What Role Do Aggregators Play in Power System Security and Resilience?

Preprint

Reiko Matsuda-Dunn,[1] Laura Leddy,[1] Eliza Hotchkiss,[1, 2]
Mukesh Gautam,[3] and Michael Abdelmalak[3]

1 National Renewable Energy Laboratory
2 Colorado School of Mines
3 University of Nevada at Reno

Presented at 2023 Resilience Week (RWS)
National Harbor, Maryland
November 27-30, 2023

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

Conference Paper
NREL/CP-6A40-85649
November 2023

Contract No. DE-AC36-08GO28308

What Role Do Aggregators Play in Power System Security and Resilience?

Preprint

Reiko Matsuda-Dunn,[1] Laura Leddy,[1] Eliza Hotchkiss,[1, 2]
Mukesh Gautam,[3] and Michael Abdelmalak[3]

1 National Renewable Energy Laboratory
2 Colorado School of Mines
3 University of Nevada at Reno

Suggested Citation
Matsuda-Dunn, Reiko, Laura Leddy, Eliza Hotchkiss, Mukesh Gautam, and Michael Abdelmalak. 2023. *What Role Do Aggregators Play in Power System Security and Resilience? Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-6A40-85649. https://www.nrel.gov/docs/fy23osti/85649.pdf.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-6A40-85649
November 2023

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported in part by the U.S. Department of Energy's National Renewable Energy Laboratory (NREL) and by the U.S. National Science Foundation (NSF) under Grant NSF 1847578. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

What Role Do Aggregators Play in Power System Security and Resilience?

Reiko Matsuda-Dunn*, Laura Leddy*, Eliza Hotchkiss* *Member, IEEE*, Mukesh Gautam‡, and Michael Abdelmalak
‡ *Member, IEEE*
*National Renewable Energy Laboratory, Golden, CO 80401 USA
†Advanced Energy Systems PhD Program, Colorado School of Mines, Colorado School of Mines, Golden, CO 80401, USA
‡Department of Electrical and Biomedical Engineering, University of Nevada at Reno, Reno, NV 89557, USA

***Abstract*—Barriers to the participation of distributed energy resources (DERs) in wholesale electricity markets have limited the use of DERs for power system security and resilience. In September 2020, the Federal Energy Regulatory Commission (FERC) approved an order to reduce these barriers. FERC Order No. 2222 enables the participation of DER aggregators in wholesale electricity markets. DERs include renewable generation and technologies that support the integration of renewable generation by increasing grid flexibility and resilience. Requiring wholesale energy markets to allow DER aggregator participation provides a path for DERs to become competitive in these markets. As the contribution from aggregated DERs continues to increase, the aggregator's role in supporting grid security and resilience will become more critical. This paper reviews work that demonstrates how DER aggregators can provide resilience support through technical capabilities, operational strategies, and secure communication architectures. Socioeconomic influences and impacts of aggregators, including implications for social resilience, are presented. In surveying the current state-of-the-art across different but interconnected topics, we illustrate how aggregators can be power system participants that enhance grid security. There is no one-size-fits-all approach to enhancing resilience in a power grid that includes a growing cohort of DER aggregators, but there are many options for aggregators to contribute to a more resilient and secure power grid.**

***Index Terms*—Aggregator, cybersecurity, distributed energy resources, energy security, resilience**

I. INTRODUCTION

The power grid is undergoing rapid and exciting changes, largely driven by the integration of renewable generation and the technologies that complement renewables by providing flexibility and energy storage. Distributed energy resources (DERs) are small-scale electrical energy resources connected at the distribution side of the power grid. DERs include renewable resources, such as solar photovoltaic (PV) and wind energy technologies, and flexible resources that complement them—such as energy storage systems, electric vehicles (EVs), and flexible loads—in the distribution system. The increasing integration of DERs promotes a more renewable power grid and, if appropriately managed and controlled, can lead to a more resilient system with increasingly distributed and diversified generation that is less susceptible to physical fuel supply issues [1]. The National Renewable Energy Laboratory (NREL) defines *resilience* as "a system's ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions through sustainable, adaptable, and holistic planning and technical solutions" [2]. Throughout this work, we consider the ways that DER aggregators can enhance power system resilience by harnessing the capabilities of DERs.

Integrating DERs also increases the complexity of the power grid, necessitating technological innovations to support grid modernization. As DERs increase in number, the interconnection and interoperability of these resources becomes essential to the health of the power grid. Interconnection and interoperability will necessitate computer-dependent communication and computation, possibly through centralized control schemes. If the increasing numbers of DER devices are to provide grid services, coordination will be required to meet the needs of the grid [3]. Aggregation is an opportunity to coordinate the capabilities of DERs to meet bulk power system (BPS) needs while encouraging the integration of renewable generation.

