. 68–73 (2020).
16. V Venkataramanan, S Kaza, AM Annaswamy, Der forecast using privacy-preserving federated learning. *IEEE Internet Things J.* **10**, 2046–2055 (2022).
17. VJ Nair, P Srivastava, A Annaswamy, Enhancing power grid resilience to cyber-physical attacks using distributed retail electricity markets in *Proceedings of the 2024 IEEE/ACM International Conference on International Conference on Cyber-Physical Systems (ICCPS)*. (IEEE), (2024).
18. TD Hardy, B Palmintier, PL Top, D Krishnamurthy, JC Fuller, HELICS: a co-simulation framework for scalable multi-domain modeling and analysis. *IEEE Access* **12**, 24325–24347 (2024).
19. DP Chassin, K Schneider, C Gerkensmeyer, GridLAB-D: An open-source power systems modeling and simulation environment in *Proceedings of the 2008 IEEE/PES Transmission and Distribution Conference and Exposition*. pp. 1–5 (2008).
20. J Kurtz, R Hovsapian, Aries: Advanced research on integrated energy systems research plan, (National Renewable Energy Lab.(NREL), Golden, CO (United States)), Technical report (2021).
21. P Kundur, *Power system stability*. (CRC Press New York) Vol. 10, (2007).
22. D Olsen, M Sohn, MA Piette, S Kiliccote, Demand Response Availability Profiles for California in the Year 2020, (Lawrence Berkeley National Laboratory (LBNL), Berkeley, CA (United States)), Technical report (2014).
23. VJ Nair, A Annaswamy, Local retail electricity markets for distribution grid services in *Proceedings of the 2023 IEEE Conference on Control Technology and Applications (CCTA)*. (IEEE), pp. 32–39 (2023).

Algorithm 1 Compute reconfiguration pathway

Given total generation G, generation units $\mathcal{G}_i = \{G_1, G_2, \ldots, G_i\}$, total load L, load nodes $\mathcal{L}_i = \{L_1, L_2, \ldots, L_i\}$, graph network, switch settings, $\mathcal{S}_i = \{S_1, \ldots, S_n\}$
while $G < L$, **do**
  for Load L_i in $\mathcal{L}_i$ **do**
    Find shortest path $path_i$ to generation units $\mathcal{G}_i$
    Sort paths based on electrical distance in the ascending order
  end for
  Find leaf nodes $\mathcal{L}_i^n$ in $\mathcal{L}_i$
  for all $\mathcal{L}_i^n$ **do**
    Find next node in $path_i$ j to $\mathcal{G}_i$
    $TotalLoss = TotalLoss + PowerLossInPath$
    Update $\mathcal{L}_i^n$ to j
    if Leaf nodes $\mathcal{L}_i^n$ is empty **then**
      break
    end if
  end for
end while
for all *paths* **do**
  If there is a $\mathcal{S}_i$ in path, then assign $\mathcal{S}_i == 1$
  if *path* is a tree **then**
    Break
  else
    Adjust $\mathcal{S}_i$ for *path* to return to tree structure
  end if
end for
Update $\mathcal{G}_{i+1} = \{G_1, G_2, \ldots, G_{i+1}\}$
Update $\mathcal{S}_i = \{S_1^0, \ldots, S_n^0\}$
Compute resiliency metric at the primary level PNR for the switch setting $\mathcal{S}_N$.
Implement the *path* with the highest PNR.

Fig. S10. Resilience-based reconfiguration algorithm.

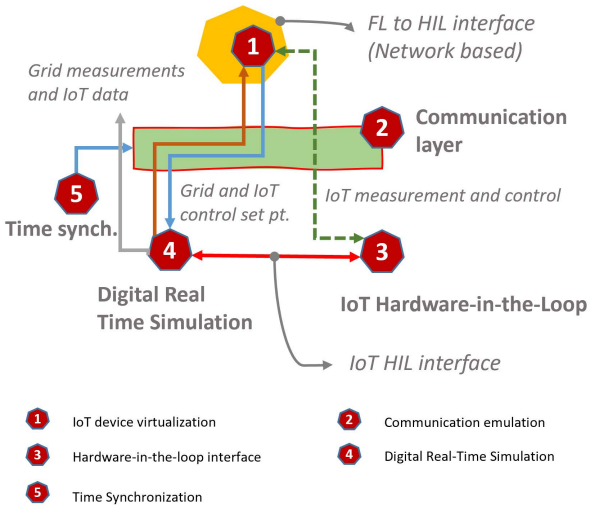


Fig. S11. ARIES-DRTS Validation Platform at NREL

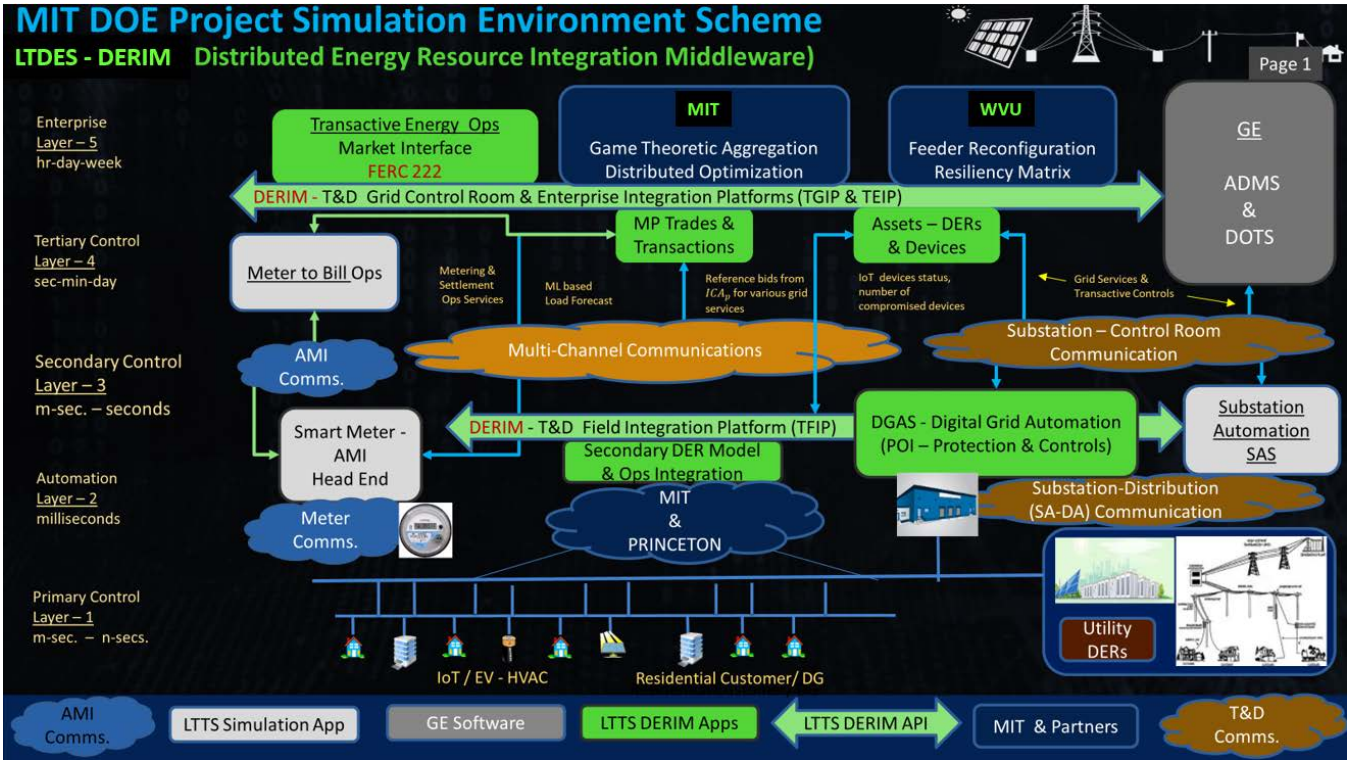


Fig. S12. DERIM interface with ADMS-DOTS in the LTDES validation platform.

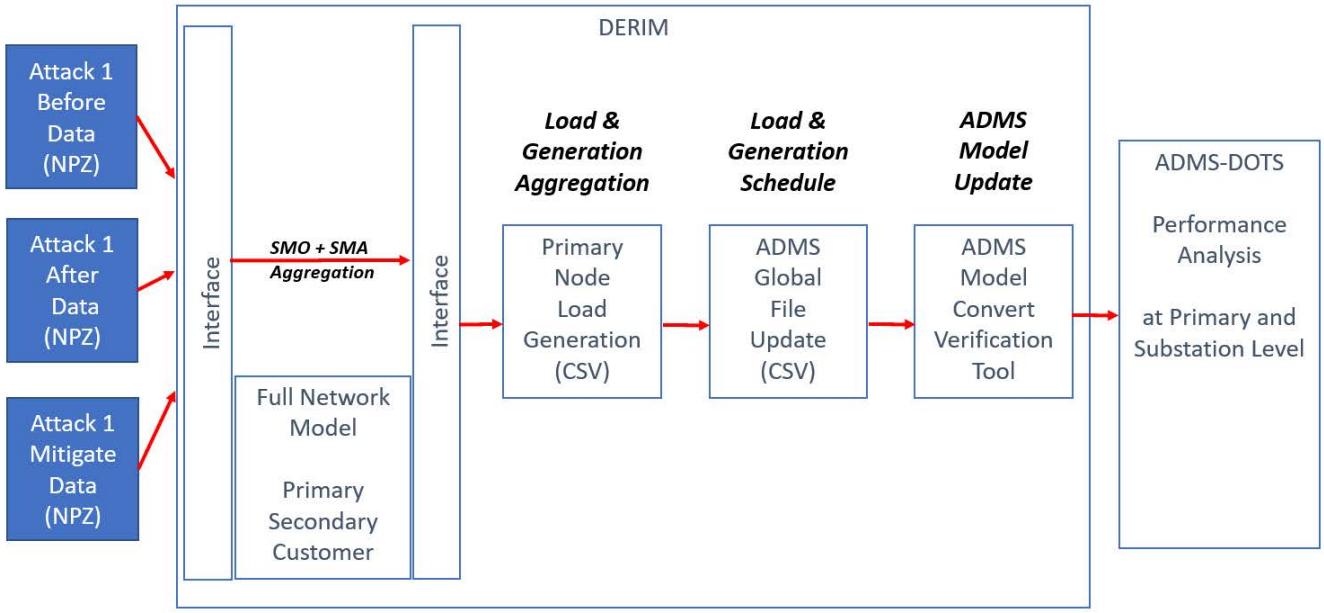


Fig. S13. Attack 1a validation process workflow in the LTDES validation platform with DERIM and ADMS-DOTS.

