PNAS RESEARCH ARTICLE | ENGINEERING

Resilience of the electric grid through trustable IoT-coordinated assets

Vineet J. Nair[a,1], Priyank Srivastava[b], Venkatesh Venkataramanan[c], Partha S. Sarker[d], Anurag Srivastava[d], Laurentiu D. Marinovici[e], Jun Zha[f], Christopher Irwin[g], Prateek Mittal[h], John Williams[i], Jayant Kumar[f], H. Vincent Poor[h,1], and Anuradha M. Annaswamy[a]

Affiliations are included on p. 12.

Contributed by H. Vincent Poor; received July 28, 2024; accepted November 25, 2024; reviewed by Jalal Kazempour and John D. McDonald

The electricity grid has evolved from a physical system to a cyberphysical system with digital devices that perform measurement, control, communication, computation, and actuation. The increased penetration of distributed energy resources (DERs) including renewable generation, flexible loads, and storage provides extraordinary opportunities for improvements in efficiency and sustainability. However, they can introduce new vulnerabilities in the form of cyberattacks, which can cause significant challenges in ensuring grid resilience. We propose a framework in this paper for achieving grid resilience through suitably coordinated assets including a network of Internet of Things devices. A local electricity market is proposed to identify trustable assets and carry out this coordination. Situational Awareness (SA) of locally available DERs with the ability to inject power or reduce consumption is enabled by the market, together with a monitoring procedure for their trustability and commitment. With this SA, we show that a variety of cyberattacks can be mitigated using local trustable resources without stressing the bulk grid. Multiple demonstrations are carried out using a high-fidelity cosimulation platform, real-time hardware-in-the-loop validation, and a utility-friendly simulator.

grid resilience | Internet of Things | local electricity market | distributed energy resources | power grid

Significance

This paper provides a framework for achieving power grid resilience against cyberphysical attacks through the coordination of resources at the grid edge that are trustable and resilient. It is proposed that such coordination can be enabled through a suite of market operators suitably located in a distribution grid. We use this coordination to validate the mitigation of attacks of different levels of severity, with attack magnitudes that range from 5 to 40% of the total peak load. Both grid-connected and islanded cases are studied. In all cases, we show that grid resilience can be obtained through a combination of locally available flexible assets and reconfiguration of the grid topology.

The electricity grid is going through a rapid transformation in an effort toward deep decarbonization. Large synchronous generators powered by fossil fuels such as oil, natural gas, and coal are being phased out in favor of solar and wind-based generation. While the latter enables the necessary move toward a reduced carbon footprint, it brings two major challenges in ensuring reliable and resilient delivery of electricity to the end-user. The first of these is the temporal signature of these renewables—the amount of generation varies with time, both in terms of intermittency and uncertainty. The second is that these are distributed and large in number. A strong enabler of the scale of the distributed energy resources (DERs) is Internet of Things (IoT), which denotes a network of physical devices such as water heaters (WHs), air-conditioners, and electric vehicles (EVs), as they enable automated and fast operation of various loads. And their pervasiveness brings in complexities of heterogeneity, decentralization, and scale. In order to ensure the reliability of the grid despite these challenges, a precise coordination of these DERs, both in space and time, has to be carried out. In particular, power balance of generation and consumption has to be ensured at all locations and at each instant. These challenges are being overcome using a pervasive cyber layer that senses, communicates, coordinates, and enables the requisite power injection and consumption throughout the grid.

In addition to reliability, an essential property of the electricity grid is resilience (1). This central property, which denotes the ability of the grid to withstand and recover quickly to supply critical loads following a major disruption, such as an outage, a natural calamity, a cyberattack, or a cascading failure, is paramount, even with higher penetration of DERs. In this context of ensuring resilience, the very transformations that enable deep decarbonization, including the development of cybergrid infrastructure, adoption of IoT devices, use of dynamic renewable energy sources, and increased electrification of transportation, could also introduce new vulnerabilities. Cyberattacks can disclose, deceive, or disrupt crucial information, thereby causing significant damage, ranging from small outages to brownouts and blackouts. Recent reports (2–5) indicate the ubiquity, ease, and scale of cyberattacks on sensitive industrial environments including supervisory control and data acquisition (SCADA), operational technology (OT), and industrial control systems (ICS), underscoring the importance of ensuring resilience to such adversaries.

Author contributions: V.J.N., P.S., V.V., C.I., P.M., J.W., J.K., H.V.P., and A.M.A. designed research; V.J.N., P.S., V.V., L.D.M., H.V.P., and A.M.A. performed research; V.J.N., P.S., V.V., P.S.S., L.D.M., J.Z., and H.V.P. contributed new reagents/analytic tools; V.J.N. and V.V. analyzed data; C.I., P.M., J.W., and J.K. provided critical inputs and valuable guidance; and V.J.N., P.S., V.V., A.S., H.V.P., and A.M.A. wrote the paper.

Reviewers: J.K., Danmarks Tekniske Universitet; and J.D.M., JDM Associates, LLC.

The authors declare no competing interest.

[1]To whom correspondence may be addressed. Email: jvineet9@mit.edu or poor@princeton.edu.

This article contains supporting information online at https://www.pnas.org/lookup/suppl/doi:10.1073/pnas.2413967121/-/DCSupplemental.

Published February 20, 2025.

By and large, most of the information for power grid operations flows through utility-controlled communication networks which are more reliable and resilient than commercial networks, and utilize commercial telecommunications services for other informational needs such as accessing the internet and communicating with customers. Such a tight separation is challenged by the increased information flow which becomes necessary with a stronger presence of a cyberlayer, which in turn is necessitated due to increased coordination and automation at the grid edge. What have remained as tight closed systems thus far, may have to relax their boundaries, introducing complexities in the underlying communication. While air gaps and protections will always be important and included, imperfect protections are inevitable as complexity increases. With increased penetration of instrumentation and automation, motors and generators may be manipulated by adversaries to open and close at will. Another point to be noted is that with increased complexities due to intermittent and uncertain generation and consumption, utilities alone cannot cater to all needs; public and private partnerships may be necessary. It is therefore extremely important to design an appropriate cyberinfrastructure that ensures that the lights stay on, despite increased communication, which may be between disparate stakeholders. The focus of this paper is on such a distributed decision-making framework.

Given the size and complexity of the problem of cyberattacks, providing a complete resilience framework for the entire power grid is a tremendously difficult task. In this paper, we propose a step, of providing SA to the grid operators in a distribution grid, with SA corresponding to the knowledge of local DERs in terms of their location and the amount of power that they are able to provide, as well as a resilience score (RS) that the operators can use to provide resilience. We argue that this step, of providing SA, is enabled through a local electricity market (LEM) structure that consists of operators at different voltage levels in a distribution grid. This market structure is proposed to be local, across the distribution grid, electrically colocated with primary and secondary circuits, with operators scheduling all DERs at the corresponding nodes in a given region. The market will also include IoT-coordinated assets (ICAs), with the assumption that each ICA will have computing capability and the ability to exchange information. The overall framework, EUREICA (Efficient, Ultra-REsilient, IoT-Coordinated Assets), is the innovation in the proposed cyberinfrastructure, and will be shown to lead to SA made available to operators placed hierarchically at various locations, thereby providing an important step in ensuring resilience.

LEMs have been addressed in several studies including refs. 6–11, with real-field implementations beginning to be reported (12, 13), all of which show the feasibility of a local market structure, and its advantages compared to alternate solutions that are designed to encourage full participation of DERs (5, 14). The LEM structure that we propose in this paper builds on that in ref. 6. The resilience of the electricity grid to cyberattacks has been explored in a very large number of studies (see refs. 3 and 15–17 and references therein), with new results appearing continuously. Broadly, these approaches can be categorized into detection and isolation of the attack (18), prevention of the attack, and resilience in the presence of attacks. For large-scale attacks such as those described in refs. 4, 19, and 20, these methods are inadequate; it may be near-impossible to identify the attacker but rather that an attack has occurred. Prevention of the attack can be enabled through varying levels of access and authorization (21) and monitoring, isolation, and protection at the component level (4). However, as the scale, location, and number of IoT devices in particular, and DERs in general grow, it becomes exceedingly difficult to completely prevent attacks. Ensuring resilience, especially in the face of large-scale attacks, for a large-scale system such as the electricity grid, is exceedingly difficult; current literature has either focused on systems at a small scale or with low levels of renewables. The EUREICA framework that we propose will provide SA that detects that an attack has occurred, and with this SA, deploys trustable ICAs in order to mitigate the impact of the attack, and ensure grid resilience through a distributed decision-making strategy.

The distributed decision-making in EUREICA is enabled through an LEM. The same market structure (6), which has been shown to lead to grid reliability (22) and provide grid services such as voltage support (23) in addition to overall power balance, is demonstrated in this paper to ensure grid resilience against cyberattacks using local trustable DERs. In particular, the results will show that local resilience is attainable through SA of locally available ICAs that have the ability to inject power or reduce consumption as well as a procedure for monitoring their trustability and commitment. The demonstrations are carried out using a variety of platforms such as (i) GridLAB-D which enables the simulation of distribution grids with high fidelity, (ii) the advanced research on integrated energy systems (ARIES) platform that includes a real-time digital simulator (RTDS) and enables hardware-in-the-loop (HIL) validation, and (iii) General Electric's advanced distribution management system (ADMS) (24), distribution operations training simulator (DOTS), and DER integration middleware (DERIM).

The problem statement is laid out in Section 1, and the local market structure together with the SA and Resilience score (RS) it will facilitate, is described in Section 2. Various use cases that constitute the various attack surfaces on the grid are described in Section 3. The main results are presented in Section 4, followed by a summary in Section 5.