Here, we use the definition of aggregation from the MIT and IIT Comillas study *Utility of the Future*. Aggregation is "the act of grouping distinct agents in a power system (i.e., consumers, producers, prosumers, or any mix thereof) to act as a single entity when engaging in power system markets (whether wholesale or retail) or selling services to the system operator(s)" [4]. When participating in electricity markets, the aggregated capabilities of one or more (possibly heterogeneous) DER components can be coordinated and dispatched according to market signals. A third-party aggregator serves as a facilitator between the aggregation and the utilities requiring the services offered by the DERs in their fleet, making them a DER aggregator [5].

Recent events have created opportunities to define the role that aggregators will play as new stakeholders in the power system. In September 2020, the Federal Energy Regulatory Commission (FERC) issued Order No. 2222, mandating that regional transmission organizations (RTOs) and independent system operators (ISOs) enable the participation of DER aggregators in wholesale electricity markets, including energy, capacity, and ancillary service markets [6]. The order aims to

---

This work was supported in part by the U.S. Department of Energy's National Renewable Energy Laboratory (NREL) and by the U.S. National Science Foundation (NSF) under Grant NSF 1847578.

foster market competition, to increase the precision and clarity of market rules, and to create an equitable environment for DERs, including behind-the-meter (BTM) resources. Because of FERC Order No. 2222, these relatively new entities are able to offer services and, like conventional thermal generation, play an essential role in maintaining power system security and resilience. This work explores the ways that aggregators can contribute to the power system's ability to anticipate, withstand, and recover from changing conditions. We review the potential for DER aggregations to support grid stability before, during, and after disruptive events, such as natural or human-driven disasters.

As DERs are increasingly integrated into the power grid and connected to the Internet, more Internet of Things (IoT) devices are integrated into a cyber-physical power system that had previously been insulated from such a high degree of direct connection to a public infrastructure. DERs are often described as increasing the attack surface area of the power grid [7]–[10]. Because DERs are small, typically producing less than 10 MW of power, malicious command and control or other detrimental modes of operation of an individual DER might have minimal impacts on grid operations; however, the impacts of maliciously or erroneously controlled systems in aggregate can have much greater impacts on grid stability and resilience [9], [11].

The modern power grid is a complex, rapidly evolving system of various stakeholders. Roles and responsibilities regarding cybersecurity policies lack clarity and consensus [12]. The expected growth of aggregators, supported, in part, by the approval of FERC Order No. 2222, introduces an opportunity to evaluate the role and impact of the centralized control of many small DER systems on power system resilience and security. This paper seeks to identify the technological, operational, and socioeconomic opportunities and challenges that aggregators face to enhance grid resilience.

We identify concrete measures that aggregators can implement in various components of their system and in aggregation operation to enhance grid resilience. We also identify research gaps and define unknowns that can be addressed to build confidence in the safety and resilience of a grid reliant on aggregator contributions. While previous work exists to document comprehensive cybersecurity considerations for aggregators [9], this paper takes a holistic view of the various capabilities different aggregators might have and the resulting strategies they can implement to improve system resilience in the face of human-driven and natural hazards. We synthesize work that considers state-of-the-art technologies, as well as work that anticipates vulnerabilities that aggregations could introduce, to document the overall potential of aggregators to provide security and resilience.

The remainder of the paper is organized as follows: Section II addresses the operational strategies for aggregators, including coordination with ISOs/RTOs and utilities. Section III discusses the potential of aggregations to support resilience, including the types of services that DER aggregations are capable of supplying and the gaps that must be addressed. Section IV describes the controls and communication networks necessary to provide grid services. Because power system security and resilience rely on the cybersecurity of increasingly interconnected systems, this section also reviews the mitigations aggregators can use to ensure a secure communication network. Finally, Section V examines the socioeconomic implications and benefits of aggregators, including considerations of social resilience and equity.

II. OPERATIONAL STRATEGIES FOR AGGREGATORS

The role of aggregators in the power system will be shaped by the transmission system operator (TSO) in the area in which they operate. RTO/ISO compliance filings for FERC Order No. 2222 require tight coordination among the aggregator, the RTO/ISO, and the distribution utilities [13]–[16]. As will be discussed in sections III and III-C, this interagency coordination is crucial for safe grid operations, particularly in the face of disturbances and unplanned events, and it can enable additional capabilities to support resilience; therefore, the role of the aggregator in resilience includes coordination with the RTO/ISO and the distribution utility.

The requirement that aggregators coordinate with RTOs/ISOs and distribution utilities makes operational considerations a key component of resilient DER aggregation. Coordination is essential because aggregators lack full visibility into existing grid models, constraints, and technical boundaries. In particular, better coordination between DER aggregators and utilities can help aggregators avoid potential violations related to network congestion, voltage, and protection issues [17].

With adequate coordination and correct implementation, aggregation can provide important operational benefits over many individual DER components operating independently. These benefits include reducing the number of individual DERs that system operators need to maintain and improving grid services, such as frequency response, load shifting, and voltage regulation [18], [19]. We discuss the role of DER aggregators in grid resilience at greater length in Section III, but aggregation can help enable grid services at both the system and device levels [17]. To provide these benefits and services, however, it is essential to optimize DER aggregation operations. Two important operational considerations for aggregators are developing resilient control strategies and dealing with uncertainty.