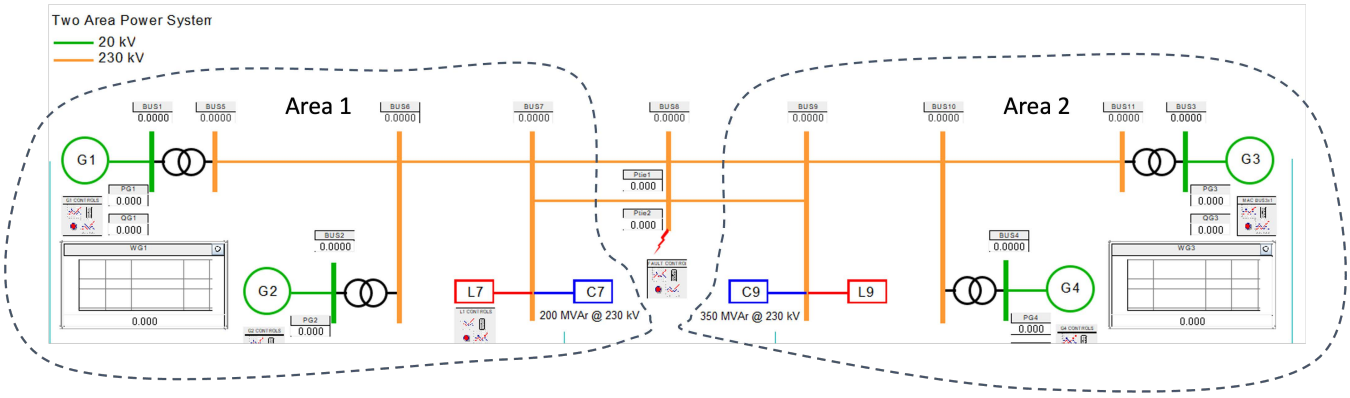
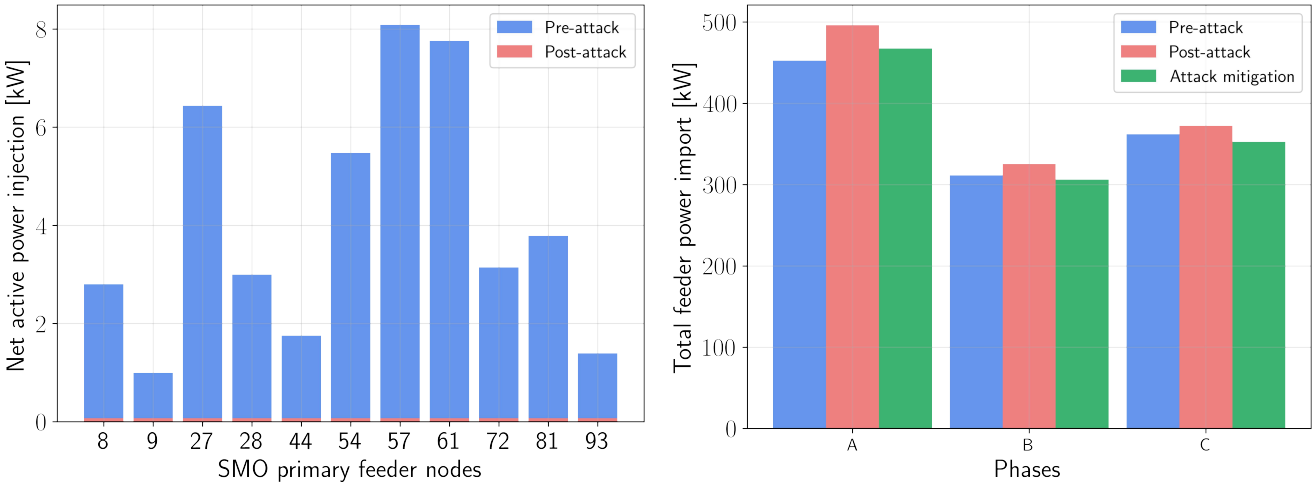


Fig. S14. Schematic of Kundur 2-area power system



(a) Generation with and without attack 1b.

(b) Feeder power import.

Fig. S15. Effects of attack 1b on SMO net generation and power import.

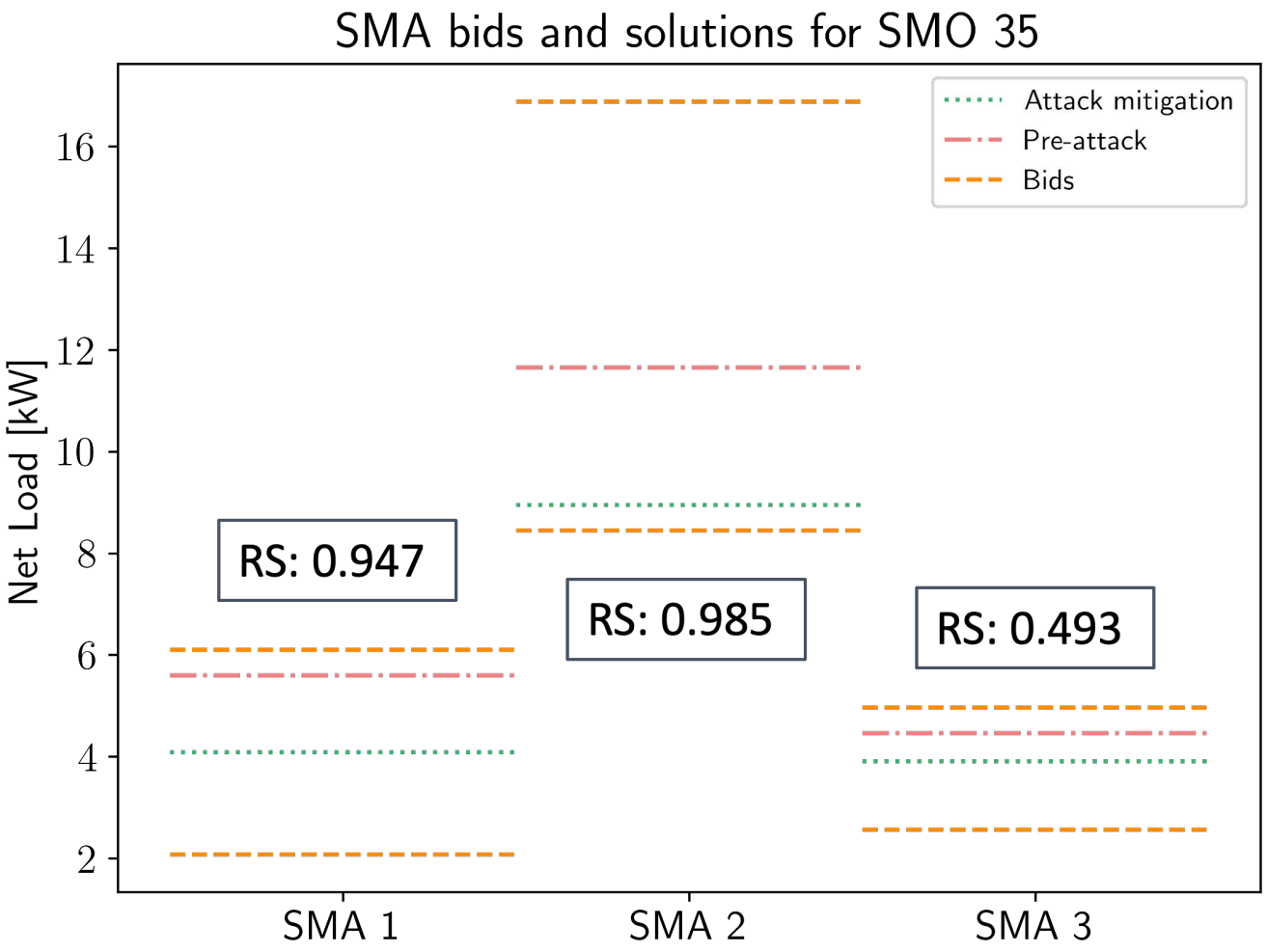


Fig. S16. Dis-aggregation of changes in the setpoints for SMO (from the PM) at node 35 across its 3 SMAs (in the SM), resulting from attack 1b mitigation, along with each SMA's RS. All 3 SMAs are on phase A.

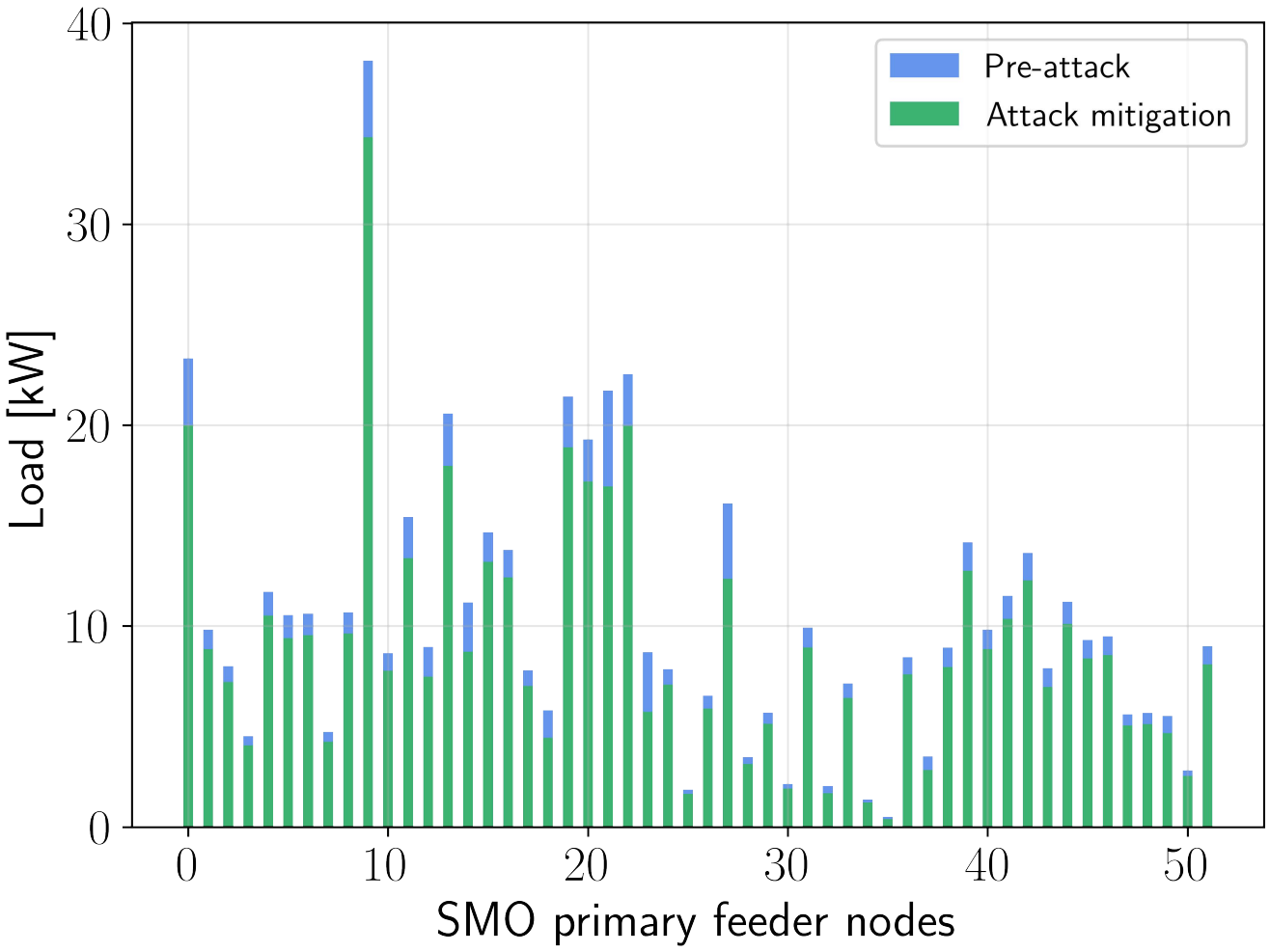


Fig. S17. Curtailment of flexible loads for attack 1b mitigation.