1. Problem Statement

A typical path of electricity delivery to end users traverses generation, transmission, and distribution. Distribution substations connect to the transmission system and gradually step down the voltage from 44 kV or higher to 33 kV (denoted as a primary network), then down to 11.2/4.6 kV (denoted as a secondary network), and further down to 110 V or 220 V, depending on the specific region in the world. While the 20th century witnessed distribution systems operating as simple distribution lines as vehicles for sharing the electricity from transmission networks, today's distribution systems are increasingly becoming heavily integrated with distributed energy resources, that correspond to resources that are located closer to the load, including renewable generation, some of which may be behind the meter (5), batteries, and flexible consumption units. This in turn is causing distribution systems to become more independent and requiring them to take on increased responsibilities of services such as grid reliability and grid resilience. Other examples of DERs are distributed photovoltaics (DPVs) like rooftop solar systems, combined heat and power plants, electric vehicles, and diesel generators. DERs vary in size, from DPV systems that range between 1 to 1,000 kW in size to larger ground-mounted solar farms that range to several MW. With technological advances in power electronics and associated smart inverters as well as protection systems, fewer restrictions are being placed on the size and locations of the DERs, providing an opportunity for them to play stronger and more central roles in grid reliability and resilience (25).

Over the past years, DERs have been shown to be increasingly useful in providing key grid services such as volt-var control (26). The central idea in these explorations is that key information is exchanged, in a distributed manner, between suitable individual components in the primary and secondary networks, coordinated both in space and time, thereby allowing local control over power injection and reduction of load at key locations and instants. Such a correct operation of the complete distribution network is predicated on this key information reaching the recipients in a secure manner. This sets the stage for malicious attacks that can disconnect and disrupt the overall grid by impairing key components.

Several attacks on power systems have been recently reported (4, 19, 27–32) on the central control systems, key nodes in the distribution grid, or on devices at the end-user level. Those at the device end, denoted as MadIoT (Manipulation of Demand via IoT) attacks, correspond to a botnet at a secondary network node that causes the corresponding load to change abruptly. If this node corresponds to a high-wattage device, and the attack is coordinated through malware that simultaneously corrupts a large number of these devices, an argument can be made that it can cause frequency instabilities, line failures, and subsequently a severe disruption on the overall power grid. Building on the results in refs. 31 and 32, the results in ref. 19 show that even with realistic load profiles, a strategically coordinated attack can show a better success rate than in refs. 31 and 32 requiring fewer compromised IoT devices without triggering well-established protection systems. The well-known attack studied in ref. 4 on the other hand is at the central control system level, which was a well-planned strategic attack that led to a power outage affecting 250,000 customers over a significant period of time. The question we address in this paper is: How can we use a cyberinfrastructure with ICA to support grid resilience against cyberattacks?

The specific approach that we propose to circumvent the anomalous scenario consists of two steps: 1) Enable improved visibility over the grid and net power injections available at various nodes through a hierarchical market structure with operators at the primary network and secondary network nodes; 2) Enable the market operators to determine an RS computed through monitoring of various features of the communication network. Steps 1) and 2) together provide SA to the grid operators (as shown in Eq. **1**). Our central thesis is that through this SA, operators can determine that an attack has occurred and take appropriate steps to mitigate the impact of the attack in a timely manner. The system operators and resilience managers are suitably colocated with the electrical assets so as to respond quickly through a distributed decision-making framework. The framework therefore avoids the computational pitfalls of a centralized architecture while still underpinned by a substrate of communication, sensing, and actuation. The overall solution is also well-placed to integrate with the existing grid operational and market structures, helping accelerate its adoption in the field.

2. Our Approach: Local Electricity Markets

In order to provide visibility into a distribution grid, we propose an LEM that is hierarchical (Fig. 1) in nature and electrically collocated with a radial network. The starting point for the overall LEM is a distribution system operator (DSO) that oversees several substations in the distribution grid with multiple primary and secondary markets downstream and acts as their representative in its transactions with the wholesale electricity market (WEM).

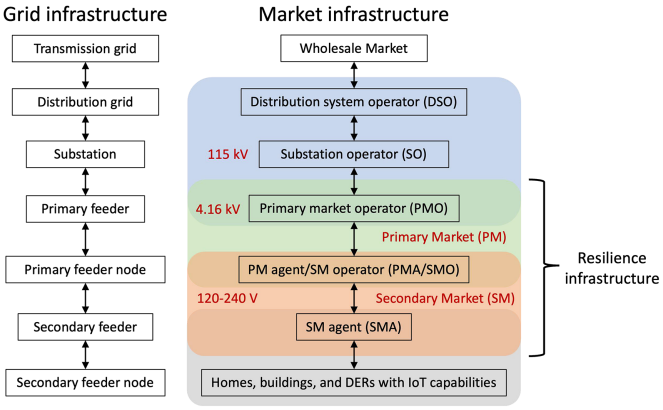

Fig. 1. A Hierarchical LEM for a Distribution Grid. The resilience infrastructure utilizes the dual market layer consisting of PM-SM.

The substation connects the distribution grid to the high voltage transmission grid at the point of common coupling (PCC) (node 150 in Fig. 2). The dual-layer downstream of the substation, consisting of a primary market (PM) and a secondary market (SM), is the core of the resilience infrastructure of this paper. The PM consists of Primary market operators (PMOs) and Primary market agents (PMAs). The PMA at each of the primary nodes either own a DER at a primary feeder node or are aggregators representing DERs at the secondary feeder level and below. In the latter case, the PMA plays a second role as an SM operator (SMO) and coordinates with SM agents (SMAs). The PMO, PMAs/SMOs, and the SMAs are located at the coupling between the substation and the primary feeder, primary feeder nodes, and secondary feeder nodes, respectively (Fig. 2). The PM and SM operate at medium- and low-voltage levels, respectively. The DSO supervises the entire distribution grid—our proposal could be viewed as an expansion of the current responsibilities of a DSO, which comprise grid maintenance and grid reliability, to include market oversight and regulation as well. In this sense, the role of the DSO would be analogous to that of existing independent system operators for transmission grids (33). *SI Appendix*, section 2 illustrates a possible implementation of the dual-layer LEM for the city of Boston, MA, USA.

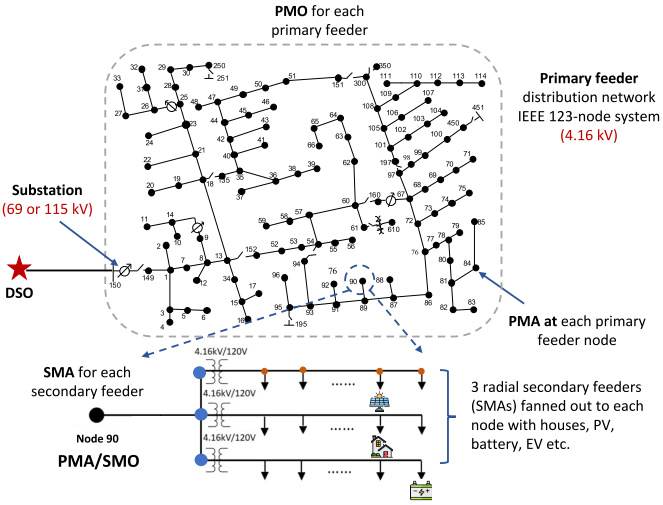

Fig. 2. LEM colocated with distribution grid. This shows a primary and secondary feeder distribution network based on the modified IEEE-123 node test case. Image Credit: Adapted with permission from Ref. 6.

Formally, we define SA at an operator x as the tuple

$$\mathrm{SA}_x = \{\mathrm{ICA}_x, \mathrm{RS}_x\}, \quad [1]$$

where ICA_x stands for IoT-coordinated assets and denotes the generation and/or consumption flexibilities of DERs under the purview of agent $x \in \{\mathrm{SMA}, \mathrm{SMO}\}$, and RS_x denotes their resilience scores, to be defined in Section 2.1.3. We will show that RS_x can be determined based on the asset's market performance and security against possible attacks.

We now show how the LEM made of the PM-SM layers will allow the computation of SA. The operation of a distribution grid is challenging due to its scale, complex topology, and presence of various active DER assets and fixed load nodes. We separate this complex task by having the PM focus on grid-specific costs and constraints while the SM focuses on consumer-centric costs and constraints. We assume that PM and SM clear once every 5 min and 1 min respectively. The main reason for this separation of timescales is that the SM typically needs to monitor fewer assets than the PM and is closer to DER devices (such as rooftop solar and batteries) and therefore may need to operate at a faster timescale than a PM. The starting point for both markets is the submission of bids by the corresponding agents. Bids for the SM are submitted by the SMAs exogenously, whereas bids for the PM are computed by the SMOs via the SM. We describe the operation of the SM before going into the details of the PM.

2.1. Secondary Market. The operation of the SM consists of three sequential stages: bidding, clearing, and monitoring. We denote $\mathcal{N}$ to be the set of all SMOs in the network and $\mathcal{N}_i$ to be the set of all SMAs under a given SMO $i \in \mathcal{N}$.

2.1.1. SM bidding. During the bidding phase, each SMA $j \in \mathcal{N}_i$ submits a bid $\mathcal{B}_j^{iS}$ defined as

$$\mathcal{B}_j^{iS} = \left\{P_j^{i0}, Q_j^{i0}, \underline{P}_j^i, \underline{Q}_j^i, \overline{P}_j^i, \overline{Q}_j^i, \beta_j^{iP}, \beta_j^{iQ}\right\}.$$

P_j^{i0} and Q_j^{i0} denote the baseline active and reactive injections of SMA j, along with the upward $(\overline{P}_j^i, \overline{Q}_j^i)$ and downward flexibility $(\underline{P}_j^i, \underline{Q}_j^i)$. β_j^{iP} and β_j^{iQ} denote the disutility parameters associated with providing active and reactive power flexibility, respectively. It should be noted that Bid B_j^{iS} requires SMA j to have a realistic estimate of its energy profile for the next 1 min. Since it is not always trivial to predict future power availability, agents deploy a decentralized federated learning (FL)-based framework (34) to determine their bids. Using FL helps ensure that the privacy of the participating agents is preserved and the computational aspects of the prediction algorithm scale well as the number of agents increases. Further details on the FL implementation can be found in *SI Appendix*, section 7. *SI Appendix*, Fig. S5 summarizes details of the overall LEM.