A. *Resilient Control Strategies*

DER aggregation comes in a variety of forms, so there are a myriad of potential control strategies for DER aggregators. Resilient control strategies support an energy system's ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions [2]. Three control strategies are considered here to support operational resilience for DER aggregation: 1) use case prioritization, 2) hierarchical control architectures, and 3) distributed energy resource management systems (DERMS). The literature on DERMS in particular is rapidly expanding. In this section, we review the operational needs and challenges related to DERMS implementation. In Section IV, we then explore how DERMS can help support the technical requirements for DER aggregation and resilience features.

Use case prioritization is the process of identifying and ranking potential use cases based on business and strategic objectives [20]. In an analysis of five case studies for utility-led DER aggregation in the United States, Cook et al. discuss the potential benefits of use case prioritization for DER aggregators [19]. One of the study's participating utilities tested the impact of aggregation on six use cases, ranging from load shifting to PV firming. PV firming is the reduction in the ramp rate of the PV power output, which is beneficial because large fluctuations in PV power output can result in voltage instability [21], [22]. Because the utility's use cases serve different (or even cross-) purposes, a prioritization process can help clarify how aggregation affects the utility's top one or two business objectives. In prioritizing potential use cases, the utility could emphasize customer value to help influence customer interest in next-generation programs [19].

Hierarchical control architectures can also help maximize the benefits of aggregation to customers and the broader grid. A hierarchical control system consists of devices and software arranged in layers, with some layers overriding or supervising the actions of others [23]. Utkarsh et al. propose a control system with a home energy management system (HEMS) at the lowest computational layer, aggregators at the middle layer, and the utility controller at the highest level. Each controller in the hierarchy helps maximize the benefits of aggregation by evaluating the flexibility of DERs and providing optimal set points for DERs to best support the distribution system in providing grid services [24]. This hierarchical control architecture reiterates the need for tight coordination between DER aggregators and distribution utilities.

It is also essential to ensure flexibility—or the ability to respond to changes in demand and supply—in hierarchical control arrangements [25]. Control structure flexibility improves operations in normal conditions and in times of system stress due to changing conditions caused by natural or human-driven hazards. It also provides cost savings for aggregators and DER asset owners. Such flexibility can be optimized to maximize a community's energy independence from the distribution feeder [24]. Further research is needed into the potential role of community DER aggregators for energy security and resilience.

As both an operational and technical tool, a DERMS has an outsize role to play in resilient DER aggregator control strategies. The definition of a DERMS is broad, encompassing everything from virtual power plants to centralized enterprise systems, such as utility or grid DERMs. In all cases, however, a DERMS can be considered a logical entity rather than a physical platform [17].

Both challenges and opportunities are associated with DERMS implementation for aggregators. Cook et al. cite DERMS development and deployment as some of the major challenges for utilities trying to implement aggregation programs [19]. Three of the five participating utilities experienced challenges with developing DERMS software to control disparate DER technologies and participants, demonstrating the operational significance of system-level complexity. DERMS developers also operate on different processes and timelines from one another, so it is essential for DER aggregators to select vendors that provide both functionality and a timeline that aligns with the aggregator's goals and scheduling needs. When implemented correctly, however, DERMS can help improve operational flexibility via refined load and generation forecasting methods and the development of DER optimizations, especially during abnormal DER switching configurations.

Any discussion of aggregation control strategies must also consider that DER aggregation combines both human and technical networks. Because people represent the first transition point between the cyber and physical worlds, basic human-side mitigations are essential for resilient operations [26]. Examples of mitigation solutions include operator capacity building, training, and other workforce development activities.

B. Addressing Uncertainty

One of the most difficult questions for aggregators to address is how to operate under uncertainty. From an operational perspective, there are multiple sources of uncertainty for DERs. These include intermittent electricity generation as well as questions related to electricity consumption and the generation reliability of DER asset owners [18], [27]. Yet aggregation itself can help solve some of these uncertainties. The fundamental value of aggregation is in upscaling and diversifying DERs to mitigate the network impact of increased DER penetrations [18]. DER aggregation can also help address issues of intermittent electricity generation by allowing a single aggregation to leverage both battery and distributed generation sources [28].

The best way to deal with uncertainty is through timely and accurate data. Aggregators require data for weather forecasts, load projections, and wholesale prices. By merging distributed generation and load forecasting, aggregators can obtain net load forecasts that help increase visibility into demand-side variations [29]. Coordination between the DER aggregator and the utility DERMS can also help facilitate near-real-time communications and data exchange, allowing system operators more insight into BTM DERs and customer-related management needs [17].