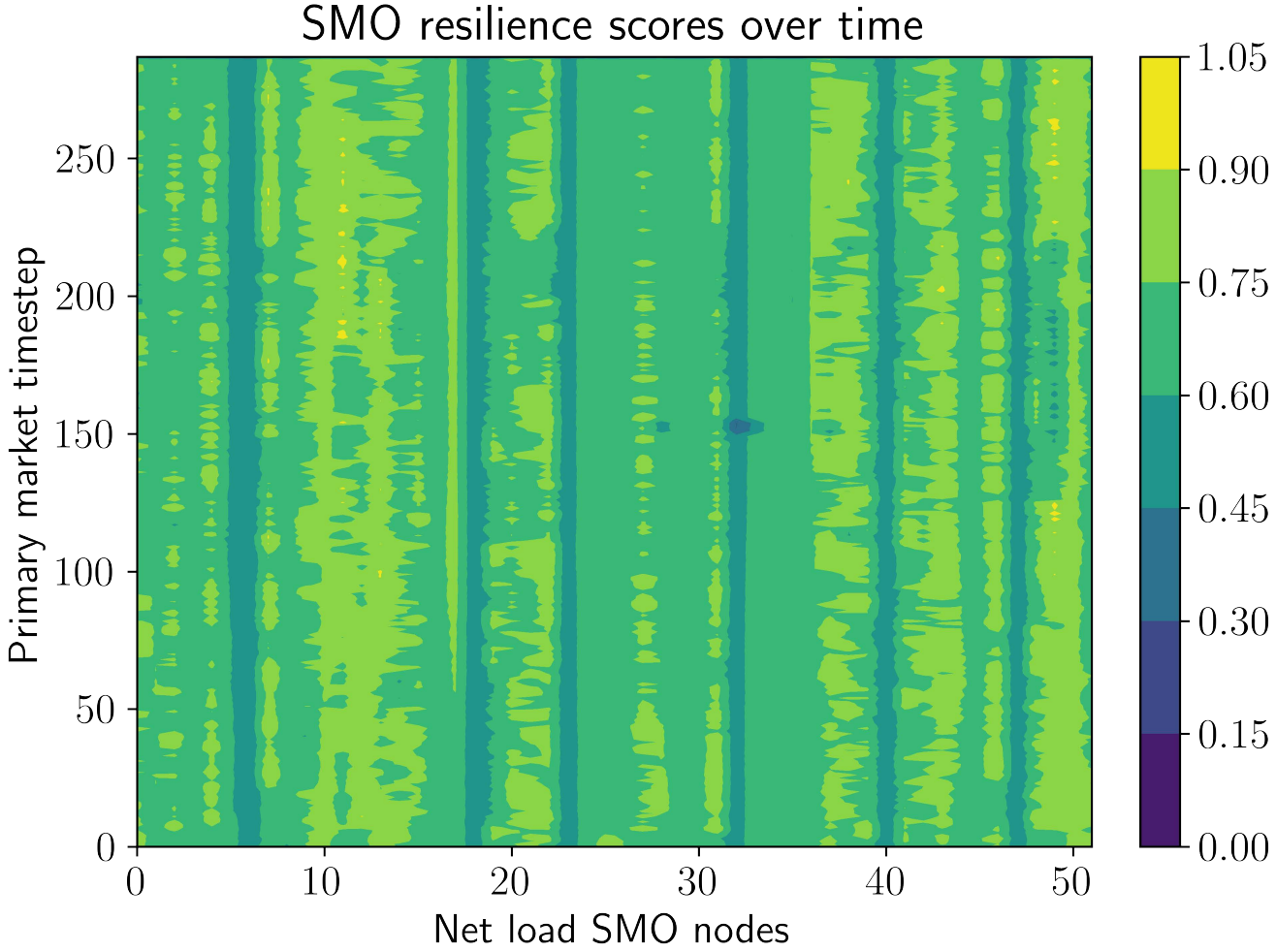
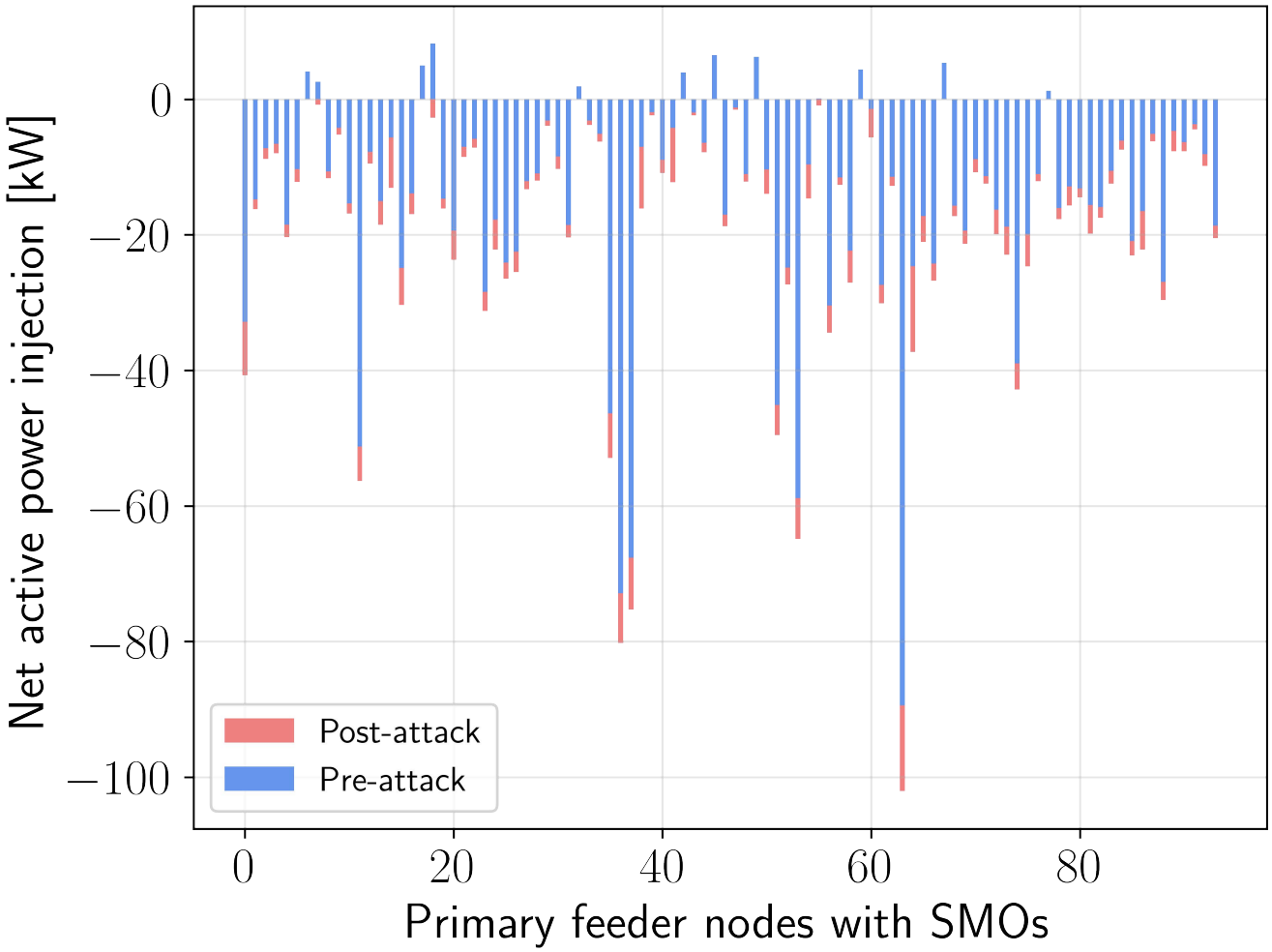
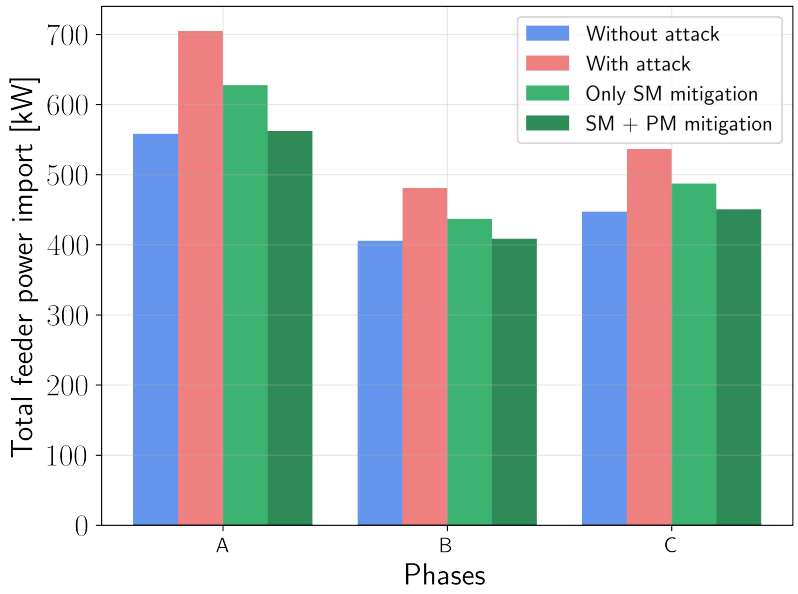


Fig. S18. Locational-temporal trends of RS across all flexible SMO nodes and over the whole simulation period of 24h.



(a) SMO injections.



(b) 3-phase power imports from the main grid.

Fig. S19. Effects of attack 1c on SMO injections and power import.

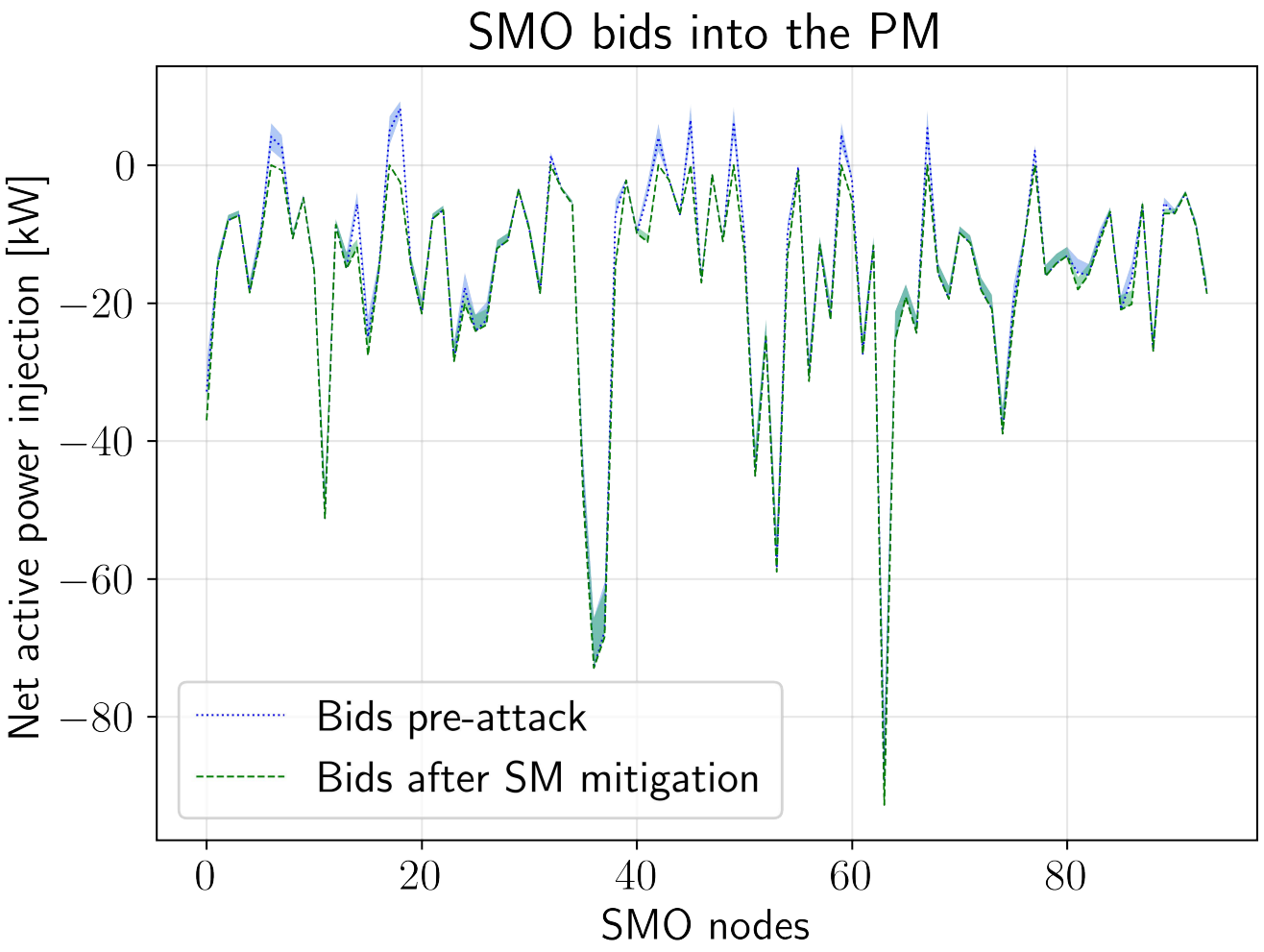


Fig. S20. Comparison of SMO flexibility bids into the PM before and after the attack. The dashed and dotted lines indicate the baseline values while the shaded regions are the flexibility bids around the baseline.