2.1.2. SM clearing. Once the SMO i has received bids from the participating SMAs, it clears the market with active and reactive power injection setpoints (P_j^{i*}, Q_j^{i*}) and the corresponding retail tariffs $(\mu_j^{iP*}, \mu_j^{iQ*})$. In addition, the SMO also solves for the optimal flexibility ranges $(\delta P_j^{i*}, \delta Q_j^{i*})$ for $j \in \mathcal{N}_i$. The SMO clears the markets with the following objectives: (O1) maximization of aggregate resilience f_i^1, (O2) minimization of the net cost to the SMO, f_i^2, (O3) maximization of total flexibility f_i^3 that the SMO can extract from all its SMAs and (O4) minimization of the disutility of the SMAs f_i^4, arising from flexibility provision (see *SI Appendix*, section 3 for all details). This gives rise to a multiobjective constrained optimization problem:

$$\min_{\mathbf{y}_i^S} f_i^S = \{f_i^1, f_i^2, f_i^3, f_i^4\}^\top \quad [2a]$$

$$\text{s.t.} \underline{P}_j^i + \delta P_j^i \le P_j^i \le \overline{P}_j^i - \delta P_j^i \ \forall j \in \mathcal{N}_i, \ \forall \text{ constraints}$$

$$\underline{Q}_j^i + \delta Q_j^i \le Q_j^i \le \overline{Q}_j^i - \delta Q_j^i$$

$$\delta P_j^i, \ \delta Q_j^i \ge 0, 0 \le \mu_j^{iP} \le \overline{\mu}^{iP}, 0 \le \mu_j^{iP} \le \overline{\mu}^{iQ}$$

$$\sum_{t_p \in \mathcal{T}_p} \sum_{t_s \in \mathcal{T}_s} \sum_{j \in \mathcal{N}_i} \mu_j^{iP}(t) P_j^i(t) \Delta t_s \le \sum_{t_p \in \mathcal{T}_p} \mu^{iP*}(\hat{t}_p) P_i^*(\hat{t}_p) \Delta t_p$$

$$\sum_{t_p \in \mathcal{T}_p} \sum_{t_s \in \mathcal{T}_s} \sum_{j \in \mathcal{N}_i} \mu_j^{iQ}(t) Q_j^i(t) \Delta t_s \le \sum_{t_p \in \mathcal{T}_p} \mu^{iQ*}(\hat{t}_p) Q_i^*(\hat{t}_p) \Delta t_p$$

$$\sum_{j \in \mathcal{N}_i} P_j^i(t_s) = P^{i*}(\hat{t}_p), \quad \sum_{j \in \mathcal{N}_i} Q_j^i(t_s) = Q^{i*}(\hat{t}_p) \ \forall t_s \in \mathcal{T}_s$$

The constraints include capacity limits and operational bounds on SMA injections (including flexibilities), budget balance constraints, price ceilings, and lossless power balance (6). $\mathcal{T}_p, \mathcal{T}_s$ denote the set of all PM clearing timesteps, and secondary timesteps per PM clearing, respectively. $\hat{t}_p$ refers to the most recent PM timestep before each SM clearing. Note that, here we do not account for all the power physics, these will be considered in the PM. The decision variables consist of the P and Q injection setpoints as well as retail tariffs for each SMA i.e. $\mathbf{y}_i^S = \{\mathbf{y}_j^{iS}\} \ \forall j \in \mathcal{N}_i$, where $\mathbf{y}_j^{iS} = [P_j^i, Q_j^i, \delta P_j^i, \delta Q_j^i, \mu_j^{iP}, \mu_j^{iQ}]$. We note from the choice of f^1 that the solution of Eq. **2** requires the resilience scores RS_j^i. This is assumed to be communicated by the secondary resilience manager (SRM) to the SMA, the details of the SRM are addressed in the next section.

In general, the optimization problem in Eq. **2** has multiple solutions known as Pareto points, with each solution prioritizing different objectives. However, since the objective functions have different units, instead of finding the Pareto solutions, we use a hierarchical ranked approach proposed in ref. 23 where the SMO optimizes one objective at a time in descending order of importance. While optimizing the subsequent objective functions, additional constraints on the degradation of prior objectives are added to the optimization problem (see ref. 6 for details). The cleared market schedules $\mathbf{y}_i^{S*}$ are sent by the SMO to their corresponding SMAs, as well as to their SRM.

2.1.3. SM monitoring and resilience scores. The final stage in the SM is monitoring. During the market operation, the responses of each SMA j to the market schedules, in terms of its actual DER injections $\hat{P}_j^i$ and $\hat{Q}_j^i$ are suitably monitored by its corresponding SRM. In addition to the market operators, we also propose the addition of two entities, which we denote as the primary resilience manager (PRM) and the SRM, both of which provide grid functionalities, with the PRM located at the primary circuit level and the SRM at the secondary level, as shown in Fig. 3. With the market clearing providing the first step of awareness in the form of power available at each of the nodes at the secondary and primary level, the PRM and SRM monitor the actual injections, determine corresponding scores of commitment, trustability, and resilience (to be defined below), and communicate them using protected channels. Not only do these entities enable a separation between grid-specific decision-making from market-specific decisions, but they also provide a pathway for mitigating the impact of any

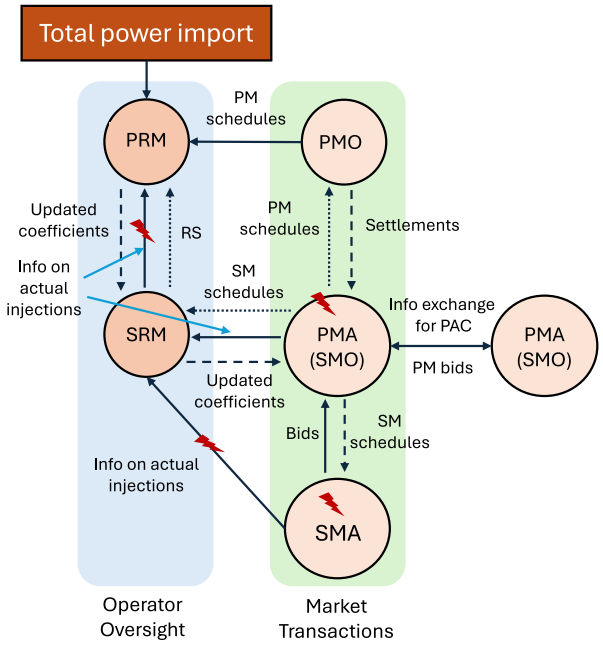

Fig. 3. Sequence of communication steps and events leading to SA with an LEM. The red arrows indicate the entities and communication links that would be affected by an attack. A more detailed diagram can be found in *SI Appendix*, Fig. S9.

attacks that can occur through the addition of local resources, as will be shown in the following sections.

In this monitoring stage, the SRM assigns each SMA an RS that is updated constantly based on its performance in the market and susceptibility to being compromised. The RS is a weighted combination of its commitment score (CS) and trustability score (TS). Formally, for an agent j

$$\mathrm{RS}_j = \alpha \mathrm{CS}_j + (1-\alpha)\mathrm{TS}_j,$$

where $\alpha \in (0, 1)$ is a parameter chosen by the SRM. The CS and TS are defined below.

- *Commitment score (CS).* The CS of an agent measures its reliability in executing its cleared schedules and is updated at every SM clearing instance. The first step in updating CS_j for each agent $j \in \mathcal{N}_i$ is the computation of any relative deviation between the cleared schedule and its executed value over the past market period. A moving average is then computed to account for the past performance. Finally, a min-max normalization across all the SMAs is performed to keep $CS_j \in [0, 1]$ for all j (see *SI Appendix*, section 3.E for further details).
- *IoT Trustability score (TS).* The TS captures the possibility of the agents (or the devices underneath them) being compromised. TSs are computed using an FL-based anomaly detector and like the CS, past values are used again to compute a weighted moving average. However, unlike the CS, which solely depends on power injections, the TS is a cyberpower metric (35) that also takes into account the associated cyber information, e.g., packet length, arrival time, and communication protocols, etc. (see *SI Appendix*, section 4 for further details).

In summary, the overall SM operation allows the computation of schedules $\mathbf{y}_i^{S*} = [P_j^{i*}, Q_j^{i*}, \delta P_j^{i*}, \delta Q_j^{i*}, \mu_j^{iP*}, \mu_j^{iQ^*}]$ and $\mathrm{RS}_j^i \ \forall$ SMAs j, all of which provide SA_j^i for the SRMs corresponding to all SMAs j at primary node i. Similar measures of the resilience of large-scale networks to attacks can be found in ref. 36.

2.2. Primary Market. PM transactions happen between the PMO and the PMAs. Similar to the SM, the operation of the PM also consists of bidding, clearing, and monitoring.

2.2.1. PM bidding. Here, we describe the link between the PM and SM. As noted previously, the PM is cleared every 5 min while the SM operates more frequently at 1-min intervals. Before each PM clearing, the SMOs (or PMAs) aggregate the schedules and cleared flexibilities of all their SMAs resulting from the most recent prior SM clearing (at the lower level) to submit their flexibility bid to the upper-level PM. All market bidding and clearing for both the SM and PM are based on forecasts (assuming perfect foresight) and for the very next period. The complete bid submitted by each SMO $j \in \mathcal{N}$ into the PM $\mathcal{B}_i^P$ defined as

$$\mathcal{B}_i^P = \left\{ P_i^0, Q_i^0, \underline{P}_i, \underline{Q}_i, \overline{P}_i, \overline{Q}_i, \alpha_i^P, \alpha_i^Q, \beta_i^P, \beta_i^Q \right\}. \quad [3]$$

This includes the nominal power available, the lower and upper bounds, net generation cost coefficients, and flexibility disutility parameters (see details in *SI Appendix*, section 3.C). We note that standalone PMAs such as a large industrial facility, a community solar farm, or an EV charging station, may also be present. In this case, the PMA would directly bid into the PM on its own instead of aggregating over SMAs.