Specific control strategies can also help optimize DER aggregator performance under conditions of uncertainty. Zakernezhad et al. propose one such control strategy, optimal resilient operational scheduling [27]. The optimal resilient operational scheduling framework combines three levels of optimization: 1) day-ahead scheduling of DERs, 2) real-time market scheduling of DERs, and 3) the simulation of preventive and corrective actions for external shocks. When tested on a modified 123-bus system, optimal resilient operational scheduling reduced the expected cost by approximately 75% for the worst-case external shock.

III. PHYSICAL RESILIENCE CAPABILITIES OF AGGREGATED RESOURCES

There are many ways in which DERs can support grid resilience in the face of contingencies such as a failure of power system assets or major unplanned outages. This section reviews the DER configurations and responses that can support grid services and how the aggregator can further enable DERs to support grid resilience. Grid services provide resilience by stabilizing the power grid during disruptions [1], allowing for faster recovery and possibly preventing additional contingencies caused by abnormal voltage and frequency deviations [30], [31]. In practice, the aggregator's ability to provide grid support will be determined by the TSO in which they operate. NYISO, for example, does not permit DER aggregators to offer voltage support, but other ancillary services may be provided [13]. Other RTOs/ISOs do not specify such restrictions. In general, DER aggregators are explicitly permitted to offer grid services in the RTO/ISO markets [13]–[16].

An aggregator can support the management of each function described here by documenting the capabilities of each component DER in their fleet and by providing situational awareness to the utility. IEEE 2030.11, the *Guide for DERMS Functional Specification*, advises that DER device registration information should include device settings and interconnection ratings, such as volt-var, volt-watt, frequency droop, and ride-through settings [30]. Because DERMS are critical platforms to the implementation of aggregation, an aggregator will have access to this registration information. The influence of these capabilities on a DER aggregator's performance in abnormal operating conditions is important to consider. In some cases, there might be an opportunity to configure these capabilities to optimize the performance of a DER aggregator during and after disruptions. All aggregators might not have that capability, but an aggregator can provide the necessary information to anticipate the response of their DER fleet. FERC Order No. 2222 proposes that distribution utilities have the opportunity to review the individual resources enrolled in a DER aggregator before they are allowed to participate in wholesale markets [6]. This process can provide the utility with the information that is needed to better anticipate DER aggregation behavior in all conditions.

Variation in physical aggregator capabilities dictate the aggregator's role in resilience by determining their potential to help a system withstand, absorb, and recover from changing grid conditions, but effective coordination with utilities can always support system resilience by enhancing its ability to anticipate the impacts of changing grid conditions.

A. Ride-Through

Inverter-based resources (IBRs) that trip as a result of a disturbance that causes abnormal frequency or voltage can exacerbate the impact of that disturbance. In a scenario in which IBRs trip because of a lack of proper ride-through settings, there will be a loss of generation when it is most needed. This could result in more widespread and severe outages. Extreme examples include the 2022 Odessa Disturbance in Texas and the 2016 Blue Cut Fire in California [32], [33]. Both events highlight the contribution of IBRs to grid stability and the consequences of additional generation tripping when it is most needed. Both incidents involved the tripping of IBRs connected to the BPS, but multiple events in which significant amounts (46–145 MW) of DERs tripped as a result of a fault have also been reported [34]. As the presence of inverter-based DERs increases, so does their influence on system stability in the face of contingencies and natural disasters. Ride-through performance for all IBRs is critical to a system's ability to withstand and recover from disturbances [35].

The Electric Power Research Institute, NREL, and Sandia National Laboratories coordinated to conduct a stability analysis of various faults modeled in California to inform California Rule 21, which requires inverter-based DERs to ride through disturbances [36]. The results demonstrate that system stability increases when inverter-based DERs ride through faults. Aggregators can collect information on inverter-based DER component ride-through capabilities and settings and can possibly influence owners to adjust these configurations to ride through different types of disturbances.

B. Grid Services and Resilience

Grid services have been identified as technologies critical for grid resilience [1]. Reserves, frequency regulation, and voltage regulation stabilize the grid during and after a disruption [37], and there are pathways for aggregators to enhance the ability of DERs to provide grid services. The U.S. Department of Energy's (DOE's) Grid Modernization Laboratory Consortium identified the harmonization of requirements for interconnection and interoperability standards for DERs as a gap that limits the contribution of DERs to grid services [38]. Inverter-based DER owners might not be incentivized to configure their devices to provide such services because the owners would be required to reduce the maximum active power output of the DERs to do so [39]. Work by Giraldez et al. shows that these reductions in active power production can be negligible, and the DER owner can benefit more from improved grid health [40], but customer perception might not reflect this. Aggregators have the potential to influence customer perception, to provide incentives—such as a path for participation in ancillary service markets—and to coordinate grid services that require aggregate device behavior, such as reserves.