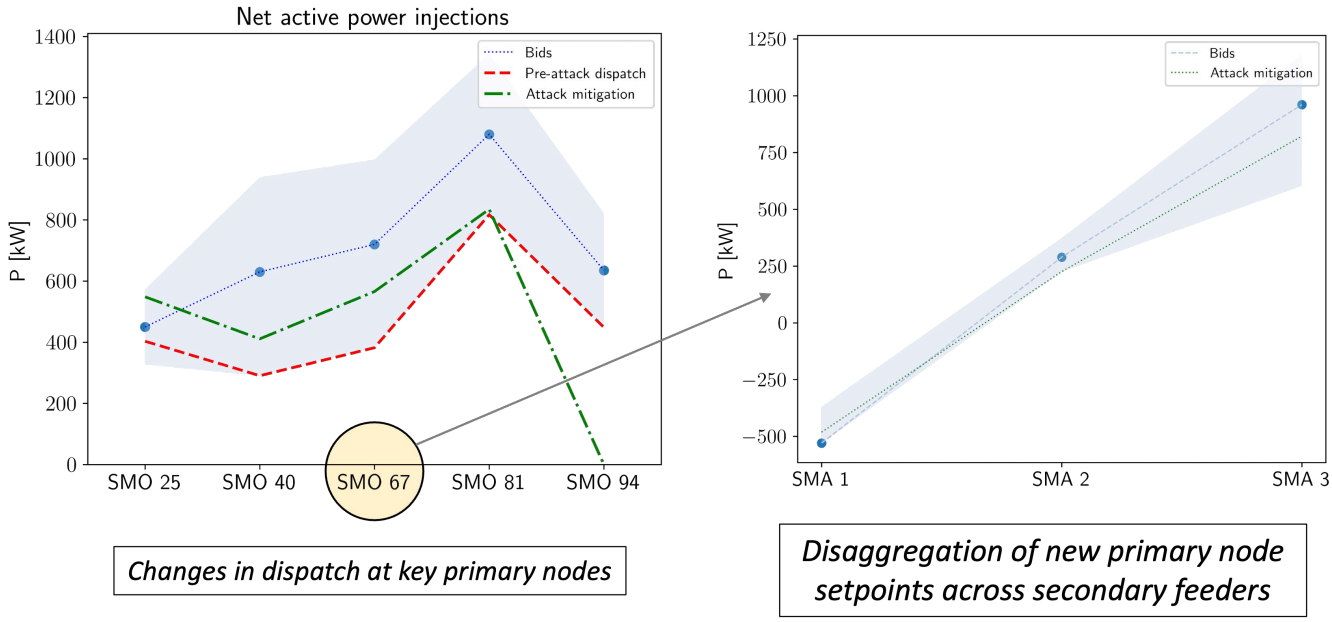


Fig. S21. Mitigation of small-scale attack 2a. Image Credit: Reprinted with permission from (17).

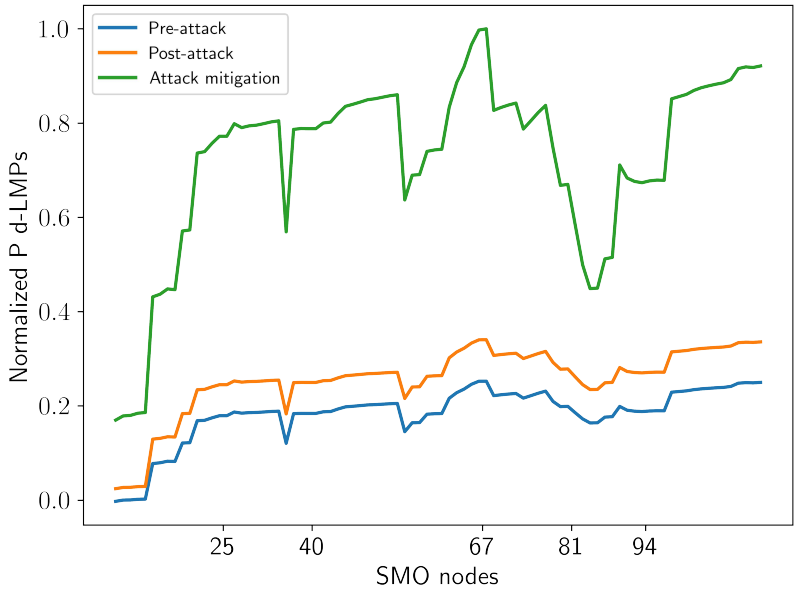


Fig. S22. Effects of large-scale attack and mitigation on nodal d-LMPs at SMO nodes. Image Credit: Reprinted with permission from (17).

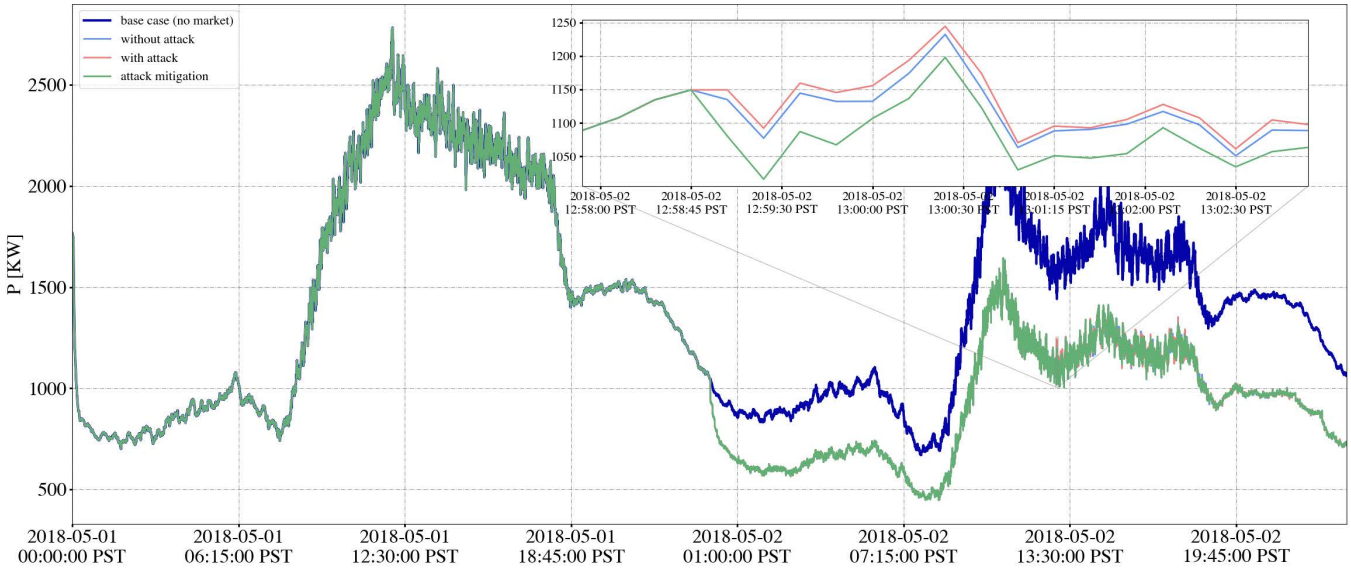


Fig. S23. Validation of attack 1a mitigation effects of the EUREICA framework using HELICS, showing system load over 48 hours.

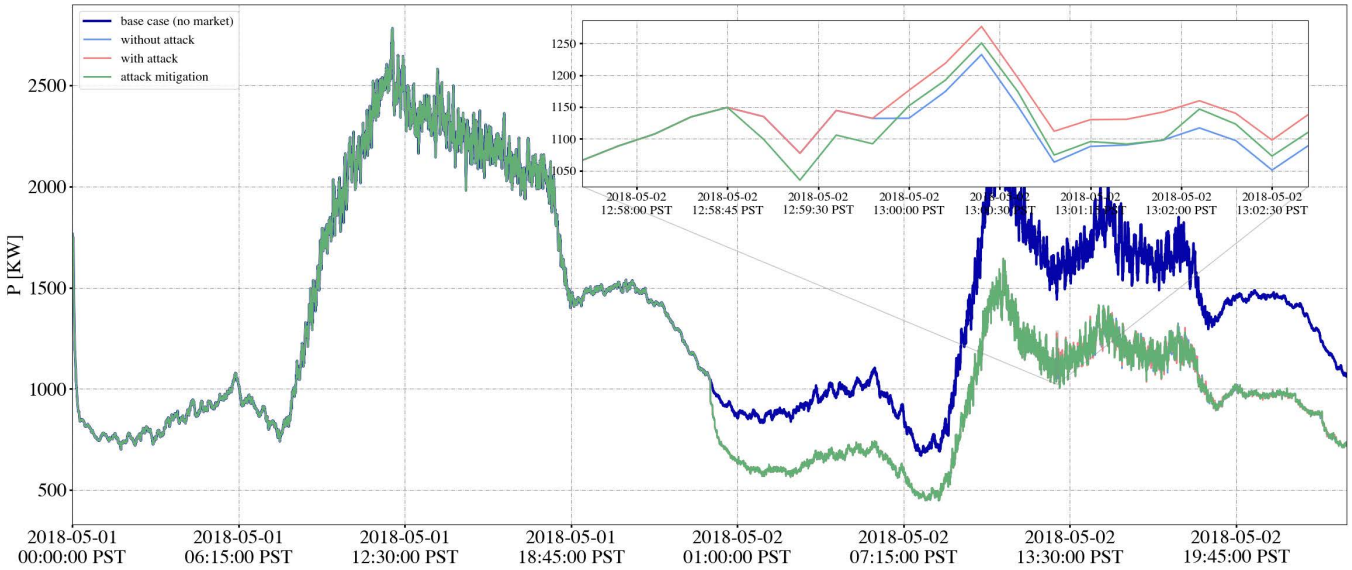


Fig. S24. Validation of attack 1b mitigation effects of the EUREICA framework using HELICS, showing system load over 48 hours.

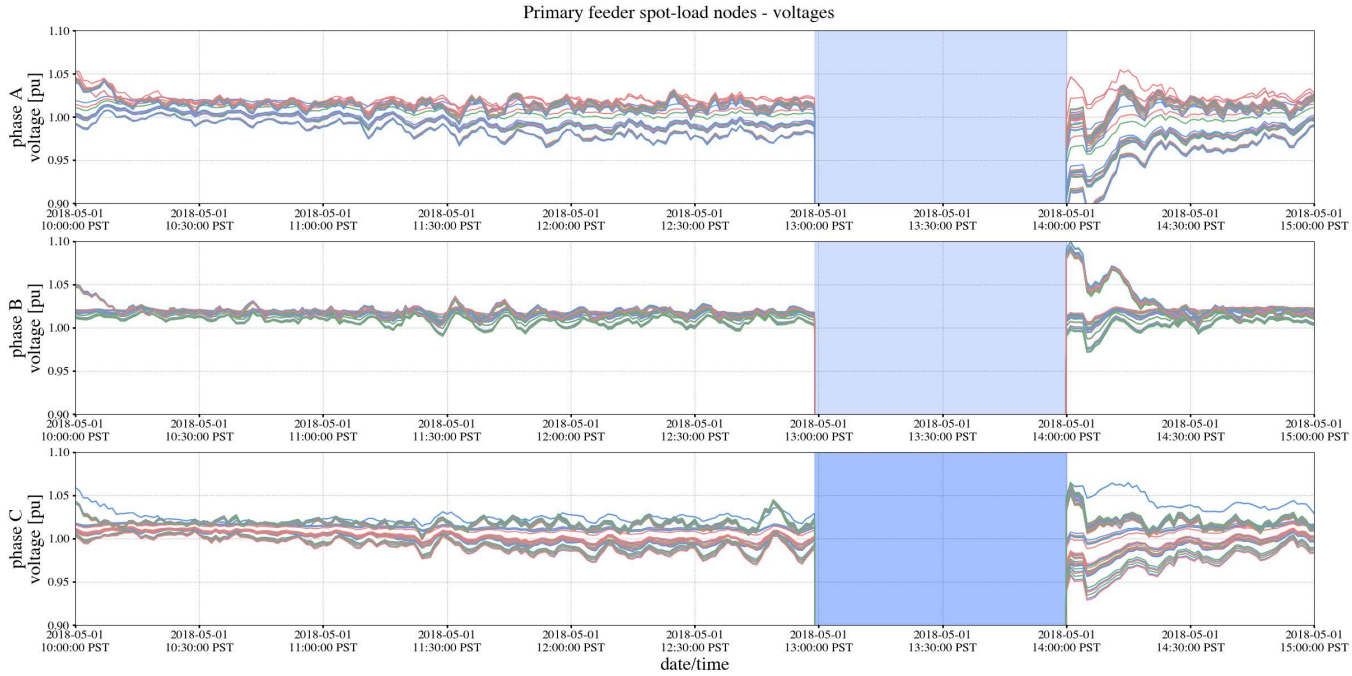


Fig. S25. Black-out as a result of distribution system islanding in attack 3.