2.2.2. PM clearing. At each PM clearing instance, an optimal power flow (OPF) problem is solved to optimize the PMO's objective while satisfying all grid physics and network power flow constraints. For simplicity, in this work, we consider the cost functions of all the PMAs (or SMOs) to be quadratic. The objective function utilized is a weighted linear combination of (i) maximization of social welfare, (ii) minimization of total generation costs, and (iii) minimization of electrical line losses (see *SI Appendix*, section 3.D for details of these functions). The total cost includes paying the locational marginal price (LMP) λ for importing power from the transmission grid at the 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.

With the objective function thus defined, the constraints are determined by the choice of the power flow model used to describe the system. Since the original alternating current OPF (ACOPF) is inherently nonconvex and NP-hard, we need to convexify the problem to make it more tractable. In this study, we considered two different approaches for this convexification. The first is a branch flow (BF) model or nonlinear DistFlow (37) based on a second-order conic program (SOCP) convex relaxation—this is a simpler implementation that is valid for radial and balanced networks. The second is a linear current injection (CI) model (38) based on a McCormick envelope convex relaxation that is more generally applicable to unbalanced and meshed grids common in distribution systems (in addition to radial, balanced), although this adds some overhead due to certain preprocessing steps needed.

We deployed both of these models for different use cases considered in this paper, as shown in Table 1. Further details of the BF and CI approaches are provided in *SI Appendix*, sections 5.A and 5.C, respectively. The exact set of decision variables $\mathbf{y}_i^P$

Table 1. Summary of attack scenarios and use-cases, LA = load alteration attack, DG = distributed generator attack

Attack no.	Attack type	Attack surface	Grid connection	Power flow model	Grid model	Scale of attack [kW]
1a	LA	PMA	Grid-connected	Current injection	Unbalanced, 3-phase	36
1b	DG	PMA	Grid-connected	Current injection	Unbalanced, 3-phase	45
1c	DG	SMA	Grid-connected	Current injection	Unbalanced, 3-phase	157
2a	DG	PMA	Grid-connected	Branch flow	Balanced, single-phase	261
2b	DG	PMA	Grid-connected	Branch flow	Balanced, single-phase	650
3	DG	PMA	Islanded	Current injection	Unbalanced, 3-phase	2,500

for each PMA i differs slightly depending on the OPF model used. Both models solve for the nodal power injections and voltages. However, the BF model only considers branch currents while the CI model also considers nodal current injections. BF also models all variables as only having a single phase while the CI models these as three-phase, complex phasor quantities. For simplicity, we have only included the single-phase formulations in the paper thus far. However, these can easily be extended to the complex three-phase representation by simply modifying all variables to be 3-dimensional complex vectors instead of scalars. A three-phase extension of the SM optimization is given in *SI Appendix*, section 3.B.

2.2.3. Distributed optimization for PM clearing. We employ a distributed proximal atomic coordination (PAC) algorithm (39) to solve the OPF using peer-to-peer communication between the agents. This approach is preferred over traditional centralized optimization solvers since the number of nodes (and hence the number of PMAs) in a primary feeder could be arbitrarily large. It also helps preserve data privacy since each PMA only needs to exchange limited information with its immediate neighbors. A distributed approach also enables the PMAs to clear the market independently of the PMO, alleviates the communication burden, and reduces latencies since PMAs do not need to send all their data to a centralized entity, thus allowing for scalability. This is achieved by a process called atomization wherein the overall global optimization problem is decomposed into several local optimization problems called atoms, for each PMA. The constraints can also similarly be decoupled. However, certain network constraints also depend on other PMAs' variables. To deal with this, we include additional coupling or consensus constraints to ensure consistency. We also used an enhanced variant of PAC known as NST-PAC that employs Nesterov (NST) acceleration and has enhanced privacy features by further masking the variables exchanged between atoms (i.e., the PMAs) (40). After a sufficient number of iterations, both the PAC and NST-PAC algorithms provably converge to globally optimal and feasible solutions $\mathbf{y}^{P*} = \{\mathbf{y}_i^{P*}\}$ for each of the PMAs. Further details on PAC and NST-PAC are provided in *SI Appendix*, section 6. These cleared market schedules are communicated by the PMAs to their respective SRMs as well as to the PMO.

2.2.4. PM prices. Using distributed optimization, we obtain the electricity prices for the PM from the solutions that the dual variables μ_i^{P*}, μ_i^{Q*} converge to. As indicated in ref. 14, this can be viewed as a distributed locational marginal price (d-LMP) and reflects the local value that the market agents are providing through local generation and flexible consumption.

2.2.5. PM monitoring and resilience scores. During the actual market operation, the injections $\hat{P}_i$ and $\hat{Q}_i$ from the DERs at PMA j are monitored by their SRM. These could be either from standalone PMAs or aggregated information from all the SMAs at a given PMA. The SRM also assembles resilience scores RS_i for each PMA i. This is done through aggregation (via a weighted average) of $\mathrm{RS}_j^i \ \forall j \in \mathcal{N}_i$. The RSs for standalone PMAs can also be directly computed at the SRM using their monitored injections. $\mathbf{y}_i^P$ and RS_i thus provide complete SA at each PMA node i. All SRMs send this information to the PRM so that the PRM has complete SA of all PMAs. This SA can then be used to redispatch the ICAs in both the PM and SM to mitigate the impact of various attacks. Further details on the mitigation strategy can be found in *SI Appendix*, section 9.

2.3. Reconfiguration Paths. The final tool that we use in our proposed EUREICA framework is grid reconfiguration in the wake of islanding which can occur if an attack, fault, or natural disaster causes an entire section of the grid to be disconnected from the main grid. In such cases, an algorithm that determines a self-sustaining operation of the islanded system, which is enabled by reconfiguration paths with suitable switch settings, is essential. We propose a reconfiguration algorithm (see *SI Appendix*, section 10 for details) that considers power flow feasibility, available distributed generators (DGs), critical load, as well as RS information, to determine switching actions to restore specific sections of the distribution feeder. Reconfiguration paths will be determined based on the available amount of generation and the amount of critical load to be supplied, which is obtained through the SA provided by the EUREICA framework. In addition, the TSs are used at the secondary feeder level to intelligently disconnect noncritical loads, thus enabling the maximum restoration of critical loads. Once the feasible paths are determined for the optimal selection of loads, the RSs for all feasible paths are computed, and the most resilient path is implemented in the system.

3. Use Cases

In this section, we present use cases that illustrate how SA can be leveraged to ensure grid resilience in a distribution grid with a high penetration of DERs. We consider four different attack scenarios, all of which are motivated by the two large-scale attacks in (4, 31) on power grids. Disruptive attacks are assumed to occur in the form of (a) a sudden loss of generation, and/or (b) a sudden increase in load, at multiple vulnerable locations. All use cases are simulated using an IEEE 123-node test feeder (see *SI Appendix*, section 1) modified to have a high DER penetration (see *SI Appendix*, section 1.A); extensions to more realistic and larger networks (41) can be implemented similarly.

3.1. Attack 1. In this attack, it assumed that a small percentage of generation or load resources at either the primary or secondary feeder level are compromised. In particular, it is assumed that these units are offline due to either an outage, natural calamity, or malicious cyberattacker using elevated privileges to disconnect

the units. In addition to the generation shortfall, it is assumed that the communication link between the market operators (PMO/SMO) and the resilience managers (PRM/SRM) is also affected by a denial of service (DoS) attack, which compromises the availability of a resource (see ref. 42 for an attack which occurred on an sPower installation in Utah). Attack 1 draws inspiration from ref. 4, where a malicious attacker used (i) elevated and unauthorized access to disconnect several resources, and (ii) severed communication links, to hamper operator visibility and response. While these attacks occurred at the transmission level, it is feasible that a similar impact can be had by targeting distribution grid entities, especially with the larger attack surface provided by grid-edge devices. Independently, it is possible that IoT load devices such as heating, ventilation, and air conditioning (HVAC) devices, WHs, EV chargers, or refrigerators may be attacked as well, as noted in ref. 19. Elements of both of these types of attacks are explored here in two different cases, 1a and 1b.

3.1.1. Case 1a. In this case, the grid is assumed to be subjected to a sudden increase in load at the primary feeder level (SMO or PMA) due to malicious agents. There are several large loads connected to the primary feeder such as commercial buildings or industries, and a malicious agent can manipulate the loads in these entities to affect the grid. Typically, the grid would rely on the margin provided by grid inertia to mitigate the effect of a sudden load increase. However, in a case where the grid's resources are stretched, such as a cold snap or similar natural hazards, it is imperative that the grid-edge IoT resources be tapped to mitigate this condition. Examples of this scenario are already seen in operations, such as requests from grid operators in Alaska, Texas, and others in response to cold snaps. The operators requested customers to reduce their power consumption to support large critical loads such as chillers in hospitals. Furthermore, increased DER penetration will also lead to a loss of inertia, currently provided largely by large coal and gas plants. Case 1(b) details the performance of the proposed framework from this generation shortfall, even when the PRM does not have complete observability in the system.

3.1.2. Case 1b. Here, several generating resources are assumed to be unavailable at the primary feeder level (i.e. SMO or PMA). There are several scenarios that motivate this—for example, in the case of several cloudy days in a row (affecting wind power), or unforeseen maintenance on generating units, the grid operates at a lower margin than under normal conditions. There is also the case of a malicious actor disconnecting generation resources. The grid experiences a supply shortfall, and in combination with the DoS attack, the system operator (PRM) loses observability.

3.1.3. Case 1c. In this case, the grid is subjected to a sudden increase in load and/or corruption of distributed generation from the IoT devices, in a coordinated fashion directly at the secondary feeder. DER IoT devices will soon be operated via cloud-based service mechanisms that allow them to be controlled remotely. Thus, a sufficiently motivated malicious actor could gain control of a large number of these to suddenly reduce generation or increase load in a coordinated fashion. We simulated a case in which a large number of DGs (such as solar PV smart inverters) are attacked at the SMA level.