More research can shed light on an aggregation's ability to further enable grid services, both via collective DERs and at the local device level, by ensuring effective management of advanced inverter functions. If managed well, aggregated DERs, particularly DER aggregations with large portions of IBRs, could respond to grid disturbances faster than conventional, thermal generation [31]. Although large penetrations of IBRs have the potential to create a grid that can be more quickly stabilized and is more resilient to emergent conditions than a grid largely comprising synchronous machines [41], IBRs must use properly programmed advanced inverter functions to do so. Large penetrations of aggregated IBRs could amplify the potential stabilizing or destabilizing effects of IBR integration. Aggregators can survey DER components in their fleet, provide insight into the physical capabilities and programming of IBR components, and possibly even influence these characteristics if these components cannot participate in an aggregation without meeting certain specifications. Each class of grid services an aggregation could offer to support resilience is considered next:

(a) Reserves: DERs can serve as generation capacity when demand exceeds the scheduled energy supply [38]. IEEE 1547-2018 specifies that DERs shall be capable of operating at a limited percentage of nameplate capacity to provide additional power when needed [42]. This operation mode allows DERs to act as spinning reserves. RTOs and ISOs anticipate the use of DER aggregations as spinning and contingency reserves in FERC Order No. 2222 compliance filings.

The capability of DERs to provide reserves is outlined in [43], which presents a coalitional game theoretic approach for allocating total reserves among different DERs. In addition, the deployment of DERs for contingency studies is investigated and presented in [44]. Strezoski et al. demonstrate a utility dispatching aggregated DERs to meet a sudden imbalance in demand [17]. This is made possible by information provided by the aggregator DERMS and close coordination with the utility.

DER components do not need to be IBRs to provide reserves. Aggregated DERs can reduce load via demand response [45], [46]. Utkarsh et al. examine a system that enables aggregators to coordinate with utilities and HEMS to determine BTM DER flexibility [24]. Critical loads are identified, and in the case of an outage, the utility can coordinate with the aggregator to reduce the load via aggregator control of the HEMS. Load minimization, combined with optimized PV and battery operation, reduced the power import from the distribution feeder to nearly zero [24].

(b) Voltage Support: System voltage regulation has been shown to provide resilience. Noguera et al. demonstrate improved system performance and adaptability during a contingency scenario due to voltage regulation [47]. Nikoobakht et al. demonstrate improved system performance during an extreme hurricane event resulting from voltage control [48]. In this study, voltage control minimizes the impact due to N-k contingencies, including the reduction of load loss and operational cost.

Inverter-based DERs can provide voltage regulation services by adjusting the active and reactive power output [49]. Because of the strong coupling of voltage and reactive power, various voltage control devices are used to inject reactive power into the grid for voltage regulation and control. IEEE 1547-2018 enables the use of local inverter-based DERs to keep the grid voltage within specified limits by exploiting their computational, monitoring, and communication functionalities [42]. Such adjustments can be triggered by either local conditions (i.e., physical measurements at the inverter terminal trigger adjustments in the power output via preprogrammed inverter functions) or by communications [38]. The rate of response depends on whether voltage control is implemented at the local device level (autonomously) or via communications from a control center. Centralized control schemes are impacted by communication latency, but these schemes can take advantage of optimizing the response of inverter-based DERs based on the conditions of the entire system [31].

Various advanced inverter functions can accomplish voltage support. Inverter-based DERs can be programmed to inject or absorb reactive power (volt-var function) or curtail active power (volt-watt function) based on the voltage measurements at the inverter terminal [49]. Although these are autonomous functions, i.e., controlled at the device level, they can be updated, enabled, or disabled through communications such as those that aggregators might use. Power factor functions that adjust the reactive power in proportion to the active power output can also help regulate voltage. These can maintain a constant preprogrammed power factor or use a power factor profile that is informed by site-specific, historical voltage profiles. These power factor profiles can also be updated remotely. The frequency of these power factor updates is critical to their efficacy. Aggregators can enhance voltage support by accounting for the various voltage regulation functions enabled in their fleet of inverter-based DERs, and they can improve the efficiency and coordination of the aggregate voltage support by preprogramming or dispatching optimized parameters for such functions.

(c) Frequency Support: Frequency deviation occurs in power systems when the generation and load are out of balance. It can occur because of a variety of reasons, including faults, significant load variations, generating unit tripping, and islanding areas of the grid. Frequency regulating methods are used in these situations to offset frequency variations [43]. Frequency regulation supports resilience by adjusting to system stress and maintaining system health during such disturbances [50]. Conventionally, the inertia of synchronous generating units (not IBRs) and automatic generation control (AGC) have been used for frequency regulation in power systems. IBRs have quicker dynamics than conventional generators, which makes them suited for faster reserve allocation—if they are programmed to respond appropriately.

Similar to the voltage support functions, IBRs can support frequency regulation by adjusting their active power injection according to the frequency measurements (frequency-watt function). In an underfrequency scenario, IBRs cannot operate at 100% capacity to provide this service [49]. IBRs can use frequency-droop functions to provide ”synthetic” inertia in case of a precipitous drop in frequency. These functions can respond to a rate of change of frequency (ROCOF), e.g., an increase in active power in response to a ROCOF below a certain threshold. Alternatively, they can respond to a deviation from nominal frequency, e.g., an increase in active power when the terminal frequency drops below a certain threshold.