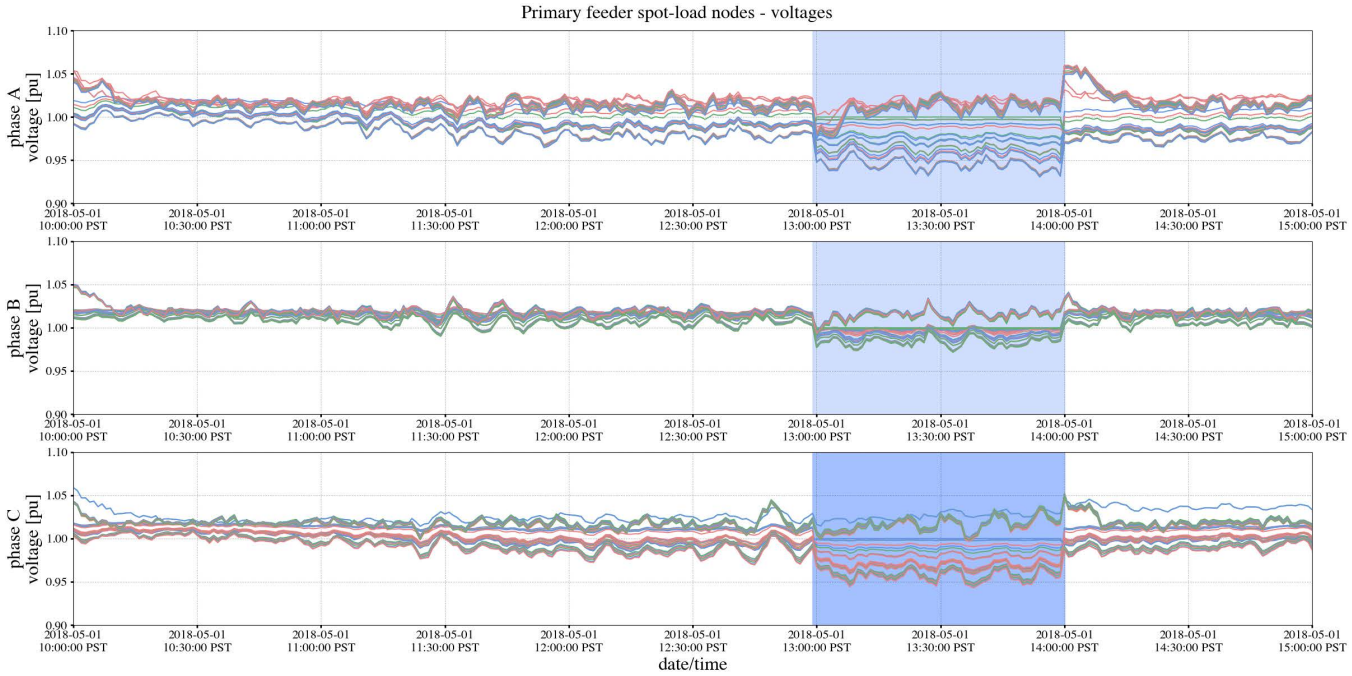


Fig. S26. Voltage recovery after engaging diesel generators during attack 3.

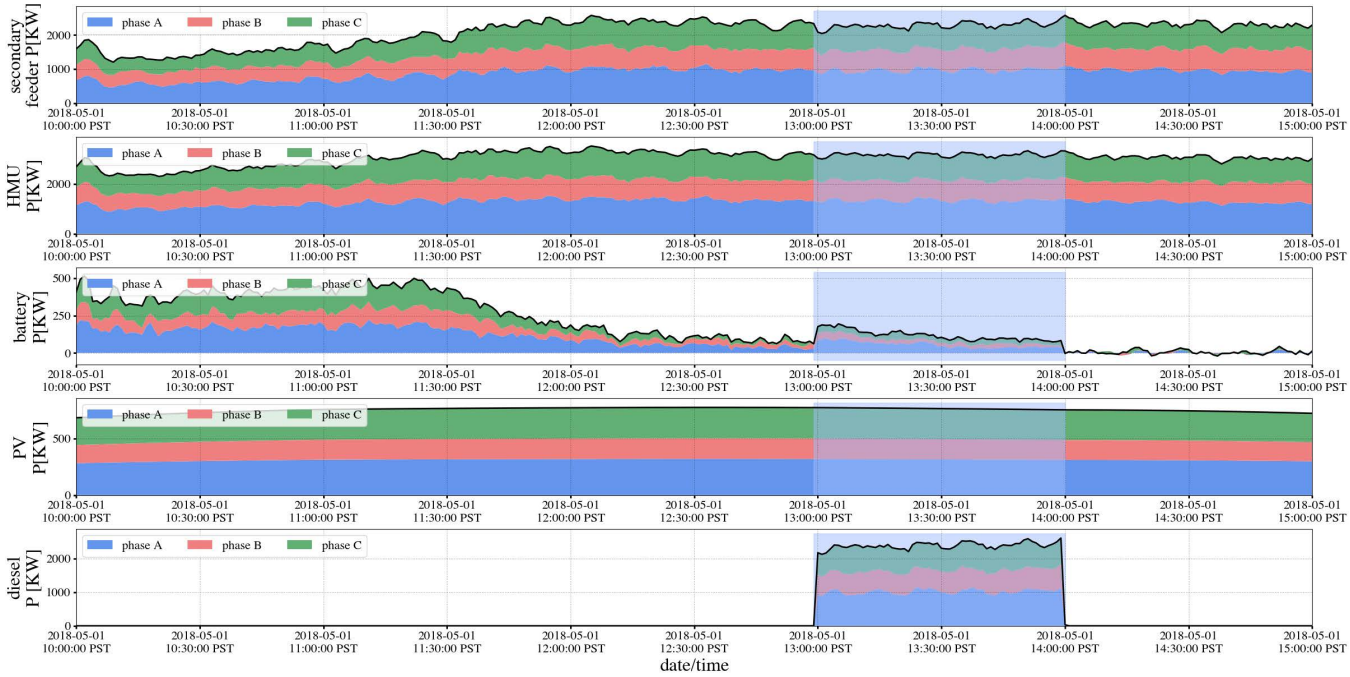


Fig. S27. Demand and distributed generation without resilience-based reconfiguration during attack 3.

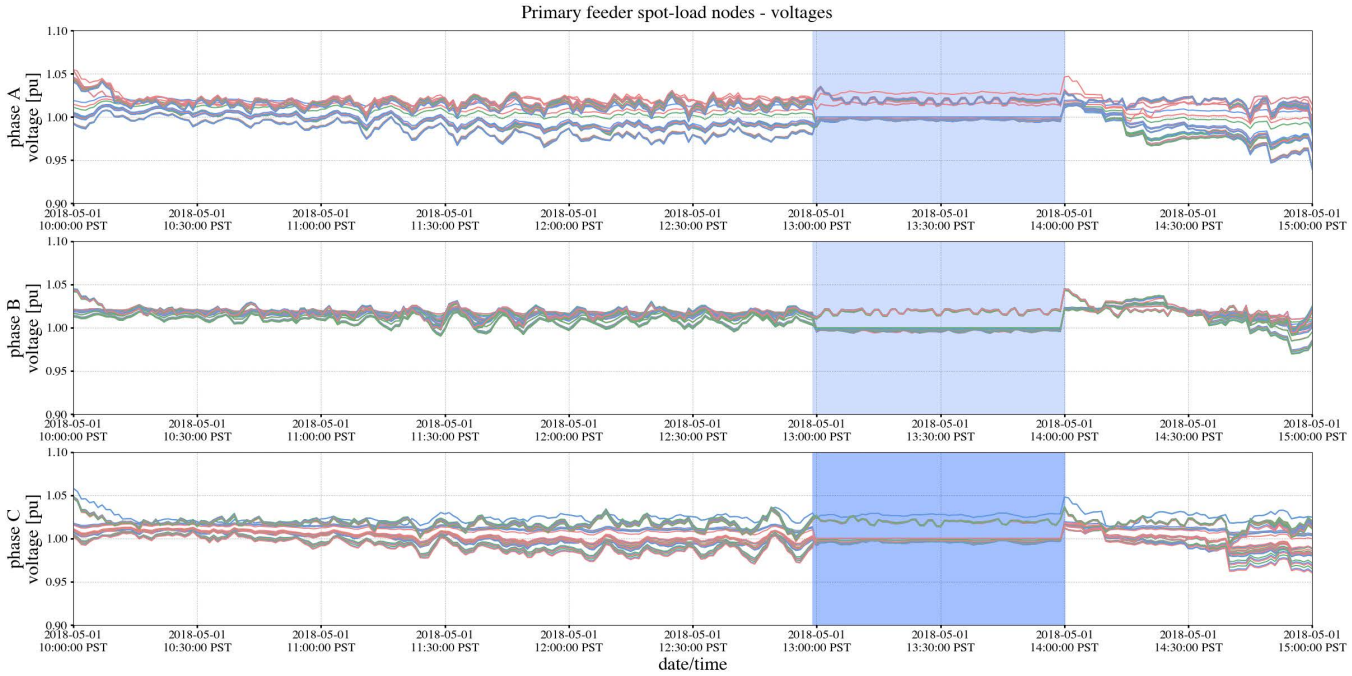


Fig. S28. Voltage recovery after resilience-based reconfiguration during attack 3.

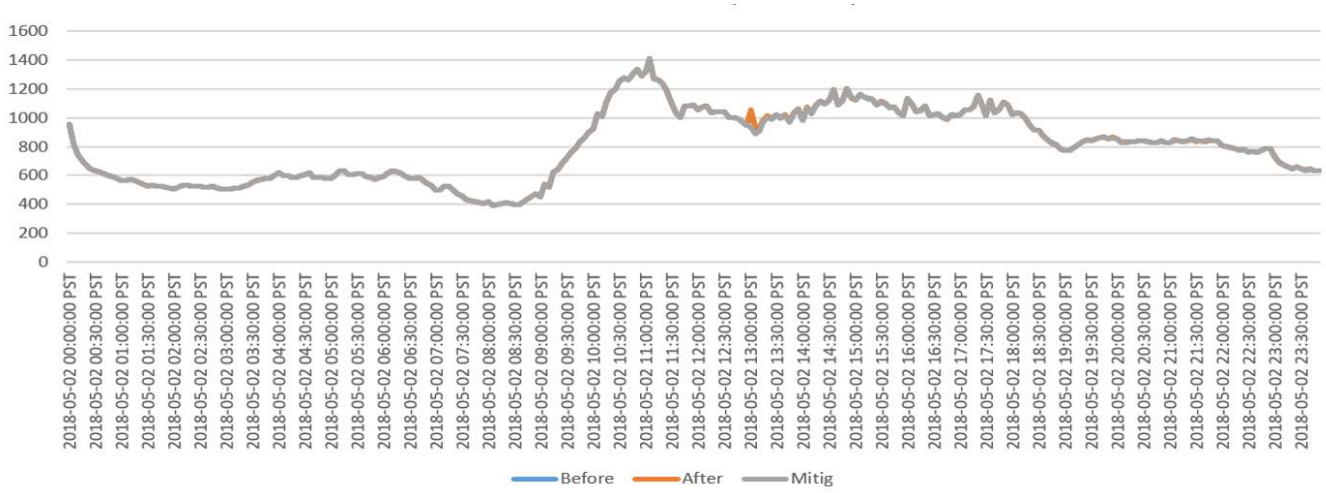


Fig. S29. Effects of attack 1a on total load at feeder head over 24 h.