3.2. Attack 2. A larger-scale attack is assumed to occur at the distribution grid level in the form of several DGs being corrupted, causing them to go offline. The scale of this attack is assumed to be such that the impact is felt even in the transmission grid. We will explore how SA by the PRM and SRM helps mitigate this impact. Similar to attack 1.0, this use case combines elements of both (19) and (4). The similarity to the latter is that the corruption is inserted in the form of outages of large DGs, while that to the former is that it introduces oscillations at the transmission level. For this purpose, we will utilize the well-known Kundur 2-area test system used to understand the transient and dynamic transmission-level impacts (43). In particular, we will assume that there is an outage in one of the two areas (Area 2) that is load-rich, which introduces additional stress on the tie-line connecting the 2 areas (see *SI Appendix*, Fig. S15 for a diagram of the 2-area system).

3.3. Attack 3. The substation transformer is located at node 150, which is connected to the main transmission grid under normal operating conditions. However, under this attack, the distribution grid is islanded from the main grid at node 150. This could be due to a multitude of factors—such as wildlife tripping the transmission line from the substation to the distribution system, or a cyberattack (i.e., integrity or disruption attack) that trips the circuit breaker from the main grid. With the increased SA introduced through our framework, we will demonstrate that the distribution system loads can be picked up in a coordinated fashion.

4. Results and Discussion

In this section, we focus on a few specific attack scenarios 1a, 2b, and 3 described in Table 1, along with some results for attacks 1b and 1c. The remaining scenarios are elaborated in *SI Appendix*, sections 14 and 15. With the numerical simulation setup described in *SI Appendix*, section 13, we present details of how each of these attacks is mitigated using the proposed EUREICA framework. Note that for all attacks except attack 2.0, we use the mitigation strategy described in *SI Appendix*, section 9.B. For attacks 2a and 2b, we use the algorithm in *SI Appendix*, section 9.A instead. In addition to market simulations, we also validated our results using high-fidelity software at the Pacific Northwest National Lab (PNNL), Larsen & Turburo Digital Energy Services (LTDES), and the National Renewable Energy Lab (NREL). Technical details for each validation platform can be found in *SI Appendix*, section 11. For each attack, we focus on a specific subset of results to highlight the most pertinent findings and insights. Complete details including the remaining market simulation results for all attack scenarios can be found in *SI Appendix*, section 14, along with the complete set of validation results in *SI Appendix*, section 15.

4.1. Mitigation of Attack 1a. We note that in attack 1a, loads are compromised leading to an increase in the power import from the bulk grid. It is also assumed that the communication from all SRMs to the PRM is disrupted, while the communication from the PRM to the 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 *SI Appendix*, section 9), which will provide the injections needed to fully mitigate the attack, and the overall power balance is thus met at all points in the distribution grid.

The steps in mitigation are as follows: 10 SMO nodes are attacked, resulting in a total increase in load (generation shortfall)

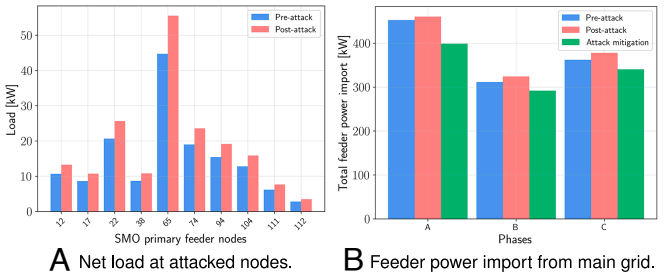

Fig. 4. Effect of attack 1a and mitigation.

of 36 kW for the entire feeder as seen in Fig. 4*A*. A large number of flexible load nodes across the entire feeder help with mitigation by curtailment and shifting as in Fig. 5. Flexible load curtailment at individual SMO nodes ranges from a minimum of 0.55 kW to a maximum of 7.8 kW reduction per primary feeder node—using a combination of resources like HVAC, WHs, batteries, and EVs to reduce the net load. There is a 123 kW decrease in power import after mitigation as seen in Fig. 4*B*. The new SMO setpoints from the PM redispatch are then disaggregated among their SMAs during the following SM redispatch, with an example for SMO 77 shown in Fig. 6.

The outputs from the PM-SM market framework were sent to the DERIM interface using which the effect on the total net load at the substation feeder head could be determined with the DERIM-ADMS-DOTS software platform (see *SI Appendix*, Fig. S14 for an overview of the validation process). It is clear from Fig. 7 that without the intervention of EUREICA, the impact of the attack is a 37 kW jump in the feeder demand; in contrast with EUREICA, the feeder demand is cut by 94 kW. Moving further ahead from the attack timestep, the feeder net load eventually approaches back to the same value as if there had not been an attack. See *SI Appendix*, section 15.D for further details on this validation. See *SI Appendix*, sections 15.A and 15.G for the other validation results using the HELICS and ARIES platforms, respectively.

4.2. Attack 1b Validation Based on Resilience. Here, we briefly highlight the effects of resilience scores on the mitigation of attack 1b, where a number of DGs are attacked. Full details on this attack can be found in *SI Appendix*, section 14.A. Here, we focus only on how the RSs of SMOs and SMAs influence which resources are utilized to mitigate the attack. The RSs of the flexible SMOs are plotted against their absolute and relative levels of net load curtailment in Fig. 8 *A* and *B*, respectively. We see that in relative terms (with respect to their nominal or baseline load), the curtailment is generally distributed evenly to ensure that no single SMO is disproportionately affected. However, if the PMO does need to utilize more flexibility from certain SMOs, it generally calls upon more reliable ones with higher RSs. The absolute amounts of curtailment vary for each SMO based on their baseline load. This also holds while disaggregating SMO setpoints at the SM level, where the SMO allocates greater flexibility to SMAs with higher RSs, as seen in Fig. 6. See *SI Appendix*, sections 15.B and 15.E for validation results of this attack using DERIM-ADMS-DOTS and HELICS, respectively.

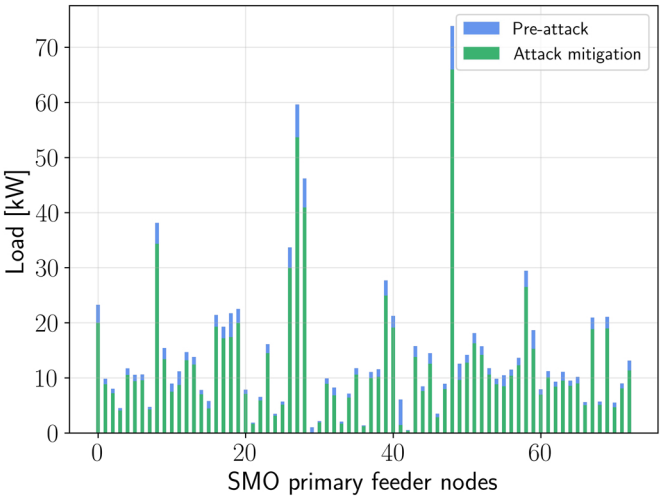

Fig. 5. Curtailment of flexible loads for attack 1a mitigation.

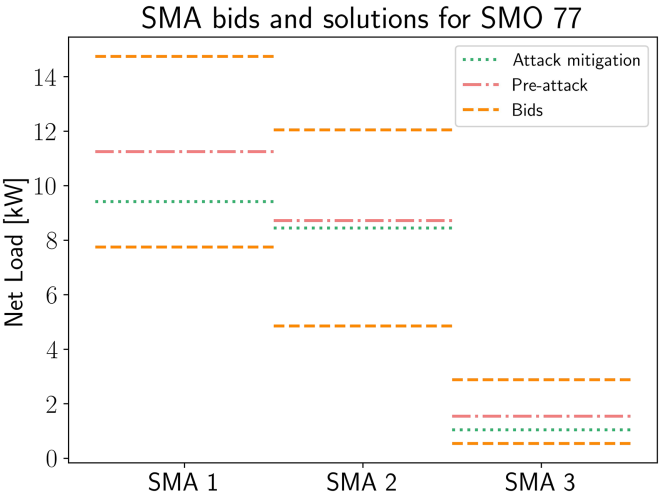

Fig. 6. Disaggregation of setpoint changes (from the PM) for SMO at node 77 across its 3 SMAs (in the SM) on phase B, after attack 1a mitigation.

4.3. Contributions of SM and PM to Attack 1c Mitigation. Attack 1c is a more distributed attack where individual SMAs are attacked directly. Here, we show how both the SM and PM flexibility are needed to fully mitigate the attack. Fig. 9 shows the contributions of the SM and PM toward attack mitigation. We see that for most of the SMO nodes, both the SM and PM flexibility play a significant role in reducing the net load compared to the post-attack case. At the SM level, we utilize the

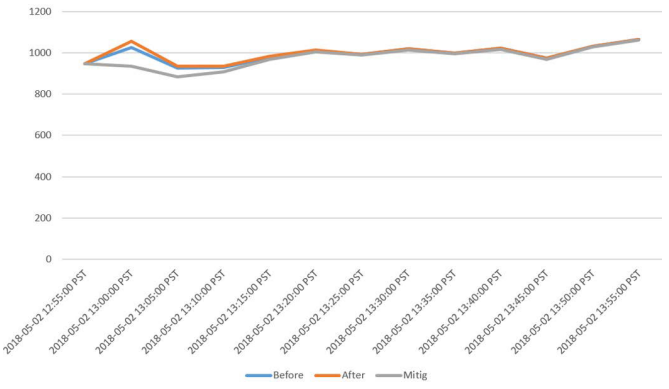

Fig. 7. LTDES validation of attack 1a in the DERIM-ADMS platform, showing total power import at the substation around the attack time at 13:00.