As with voltage support functions, aggregators can survey resources in their network to understand the available inverter functions and to provide a sense of the frequency support and inertial response that would be produced in aggregate. More research can be done in this area to determine the efficacy of such work and to understand the required coordination between the aggregator and grid operator.

C. Capabilities of Utility-Controlled Aggregations

Thus far, we have discussed the aggregator's role in security and resilience by considering the aggregator as a market participant whose role is shaped by FERC Order No. 2222 and the RTO/ISO response. The technology that can imbue an aggregation with resilience capabilities, however, is not limited to current socioeconomic constraints. Because a utility is given the responsibility of safe and reliable distribution grid operations, as well as deep knowledge of the distribution grid, utility-controlled and managed aggregations might have more complex control schemes that benefit grid operations. This could be encouraged through implementation strategies with detailed, in-house grid awareness, or it could be simply incentivized by the utility's role in safety. Two areas of consideration for control capabilities include: a) coordinated centralized control or configuration, and b) black-start and microgrids.

(a) Coordinated Control or Configuration: When directly controlled by a distribution utility, a DER aggregator can synthesize the aggregation control and visibility with awareness of grid constraints. Research into the resilience capabilities of aggregations coordinated with grid-aware control is summarized in this section.

A utility aggregator could prescribe specific grid support functions and parameter settings and possibly update these dynamically via communications. Johnson et al. describe programming advanced inverter functions at 15-minute intervals based on renewable resource and demand response forecasts [31]. In these cases, an aggregator could coordinate with the grid operator, and improved situational awareness could increase grid reliability and resilience.

Concepcion et al. investigate the advantage of the centralized control of synthetic inertia in DERs [51]. Although the communication latency of Internet-connected DERs might be prohibitive for the provision of synthetic inertia, the authors demonstrate an improved active power response to a frequency disturbance when individual DERs adjust their active power output based on a calculated system frequency instead of the devices' terminal frequencies. The response of DERs to disturbances can be improved by system information that must be communicated from a centralized source. Johnson et al. discuss the advantages of the hybrid and centralized control of advanced inverter functions to optimize dispatch for the system based on time-sensitive information, such as the available solar resources [31]. A hybrid system is described that combines autonomous inverter-based functions for fast responses to events with centralized control for coordinated reserve dispatch.

Ardani et al. examine the increased situational awareness provided by Pacific Gas and Electric Company's (PG&E's) DERMS demonstration [52]. This utility DERMS incorporated existing advanced distribution management system applications to visualize DER generation, load, and flexibility and to display the actual and forecasted voltage of the distribution feeders. This provides enhanced situational awareness.

(b) Black-Start and Microgrids:

In addition to the operation of DERs in grid-connected mode, DERs can be operated in isolated mode by forming microgrids through the reconfiguration of distribution networks. Microgrids energized by DERs can be formed by changing the status of the sectionalizing switches and tie-switches that are present in the distribution networks after the occurrence of some power outages, which enhances the system's resilience [53]; however, the control of such microgrids can sometimes be challenging and usually necessitates sophisticated infrastructure. Even though microgrids are intended to function in islanded mode, it is anticipated that they will be capable of switching between islanded and grid-connected modes as needed. Inverter-based DERs typically function in grid-following mode when they are connected to the grid; however, operating a microgrid necessitates at least one DER operating in grid-forming mode [54].

IEEE 2030.11 suggests that aggregation can support resilience through the creation of microgrids during significant events and through black-start capabilities following outages [30]. These two capabilities require sophisticated controls, detailed knowledge of the grid, and grid-forming inverters [55]. Black-start capabilities are intertwined with microgrid implementation [56]. Because DER components are connected to a circuit that is likely shared by uncontrolled loads, ad hoc microgrids would be required to reenergize that circuit.

IV. SECURE AND INTEROPERABLE COMMUNICATION

Previous sections have addressed how aggregators can provide resilience in the face of physical hazards. Here, we discuss cyber hazards, which are of particular concern to aggregators because of the novel communication architectures they must implement. Effective coordination of DERs requires interoperability, i.e., devices and networks must be capable of reliable and timely communication with each other [38]. Aggregation will require communication-enabled DERs and a communication system that can control and monitor DERs. Aggregation communication capabilities will determine the physical resilience capabilities the aggregation can offer. Typically, such communication systems are centralized, but distributed systems have been explored as well [18]. The types of controls and their implementation will dictate the services that aggregated DERs can offer and can ensure that the control of these services is coordinated among various stakeholders, e.g., customers, aggregators, and distribution system operators (DSOs) [45].

An aggregator's central server, which might be in direct communication with a utility, will maintain communications with DER devices over the public Internet. Cybersecurity is of paramount concern because the increase in the integration of IoT devices increases the attack surface area of the power grid [7]–[11]. To date, there are no universal standards for specific implementations of cybersecurity mitigations for DERs, much less the distributed systems that will comprise an aggregator's control system and DER fleet [38], [57], [58]. There is, however, a substantial amount of research and number of recommendations regarding the relevant mitigation techniques that aggregators can employ.