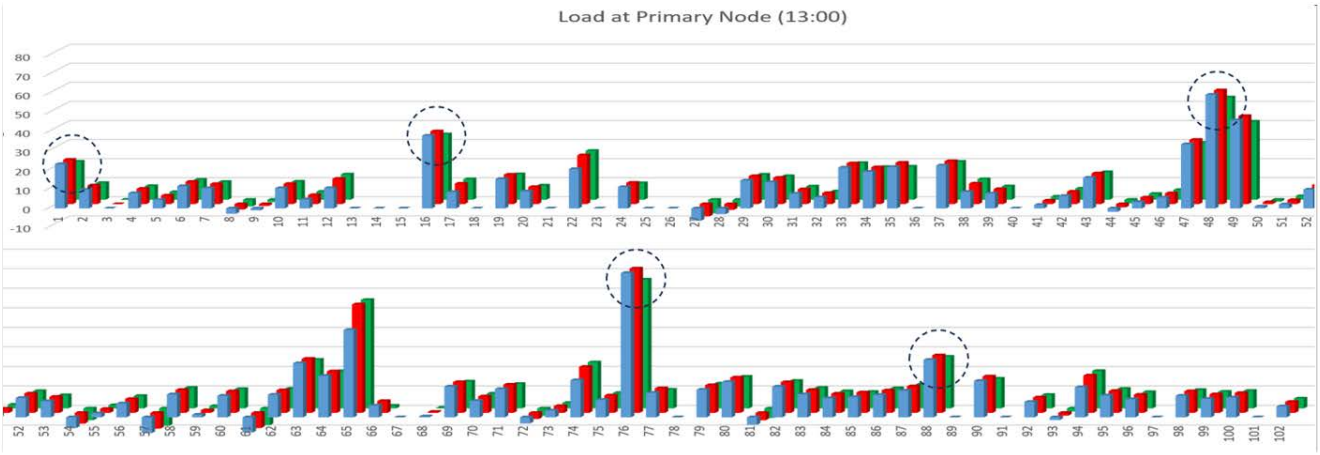


Fig. S30. Load change at primary nodes during attack 1a. The values (i) without attack, (ii) with attack, and (iii) with attack mitigation are shown in the blue, red, and green bars, respectively. The SMO nodes providing the most flexibility are circled.

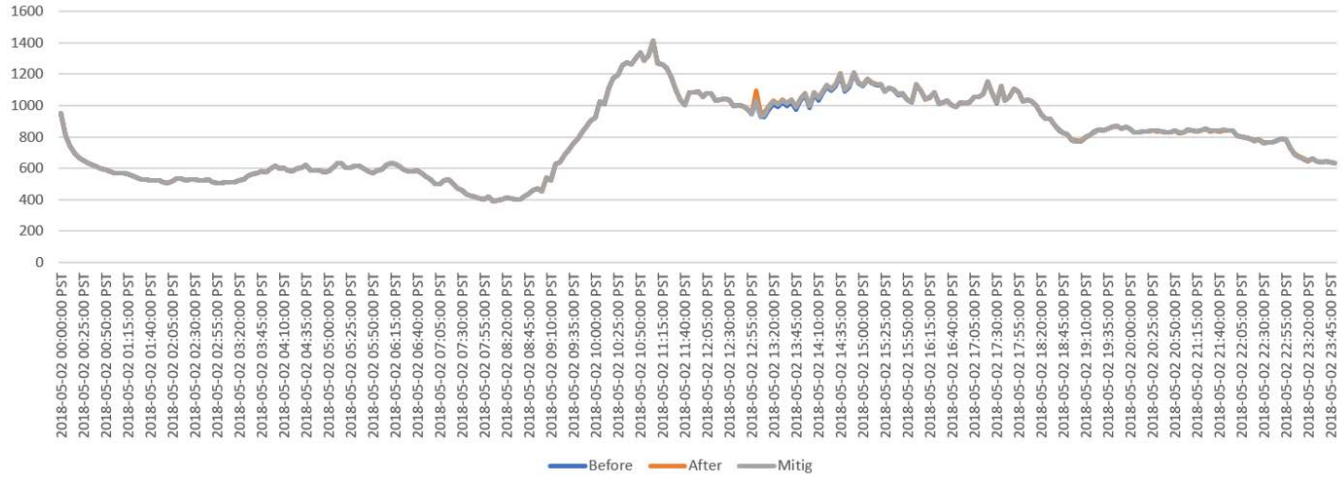


Fig. S31. Effects of attack 1b on the total load at the feeder head over 24 h.

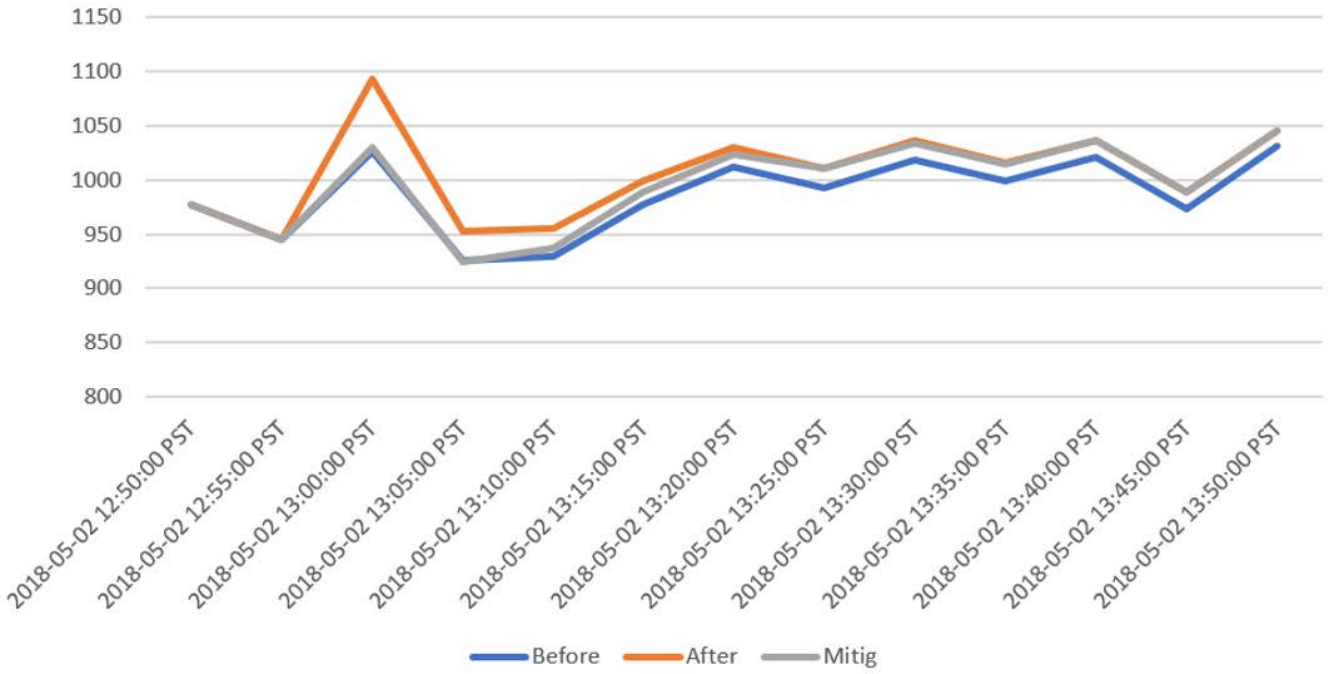


Fig. S32. LTDES validation of attack 1b in the DERIM-ADMS platform, showing total power import at the substation around the attack time at 13:00.

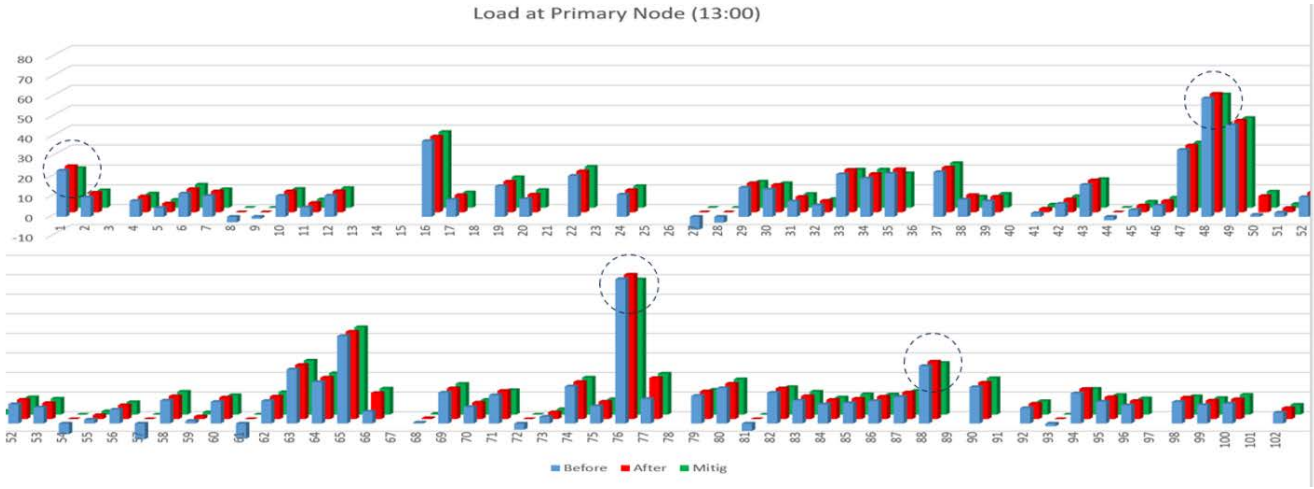


Fig. S33. Load change at primary nodes during attack 1b. The values (i) without attack, (ii) with attack, and (iii) with attack mitigation are shown in the blue, red, and green bars, respectively. The SMO nodes providing the most flexibility are circled.

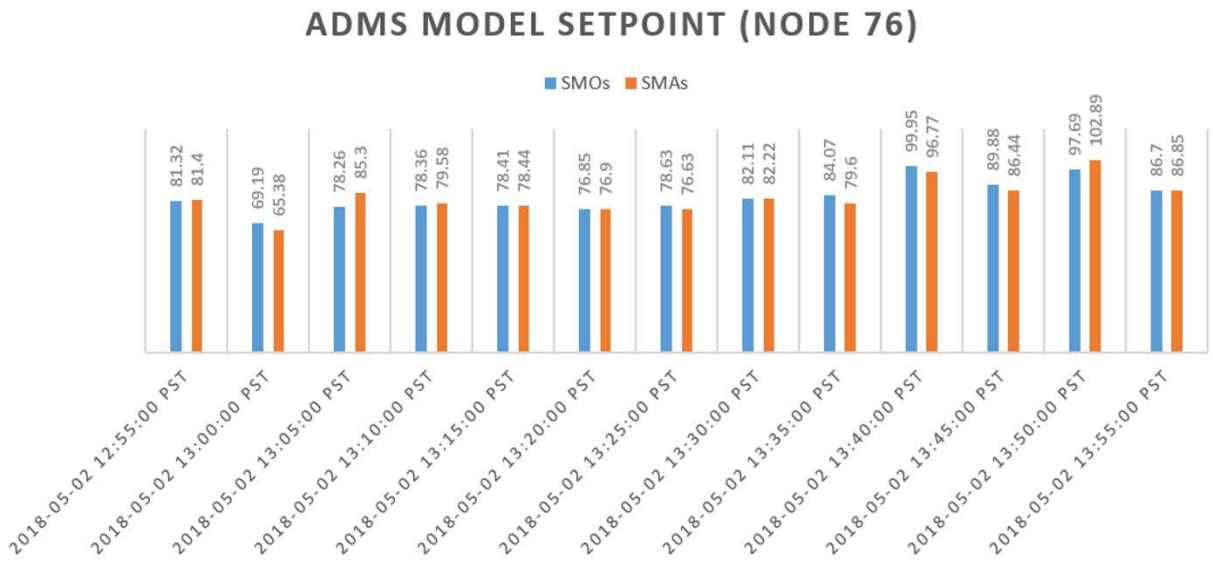


Fig. S34. Forecasted values of SMO and SMA setpoints at primary node 76 during attack 1b mitigation.