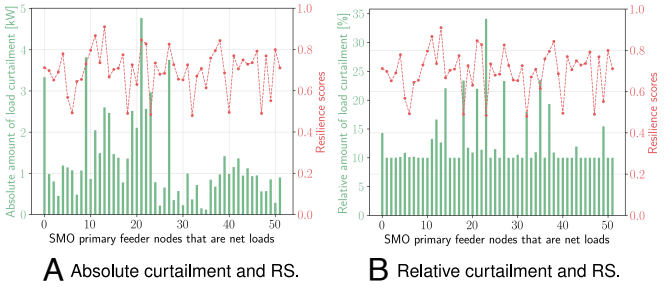

Fig. 8. Distribution of absolute and relative amounts of load curtailment across the flexible net load SMOs, along with their corresponding resilience scores.

available upward flexibility of any SMAs with remaining online DGs and use the downward flexibility of all net load SMAs. At the PM level, we utilize the downward load flexibility of the SMOs (which are all net loads after the attack). Further details on this attack can be found in *SI Appendix*, section 14.B.

4.4. Mitigation of Attack 2. Here, we describe the mitigation of two attacks at the primary feeder level that are relatively broader in scope, one is a medium-scale and the second is a large-scale attack. Both are disruption attacks where the attacker shuts down one or more of the large DGs in the network. We only consider a single primary market time step to study the effects of an instantaneous attack. Mitigation can use P dispatch from batteries, P and Q curtailment from flexible loads, limited P dispatch from PV, Q support from smart inverters (connected to PV and batteries), as well as conventional dispatchable fossil fuel sources like diesel generators. We only present results for the large-scale attack here, details on the medium-scale attack can be found in *SI Appendix*, section 14.C.

4.4.1. Large-scale attack 2b. Here, we adopted a top–down approach in emulating an attack and started with a Kundur 2-area transmission model, with the attack occurring in Area 2 (*SI Appendix*, Fig. S15) which consists of a load of 1,767 MW. Noting that Area 2 can be broken down into 552 IEEE-123 feeders, each with approximately 3.2 MW, we assume that an attack that compromises about 650 kW of generation, occurs in each of these 552 feeders. This in turn corresponds to an overall shortfall of 359 MW at the transmission level. We introduced

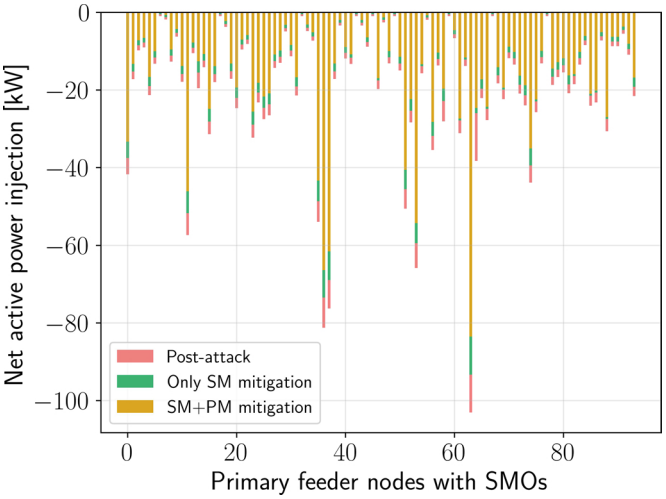

Fig. 9. Contributions of SM and PM flexibility for attack 1c mitigation.

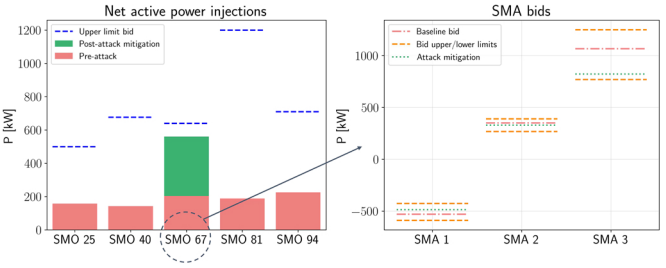

Fig. 10. Mitigation of large-scale attack 2b. Image Credit: Adapted with permission from Ref. 22.

this 650 kW shortfall in the form of a generation loss at four nodes 25, 40, 81, and 94, in each of the 552 primary feeders. The only remaining SMO with significant generation capability is at node 67. With the same procedure as outlined in the previous scenarios, the use of our proposed EUREICA framework leads to the results in Fig. 10. In order to mitigate the attack, we need to leverage the upward generation flexibility of the remaining SMO 67 to increase its output injection after attack mitigation, while the net injections for all the other four attacked SMOs drop to zero as seen in the left plot. The right plot shows the new SMA schedules resulting from the revised SM clearing.

However, due to the larger scale of the attack, redispatching the generator SMOs is no longer sufficient to fully meet the shortfall. Furthermore, as seen in Fig. 10, we are not able to utilize all the upward flexibility of the remaining online SMO 67 since its dispatch is limited by power flow constraints, on nodal voltages and line currents in particular. Thus, we also need to perform some shifting and curtailment of high-wattage flexible loads. These could include EVs and thermostatically controlled loads like HVAC and WHs. In addition, it could also involve some discharging of battery storage systems to reduce the net load. The distribution of net load reductions across the remaining SMOs is shown in Fig. 11, with a total decrease of around 14% as seen in Table 2. From Table 2, we also see that the attack would have potentially increased the power import from the transmission grid by over 37%, but the combination of increased local generation and load curtailment helps keep the imported amount almost the same as before. Further details on this attack can be found in *SI Appendix*, section 14.D.

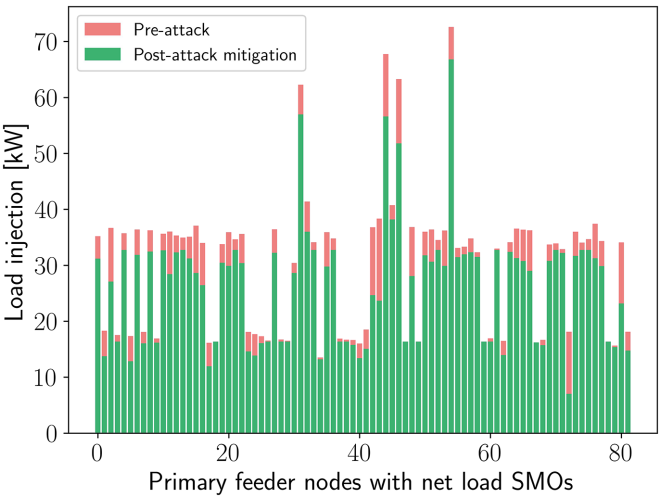

Fig. 11. Flexible load curtailment for large attack mitigation. Image Credit: Adapted with permission from Ref. 22.

Table 2. Summary of metrics for large-scale attack 2b scenario

	Preattack	Postattack	Attack mitigation
Power import from main grid [kW]	1,325	1,821 (+37.4%)	1,328
Total cost [$]	10,752	11,500 (+7%)	14,156 (+31.7%)
Total load [kW]	2,064	2,023 (−0.02%)	1,775 (−14%)

Image Credit: Reprinted with permission from Ref. 22.

4.4.2. Effects at the transmission level. The overall impact of the generation shortfall and mitigation using EUREICA is simulated in the RTDS using a proxy where the individual feeders are not modeled, but the aggregated effect is studied at the transmission scale. A combined shortfall of 359 MW, corresponding to a simultaneous compromise and outage of 650 kW in all 552 primary feeders in Area 2 triggers a frequency event (Fig. 12). Left unchecked, this can potentially lead to drastic load shedding or parts of the system being blacked out. To mitigate this situation, the power flow from Area 1 to Area 2 needs to be increased, which was observed in the RTDS, through the action of the governor system, which responds in the timescale of seconds, by increasing generation from the other generators present in the system proportionately based on a droop value. This increases the power flow from the generation-rich Area 1 to Area 2. However, changing the tie-line power flow creates a frequency imbalance, resulting in the system frequency oscillating, and settling at either a lower or higher frequency for areas 2 and area 1, respectively, as shown in Fig. 12. With the EUREICA framework, the frequency mismatch is mitigated by suitably leveraging the flexibility of the remaining generation as well as demand response (DR) mechanisms from flexible loads at both the SMO and SMA levels (see Fig. 13). Once the governor response is completed and the system settles at a suboptimal frequency, a combination of intelligent DR and generation redispatch in Area 2 facilitated by the EUREICA framework allows the system frequency to be restored to normal, ensuring grid resilience, avoiding system stress and increased operational costs.

4.4.3. Key system metrics, economic, and distributional impacts. In our simulations, we find that attack mitigation comes at the expense of increased operational costs for the PMO since it needs to dispatch more expensive local resources to a greater extent, rather than importing cheaper power from the main grid (at the LMP rate). The PMOs and SMOs also need to adequately compensate agents for the critical flexibility they provide. As shown in Table 2 for attack 2b, the attack increases the system operating costs by around 7%, and the mitigation steps raise the cost by over 31%, both relative to the preattack case. However, the PMO could recoup this through other revenue streams and cost savings. For example, the transmission system operators may compensate PMOs for locally containing attacks. Being able to leverage local DER flexibility through markets could also reduce the amount of auxiliary backup generation that the PMO needs to maintain, and lower the reserves it may have to otherwise procure from capacity or ancillary service markets. The PMO in turn could also redistribute some of these benefits among the SMOs and SMAs.

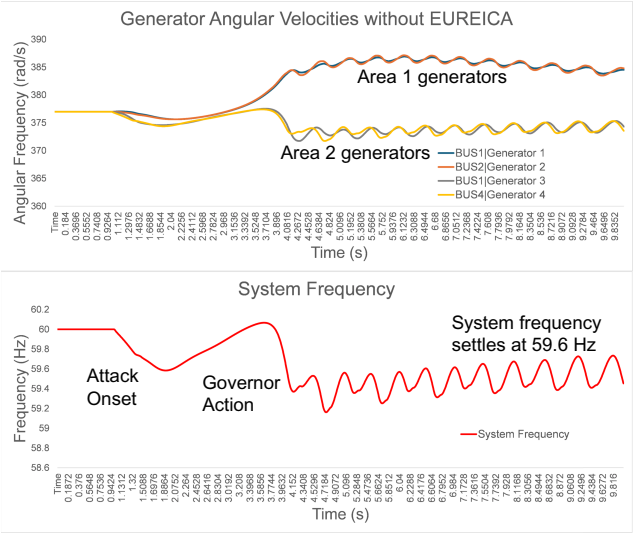

Fig. 12. Response without EUREICA; system settles at suboptimal frequency.