This section describes common cybersecurity vulnerabilities relevant to DERs, along with considerations for aggregator communication system architecture, and implications for enhancing cyber-physical security. These solutions extend from centralized aggregator control schemes, which could incorporate a utility-aggregator communication interface, to the aggregator-DER communication network, to the network-DER device interface.

A. Known Cybersecurity Vulnerabilities and Mitigations

Frequent or continuous communications among aggregators, DERs, and/or utilities are required to manage and oversee many DER operations, including, but not limited to, those previously described. The aggregator's position as the middleman between individual DER devices and the BPS puts the aggregator in a unique security position wherein they need to protect both their connection to the DERs and their connection to the grid operator [9]. The interconnection among DERs, aggregators, and utilities requires that DERs be IoT devices. Although this can improve DER integration and possibly enhance DER functionality as a component of an aggregation, it also widens the attack surface. Further, the impact of a compromised aggregation might be much greater than that of an isolated component DER [56]. Common vulnerabilities related to the interconnection of DERs, aggregators, and utilities are enumerated in Table I, along with mitigations that have been explored in the context of power systems and IoT-connected DERs.

TABLE I
COMMON CYBERATTACKS OR COMMUNICATION SYSTEM VULNERABILITIES AND MITIGATIONS FOR CONSIDERATION IN THE AGGREGATION OF DERS VIA COMMUNICATIONS OVER THE INTERNET.

Vulnerabilities	**Mitigations**
Denial of service	Network segmentation [57]
	Moving target defense [31], [57], [59]
	Disable unused ports [9], [60]
	Access control policies [9], [61], [62]
Adversary in the middle, masquerade	Use of encryption and protocols that support encryption [9], [10]
	Protocol translation (i.e., an encrypted protocol to Modbus) [9]
	Encryption and authentication via a bump-in-the-wire device [7]
	Encryption and authentication via TLS [9]
	Encryption and authentication via IPsec [9]
	Rigorous authentication via trusted certification authorities (e.g., X.509 certificates) [9]
	Access control policies [9], [61], [62]
False data injection	Bad data detection algorithms [45], [63]
	Verification and integrity checks of incoming packets [31]
Replay	Verification and integrity checks of incoming packets [31]
Advanced inverter control error	Determine and enforce safe bounds on inverter parameters [8]
	Frequent dispatch of advanced inverter function parameters [8], [64]
Voltage and frequency instability caused by physical disturbance	Advanced inverter functions [49], [51]
	Situational awareness to properly command and update individual devices that can provide voltage and frequency support [46]
Communication latency and reliability	Situational awareness of communication network reliability, latency, and congestion [51], [52], [65]
	Frequent firmware updates such that necessary functions can be properly performed autonomously at the device level [9], [60]

(a) False Data Injection Attack: Data are gathered with the help of remote sensors located at various parts of the power grid. An attacker could manipulate sensor data in such a way that computational errors are injected into state vectors and results, and such errors remain undetected. These types of attacks are referred to as false data injection (FDI) attacks. When applied to voltage, power, or even phase angle measurements, FDI attacks can result in the injection of too much or too little power, leading to outages or even equipment damage.

(b) Man-in-the-Middle Attack: A man-in-the-middle (MITM) attack, also referred to as an adversary-in-the-middle or a machine-in-the-middle attack, involves an attacker intercepting and modifying data being transmitted between different parties. An attacker can intercept communications among DERs, aggregators, and utilities to change, omit, or fabricate the data transfer. An attacker can harm different pieces of equipment used in the power system through an MITM attack by transmitting incorrect data during communications.

(c) Masquerade Attack: Masquerading describes an attacker using legitimate credentials, possibly obtained through phishing or brute-force methods, to gain access to data or to control resources.

(d) Denial-of-Service Attack: By jamming and overloading the network, an attacker can deny intended users access to the network, resulting in a denial-of-service (DoS) attack. Attackers can target servers and obstruct legitimate requests from DERs, which results in the denial of requests from genuine DERs, during communications among DERs, aggregators, and utilities.

(e) Replay Attack: In a replay attack, the legitimate transmission of data is purposefully duplicated or delayed. This is done by either the original sender or a malicious party that intercepts the packet and resends it as a type of packet spoofing. In DER communications, data packets between component DERs and an aggregator dispatch agent are collected by an attacker [54]. The data are then modified by malware and ultimately transferred. The main objective of a replay attack is to impose a communication delay. The data communication based on Transmission Control Protocol (TCP)/Internet Protocol (IP) can reduce the DERs' susceptibility to cyberattacks via a

packet replay.