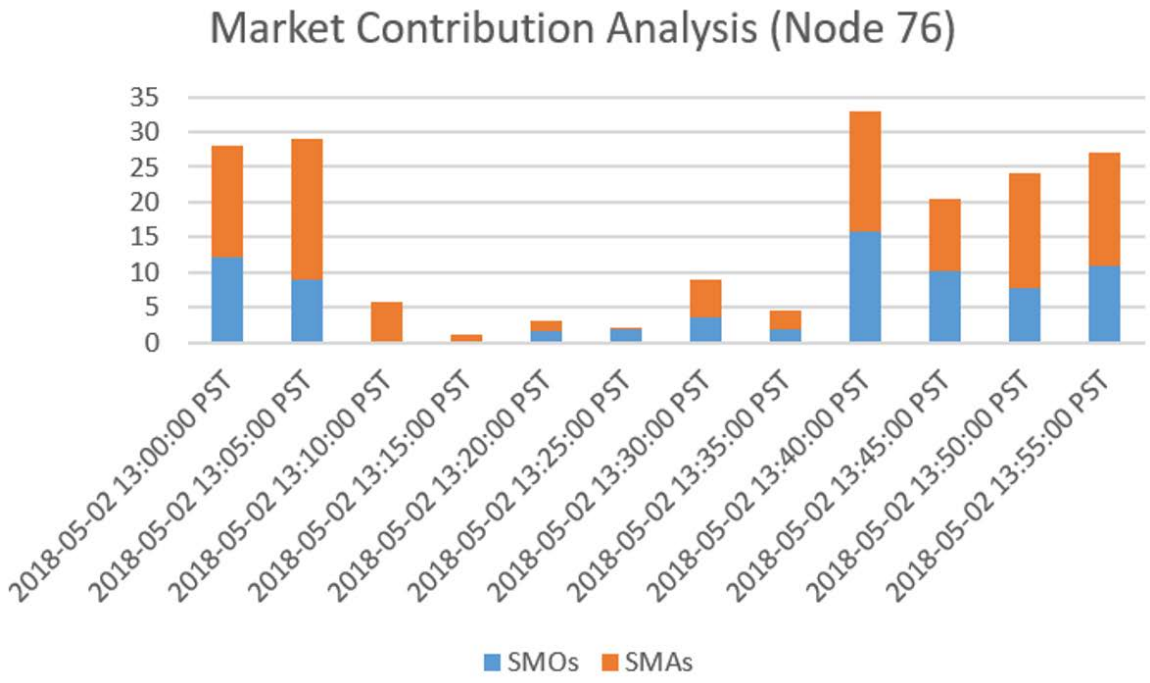
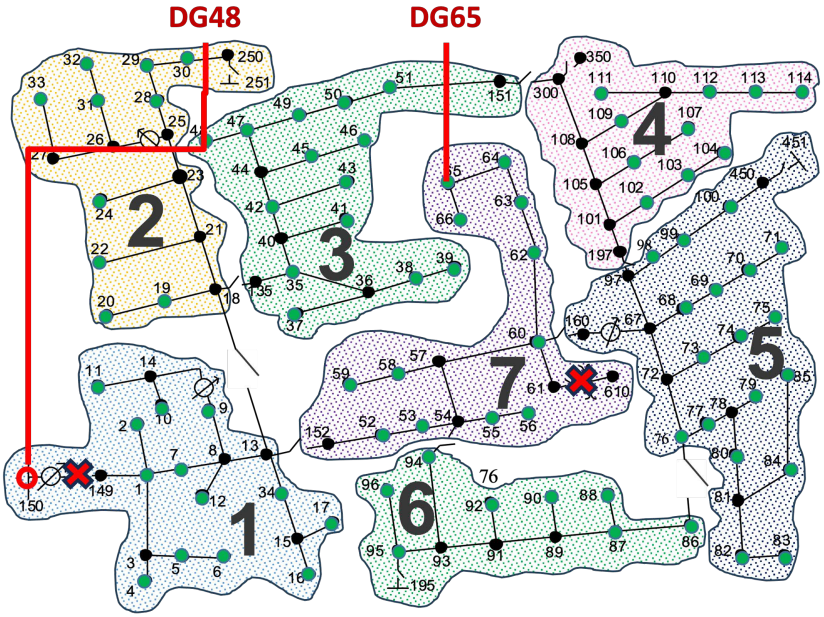


Fig. S35. Comparison of forecasted changes in SMO and SMA setpoints due to attack 1b mitigation.



SWITCH	STATE
150-149	OPEN
61-610	OPEN

JUMP	STATE
150-48	CONNECTED

DG	STATE
DG48/65	CONNECTED

1. Islanding happens at 13:00 and ends at 14:00
2. DG 48 can output up to 270 kW
3. DG 65 can output constant 15 kW
4. Using Node 150 as swing node

Fig. S36. Switch setting changes and network reconfiguration in the case when there are critical loads throughout the feeder.

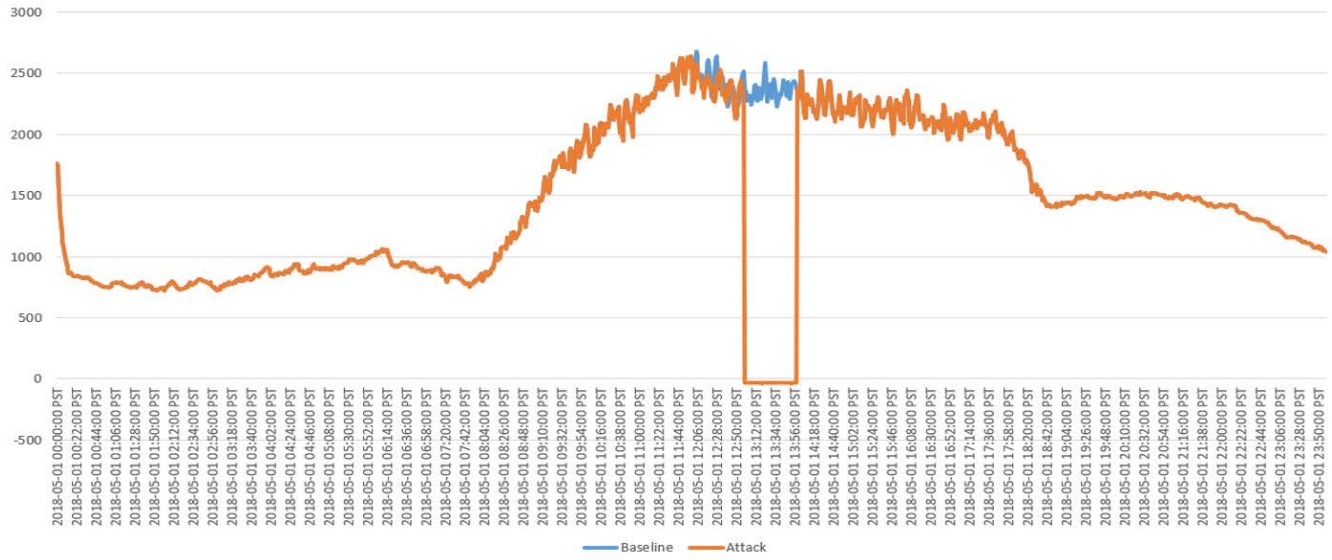


Fig. S37. Total feeder head load over 24 h simulation, when there are critical loads throughout the feeder.

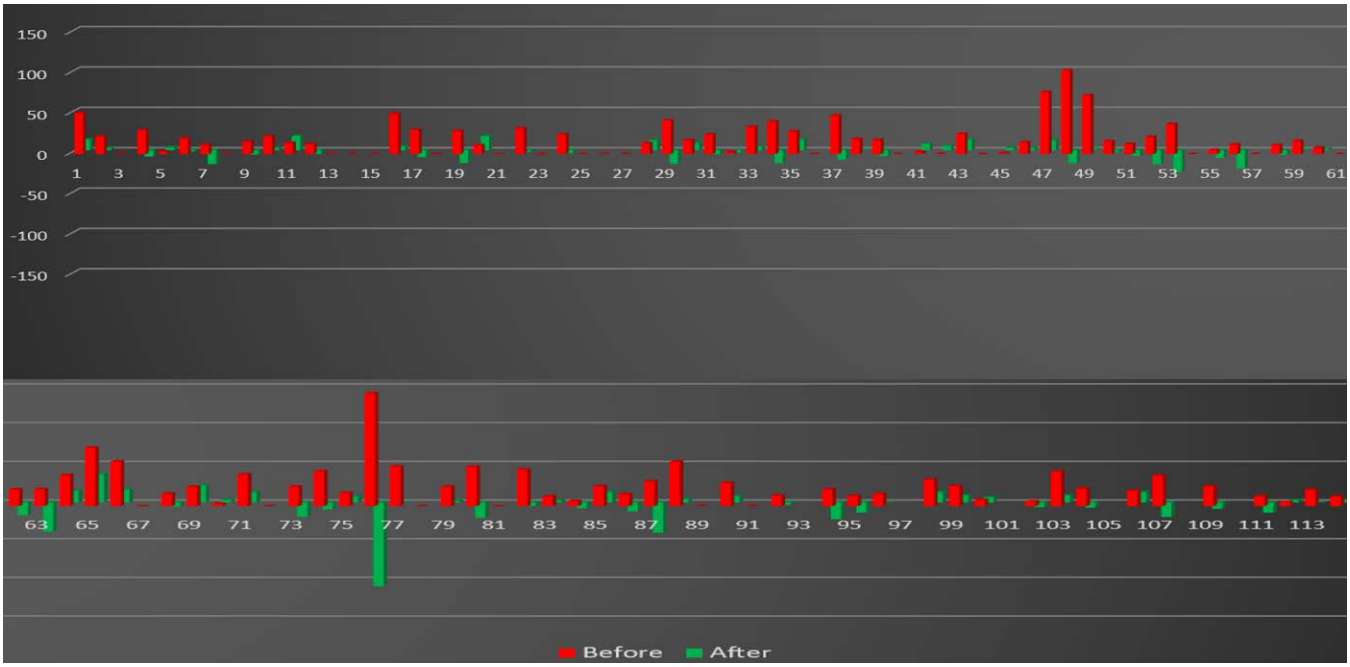
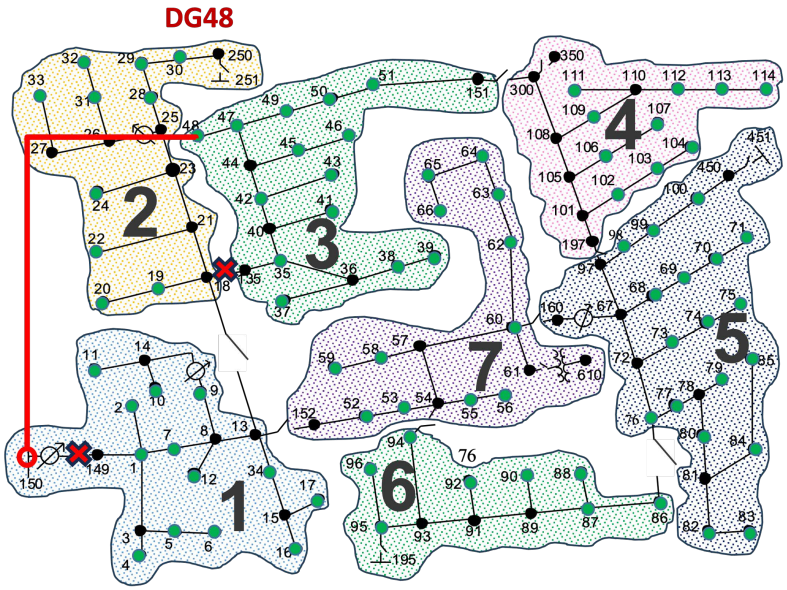


Fig. S38. Primary node load change during attack 3 between 12:59 and 13:00 PST, when there are critical loads throughout the feeder.