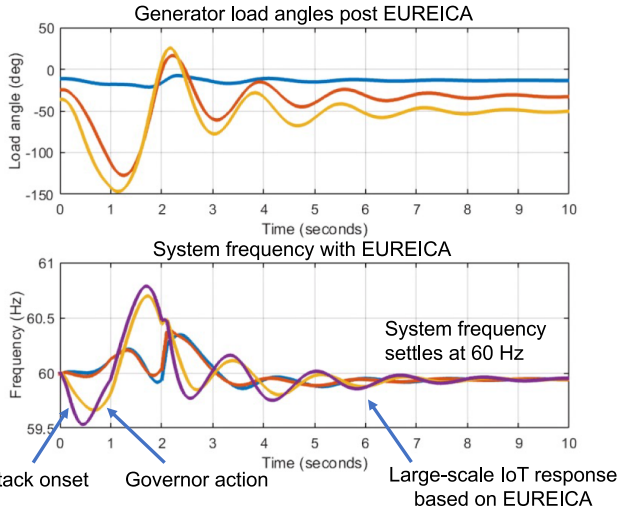

Fig. 13. Frequency response with EUREICA; system settles at 60 Hz following demand response and load shedding enabled by the EUREICA framework.

4.5. Mitigation of Attack 3. We now consider the attack scenario where the distribution grid is isolated from the transmission system. In such a case, the distribution grid is fed through an alternate circuit such as from node 350 (Fig. 14). A typical response in such a case is that the distribution grid breaks into several "zones"—creating smaller islands where only a portion

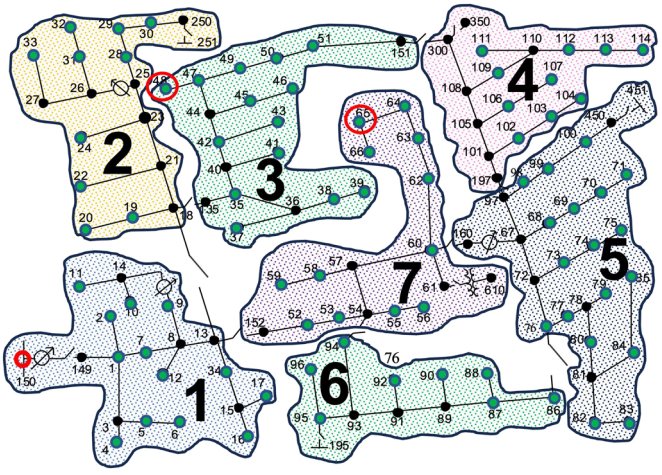

Fig. 14. EUREICA IEEE 123-node feeder for reconfiguration module validation.

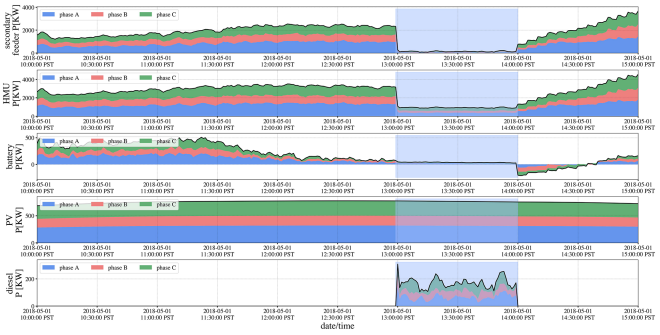

Fig. 15. Demand and DG with resilience-based reconfiguration during attack 3.

of the load is fed through any DERs that may be present. We show below that with the increased awareness provided by the EUREICA framework, a much higher percentage of consumers remain unaffected, by suitably leveraging the DERs at node 48, the microgrid system connected at node 65 (marked by the red circles in Fig. 14), and DR methodologies. In order to ensure feasibility and supply–demand balance with islanding, we also introduce two large diesel generators located at nodes 48 and 65 which may only be called upon when the feeder is islanded. Three cases are presented.

4.5.1. Critical loads distributed across the feeder. In this case, through the proposed resilience-based IoT load restoration with DR optimization strategy (see *SI Appendix*, section 10 for details), a feasible reconfiguration path is computed to open or close tie switches and completely or partially shed noncritical grid edge loads using reconfiguration to allow the available generation resources to cover approximately 30% of total load in the system. As seen in Fig. 15, with almost 70% of the load shed (second graph from the top) between 13:00 and 14:00, 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. These results were validated using the HELICS cosimulation platform at PNNL (see *SI Appendix*, section 11.A for details). Additional validation results using HELICS and LTDES are included in *SI Appendix*, sections 15.C and 15.F.1, respectively.

4.5.2. Critical loads aggregated in a single zone. In this case, the SA from EUREICA helps the reconfiguration algorithm to disconnect or open the switches 18 to 135 and 151 to 300 to island zone 3 and pick up only the critical loads in this zone using the DG at node 48, which is a total of 430 kW. The results from this case are shown in Fig. 16. These results were validated using the DERIM and ADMS-DOTS software at LTDES (see *SI Appendix*, section 11.C for details). Additional results are included in *SI Appendix*, section 15.F.2.

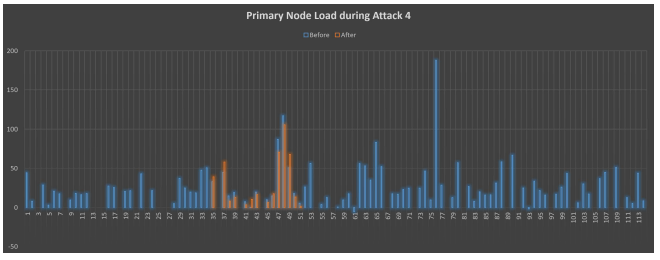

Fig. 16. Primary node load change between 12:59 (before) and 13:00 (after attack).

4.5.3. Mitigation with a military microgrid. We assume that there is a military microgrid at node 66 in the primary circuit, which serves as a backup directly in the distribution system. Under current regulations, defense critical systems have to be disconnected and isolated in the event of contingencies. Since EUREICA has the ability to identify trusted resources, our thesis is that there is confidence in the security of this resource as well as in meeting the power flow requirements, making it feasible to use this additional resource for attack 3 mitigation. First, the fault is isolated using reconfiguration based on the algorithm described in *SI Appendix*, Fig. S10. The reconfiguration algorithm returns the most resilient path for implementation, in this case, only one feasible path is present, so that is chosen. This islands the feeder by opening the switch between nodes 150 and 149 and connecting the switches to the DG and microgrid at nodes 48 and 66, respectively. Then, a combination of ≈1.7 MW from the microgrid at node 66, 560 kW from the DG at node 48,

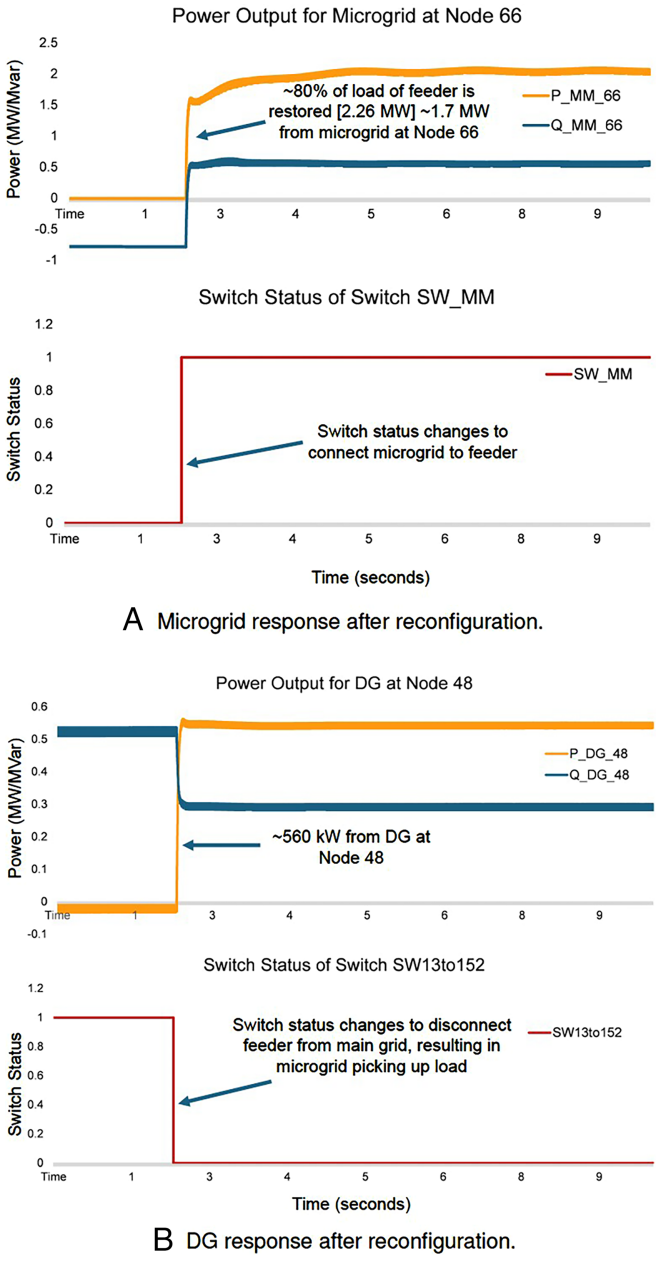

Fig. 17. System response after reconfiguration with microgrid.

and customer-side DR is utilized to pick up approximately 80% of the total load of the feeder. Some results from this case are shown in Fig. 17, validated using the ARIES platform at NREL (see *SI Appendix*, section 11.B for details). The complete set of results can be found in *SI Appendix*, section 15.H.

5. Summary

We have proposed a framework, EUREICA, for achieving grid resilience through the coordination of IoT-Coordinated Assets that are trustable. A local electricity market that has been previously shown to lead to grid reliability and provide services such as voltage support and overall power balance, is leveraged in this framework to ensure grid resilience. The local market accomplishes this through SA to colocated operators. This SA consists of information about DERs and their power injections, as well as their levels of trustability, commitment, and resilience. With this SA, we have shown that a range of cyberattacks can be mitigated using local trustable resources without stressing the bulk grid. The demonstrations have been carried out using a variety of platforms with high fidelity, hardware-in-the-loop, and utility-friendly validation software.

Data, Materials, and Software Availability. Simulation model, inputs, and results have been deposited in Zenodo (PNAS_2024_Grid_Resilience, https://doi.org/10.5281/zenodo.12793876) (44).

ACKNOWLEDGMENTS. This work was supported by the US Department of Energy under Award DOE-OE0000920 and the Massachusetts Institute of Technology (MIT) Energy Initiative. We gratefully acknowledge several useful discussions with Karan Kalsi at Pacific Northwest National Laboratory (PNNL), and Rob Hovsapian at National Renewable Energy Laboratory (NREL). V.J.N. would like to acknowledge the support of a summer internship at NREL.

Author affiliations: [a]Department of Mechanical Engineering, MIT, Cambridge, MA 02139; [b]Department of Electrical Engineering, Indian Institute of Technology Delhi, 110016, India; [c]National Renewable Energy Laboratory, Golden, CO 80401; [d]West Virginia University, Morgantown, WV 26506; [e]Pacific Northwest National Laboratory, Richland, WA 99354; [f]Larsen & Toubro Digital Energy Solutions, Fairfield, CA 94534; [g]Office of Electricity, Department of Energy, Washington, DC 20585; [h]Princeton University, Princeton, NJ 08544; and [i]Department of Civil and Environmental Engineering, MIT, Cambridge, MA 02139

1. NASEM, *Enhancing, The Resilience of the Nation's Electricity System* (The National Academies Press, Washington, DC, 2017).
2. CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) (2022). https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/ (Accessed 10 April 2024).
3. T. Nguyen *et al*., Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access* **8**, 87592–87608 (2020).
4. D. E. Whitehead, K. Owens, D. Gammel, J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies" in *Proceedings of the 2017 70th Annual Conference for Protective Relay Engineers (CPRE)* (IEEE, 2017), pp. 1–8.
5. NASEM, *The Role of Net Metering in the Evolving Electricity System* (The National Academies Press, Washington, DC, 2023).
6. V. J. Nair, V. Venkataramanan, R. Haider, A. M. Annaswamy, A hierarchical local electricity market for a der-rich grid edge. *IEEE Trans. Smart Grid* **14**, 1353–1366 (2022).
7. L. Kristov, P. De Martini, J. D. Taft, A tale of two visions: Designing a decentralized transactive electric system. *IEEE Power Energy Mag.* **14**, 63–69 (2016).
8. T. Chen, Q. Alsafasfeh, H. Pourbabak, W. Su, The next-generation us retail electricity market with customers and prosumers-A bibliographical survey. *Energies* **11**, 8 (2018).
9. S. Bjarghov *et al*., Developments and challenges in local electricity markets: A comprehensive review. *IEEE Access* **9**, 58910–58943 (2021).
10. T. Sousa *et al*., Peer-to-peer and community-based markets: A comprehensive review. *Renew. Sustain. Energy Rev.* **104**, 367–378 (2019).
11. T. Pinto, Z. Vale, S. Widergren, Eds., *Local Electricity Markets.* (Academic Press, 2021), pp i–iii.
12. Utility Dive, Coned virtual power plant shows how New York's rev is reforming utility practices (2016). https://www.utilitydive.com/news/coned-virtual-power-plant-shows-how-new-yorks-rev-is-reforming-utility-pra/421053/ (Accessed 28 March 2024).
13. A. Lüth, J. Weibezahn, J. M. Zepter, On distributional effects in local electricity market designs-evidence from a German case study. *Energies* **13**, 1993 (2020).
14. R. Haider *et al*., Reinventing the utility for distributed energy resources: A proposal for retail electricity markets. *Adv. Appl. Energy* **2**, 100026 (2021).
15. S. M. Dibaji *et al*., A systems and control perspective of CPS security. *Annu. Rev. Control.* **47**, 394–411 (2019).
16. C. D. Brummitt, R. M. D'Souza, E. A. Leicht, Suppressing cascades of load in interdependent networks. *Proc. Natl. Acad. Sci. U.S.A.* **109**, E680–E689 (2012).
17. Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, Y. Al-Turki, Networked microgrids for enhancing the power system resilience. *Proc. IEEE* **105**, 1289–1310 (2017).
18. Y. Li, X. Wei, Y. Li, Z. Dong, M. Shahidehpour, Detection of false data injection attacks in smart grid: A secure federated deep learning approach. *IEEE Trans. Smart Grid* **13**, 4862–4872 (2022).
19. T. Shekari, A. A. Cardenas, R. Beyah, "MaDIoT 2.0: Modern High-Wattage IoT botnet attacks and defenses" in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)* (USENIX Association, Boston, MA, 2022), pp. 3539–3556.
20. P. Eder-Neuhauser, T. Zseby, J. Fabini, G. Vormayr, Cyber attack models for smart grid environments. *Sustain. Energy Grids Netw.* **12**, 10–29 (2017).
21. H. He, J. Yan, Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber Phys. Syst. Theory Appl.* **1**, 13–27 (2016).
22. V. J. 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).
23. V. J. 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, 2023), pp. 32–39.
24. S. S. Amiri, M. Rahmani, J. D. McDonald, "An updated review on distribution management systems within a smart grid structure" in *Proceedings of the 2021 11th Smart Grid Conference (SGC)* (IEEE, 2021), pp. 1–5.
25. K. A. Horowitz *et al*., "An overview of distributed energy resource (der) interconnection: Current practices and emerging solutions" (Tech. Rep. NREL/TP-6A20-72102, National Renewable Energy Lab. (NREL), Golden, CO, 2019).
26. P. Srivastava *et al*., Voltage regulation in distribution grids: A survey. *Annu. Rev. Control.* **55**, 165–181 (2023).
27. K. Zetter, Inside the cunning, unprecedented hack of ukraine's power grid (2018). https://www.wired.com/2016/03/inside-cunningunprecedented-hack-ukraines-power-grid/ (Accessed 11 April 2024).
28. J. Kennedy, Dragonfly: Western energy sector targeted by sophisticated attack group (2017). https://www.symantec.com/blogs/threatintelligence/dragonfly-energy-sector-cyber-attacks (Accessed 10 April 2024).
29. R. M. Lee, M. J. Assante, T. Conway, "ICS defense use case: Analysis of the cyber attack on the Ukrainian power grid" (Tech. Rep., Electricity Information Sharing and Analysis Center, SANS ICS, 2016), vol. 388, p. 3.
30. M. Zeller, "Myth or reality - does the aurora vulnerability pose a risk to my generator?" in *Proceedings of the 64th Annual Conference for Protective Relay Engineers* (2011), pp. 130–136.
31. S. Soltan, P. Mittal, H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid" in *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)* (USENIX Association, Baltimore, MD, 2018), pp. 15–32.
32. B. Huang, A. A. Cardenas, R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks" in *Proceedings of the 28th USENIX Security Symposium (USENIX Security 19)* (USENIX Association, Santa Clara, CA, 2019), pp. 1115–1132.
33. W. W. Hogan, *Independent System Operator: Pricing and Flexibility in a Competitive Electricity Market* (Center for Business and Government, J. F. Kennedy School of Government, Harvard University, MA, 1998).
34. V. Venkataramanan, S. Kaza, A. M. Annaswamy, Der forecast using privacy-preserving federated learning. *IEEE Internet Things J.* **10**, 2046–2055 (2022).
35. P. S. Sarker, S. K. Sadanandan, A. K. Srivastava, Resiliency metrics for monitoring and analysis of cyber-power distribution system with IoTs. *IEEE Internet Things J.* **10**, 7469–7479 (2023).
36. C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., S. Havlin, H. J. Herrmann, Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. U.S.A.* **108**, 3838–3841 (2011).
37. D. K. Molzahn, I. A. Hiskens, "A survey of relaxations and approximations of the power flow equations" in *Foundations and Trends in Electric Energy Systems*, M. D. Ilic, Ed. (Publishers Inc., 2019), vol. 4, pp. 1–221.
38. G. Ferro, M. Robba, D. D'Achiardi, R. Haider, A. M. Annaswamy, A distributed approach to the Optimal Power Flow problem for unbalanced and mesh networks. *IFAC-PapersOnLine* **53**, 13287–13292 (2020).
39. J. J. Romvary, G. Ferro, R. Haider, A. M. Annaswamy, A proximal atomic coordination algorithm for distributed optimization. *IEEE Trans. Autom. Control* **67**, 646–661 (2022).
40. G. Ferro, M. Robba, R. Haider, A. M. Annaswamy, A distributed-optimization-based architecture for management of interconnected energy hubs. *IEEE Trans. on Control Netw. Syst.* **9**, 1704–1716 (2022).
41. R. Meyur *et al*., Ensembles of realistic power distribution networks. *Proc. Natl. Acad. Sci. U.S.A.* **119**, e2205772119 (2022).
42. First cyberattack on solar, wind assets revealed widespread grid weaknesses (2019). https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/ (Accessed 14 April 2024).
43. P. Kundur, *Power System Stability* (CRC Press, New York, 2007), vol. 10.
44. V. J. Nair, Data from "PNAS_2024_Grid_Resilience." Zenodo. https://doi.org/10.5281/zenodo.12793876. Deposited 17 January 2025.