SWITCH	STATE
150-149	OPEN
18-135	OPEN

JUMP	STATE
150-48	CLOSED

DG	STATE
DG48	CONNECTED

1. Islanding happens at 13:00 and end at 14:00
2. Switch 18-135 open to create an microgrid
3. DG 48 has enough generation capacity to maintain region 3 load

Fig. S39. Attack 3 case where critical loads are only located in zone 3 as a microgrid.

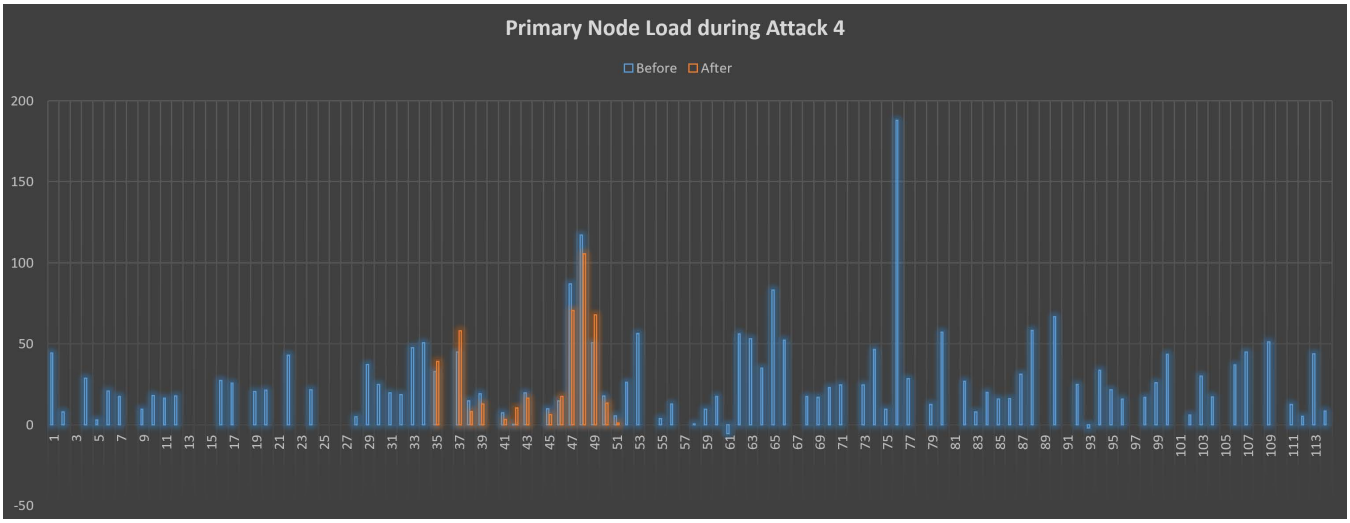


Fig. S40. Primary node load change during attack 3 between 12:59 and 13:00 PST, when critical loads are only located in zone 3 as a microgrid.

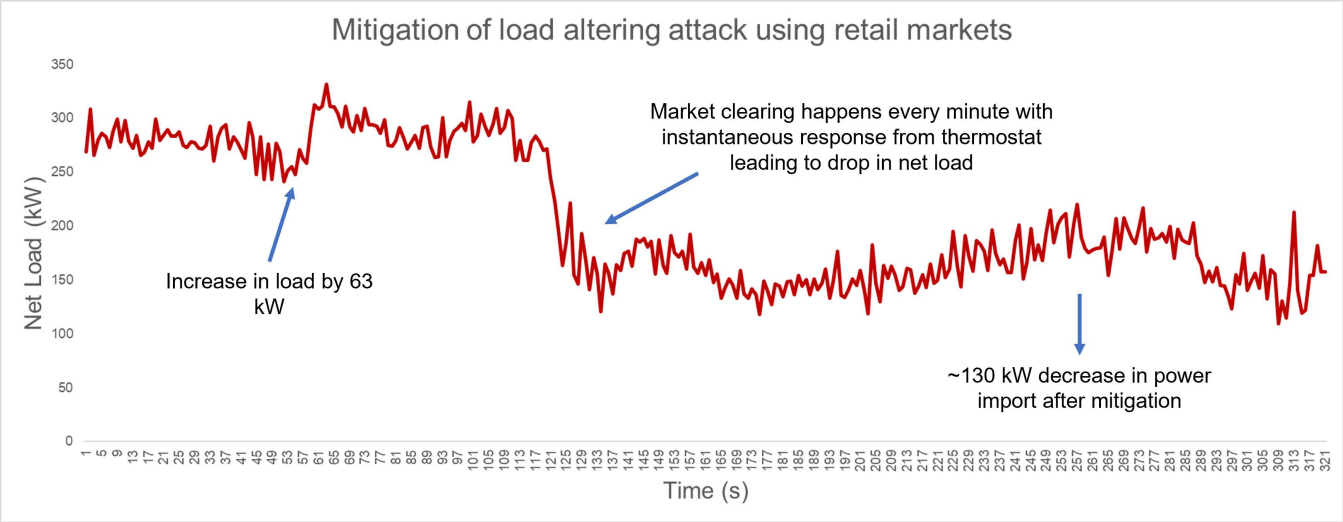


Fig. S41. Implementation of market services to mitigate load increase in attack 1a.

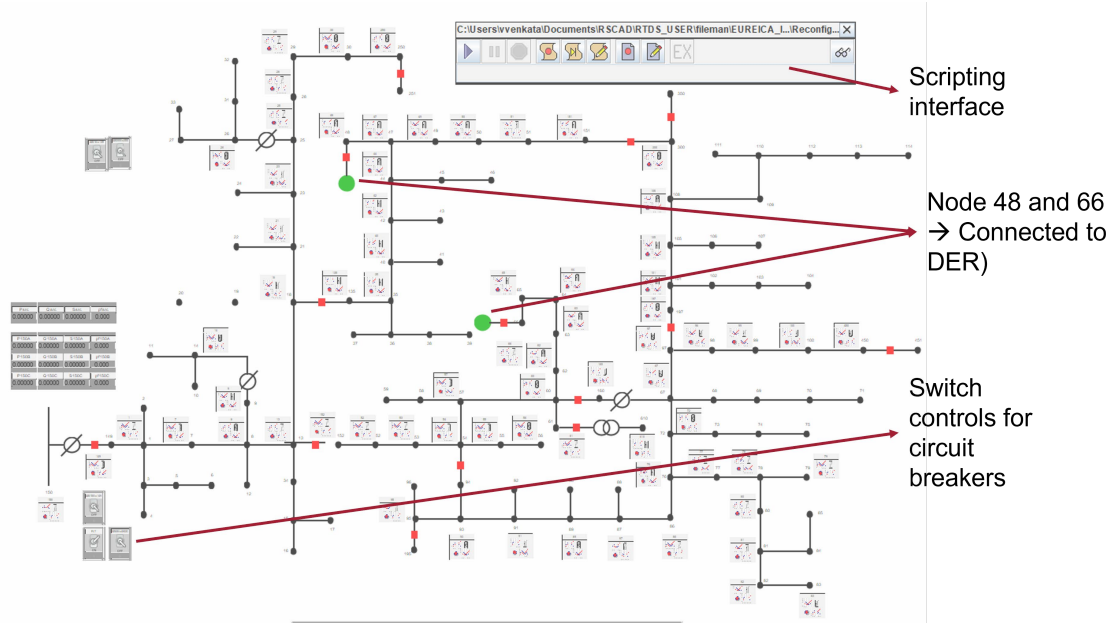


Fig. S42. Implementation of reconfiguration algorithm in RTDS.

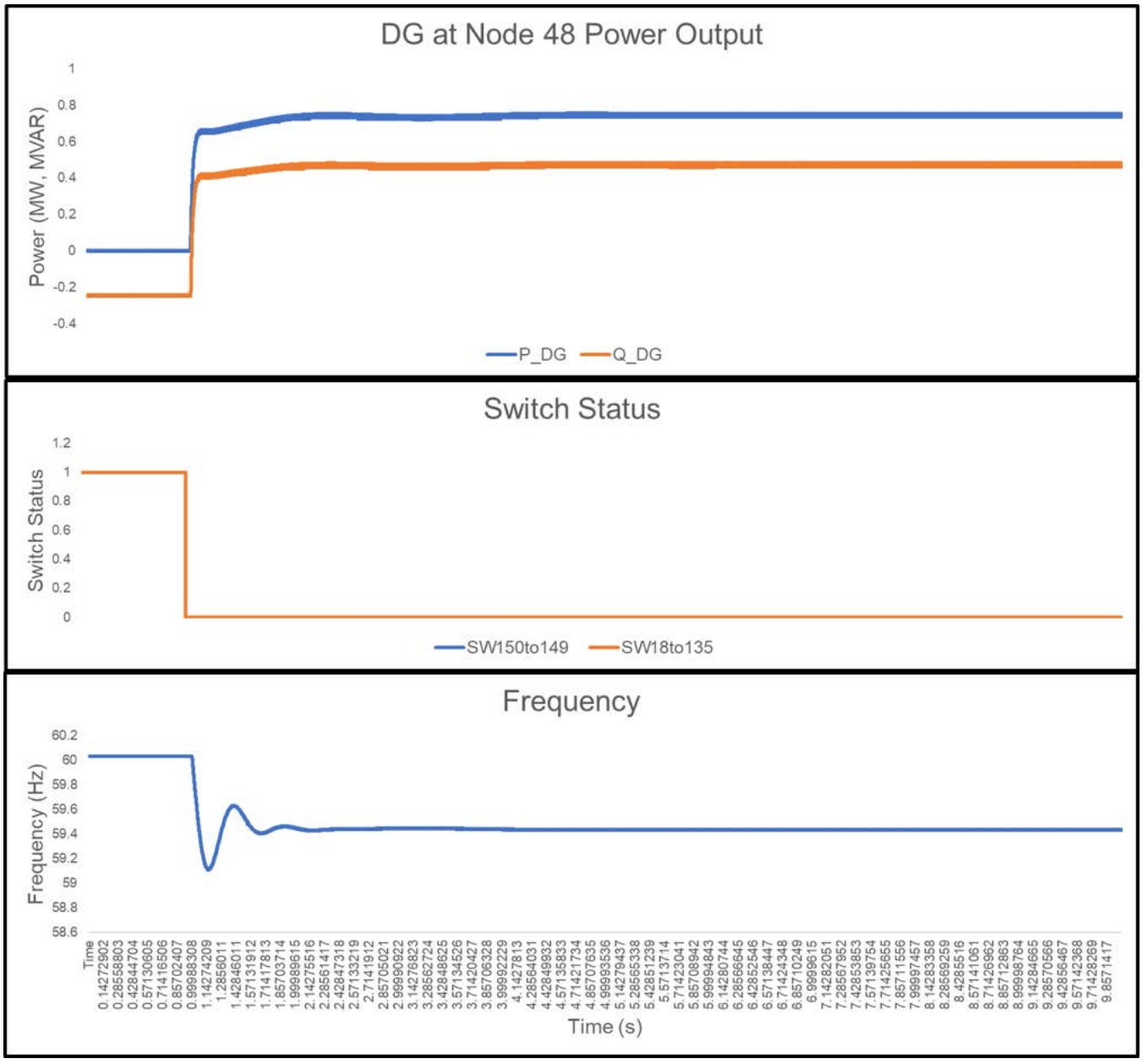


Fig. S43. Distribution feeder broken into islands, with only Zone 3 load restored by DG at Node 48.