(f) Advanced Inverter Control Error: If improperly or maliciously programmed, the advanced inverter functions of IBRs that exist to mitigate voltage and frequency instability can exacerbate this vulnerability. Johnson et al. present the destabilizing effects of IBR behavior when advanced inverter function parameters are misprogrammed [8]. For instance, instead of a drop in nominal frequency that results in an increase in the active power output from a PV system, the PV system responds by decreasing the active power output, resulting in system instability.

B. Communication System Software Platforms: DERMS

Aggregators will need to implement a control system to issue commands to DERs. A DERMS that provides visibility and the ability to send dispatch signals is required to coordinate aggregated DERs [46]. The structure of this DERMS can impact communication latency and reliability, expose cybersecurity vulnerabilities, and determine the ability of aggregated DERs to provide grid services, as described in Section III. There are many examples in the literature of DERMS successfully providing grid services.

Ding et al. propose a Federated Architecture for Secure and Transactive Distributed Energy Resource Management Solutions (FAST-DERMS) [45]. This architecture is designed to meet the objectives of resilience and security. The design of FAST-DERMS emphasizes coordination and a certain degree of the distribution utilities' control of DERs, specifying that aggregators should participate in the wholesale market via the DSO to ensure adherence to grid operational constraints. FAST-DERMS is envisioned as a utility DERMS, using a flexible resource scheduler to communicate indirectly with DERs via aggregator DERMS or directly with DERs. As such, FAST-DERMS serves as an aggregation tool that enables DSOs to leverage DER components for grid services. FAST-DERMS can coordinate with third-party aggregator DERMS. In this case, an aggregator is provided with a path to offer grid services and resilient operations through optimizing coordination and interoperability with the utility DERMS.

Strezoski et al. present various case studies demonstrating the use of utility DERMS (such as FAST-DERMS) in voltage management, peak load reduction, restoration of a de-energized island, and coordinating the participation of DERs in wholesale energy markets while maintaining grid operational constraints [46]. Also included is a case study of an aggregator DERMS providing situational awareness to enhance voltage regulation and to directly curtail solar PV in the aggregator's network.

Singh et al. develop a cloud-based utility DERMS platform and examine the resilient operation of aggregated DERs in several scenarios [11]. This DER fleet consists of PV, a battery, and a substantial number of flexible load devices, such as hot water heaters. The authors model this fleet of DERs as a virtual battery, monitor its state of charge, and demonstrate the ability of the aggregated DERs to follow an AGC signal and provide secondary frequency support. The DERMS is able to control its fleet of DERs to prioritize meeting different constraints with changing conditions, such as maintaining voltage limits as opposed to managing peak loads, or switching battery systems to grid-forming mode in an outage.

Ardani et al. study PG&E's DERMS design to coordinate residential, commercial, and utility storage and residential PV to provide grid services [52]. PG&E's utility DERMS was designed to integrate third-party aggregators and was able to enhance situational awareness and dispatch DERs to eliminate capacity, reverse power flow, and over- and undervoltage violations.

Although some of the examples discussed here are utility DERMS, not necessarily aggregator DERMS (Strezoski et al. make a clear distinction [46]), the examination of utility DERMS is useful in demonstrating the mechanics of a centralized control system that enables aggregated DERs to provide grid services. Aggregator DERMS can enhance the ability of DERs to provide grid services by designing their communication systems to incorporate features of utility DERMS. Additionally, the aggregator DERMS can design their systems to provide interoperability to coordinate with a utility DERMS. To participate in ancillary service markets, aggregators will need to specify which grid services their DERMS will support and how they will communicate with individual DERs and the utility to effectively implement those grid services.

Some reviewed DERMS designs incorporate bad data detection [31], [45]. This can mitigate FDI attacks [63] along with deep packet inspection [31]. Encrypted, authenticated communications between the DERMS and the DER fleet can add another layer of protection that will also mitigate a broader set of vulnerabilities.

C. Communication System Network Architecture

Controls and measurements between DERMS and DER devices will be transmitted over the Internet instead of a dedicated communication network, introducing communication issues caused by network congestion, lack of reliability and availability, as well as dependence on an inherently less secure channel. Appropriate considerations for cybersecurity are critical with increased exposures to the vulnerabilities described in Section IV-A. Communication networks should be designed with these considerations in mind, and they should leverage the mitigations listed in Table I.

Cybersecurity measures should be implemented with awareness of their impacts on performance. The physical impacts that can result from communication latency and unreliability are discussed in Section IV-E; however, this section reviews research describing how aggregators' network architectures can impact communication quality.

Ardani et al. find increases in communication efficiency when a central controller communicates with nodes of common assets instead of individual devices, which have positive implications for performance and the implementation of network segmentation [52]. An aggregator can design a more cyber-resilient network by segmenting DERs such that adversarial control of a single DER enclave would have minimal system impact. This can be accomplished with firewalls, proxies, virtual local area networks, or virtual private networks. All these approaches can contribute to communication latency and add complexity to the implementation of a communication system. Network segmentation does not guarantee immunity to DoS attacks, but it makes them more difficult and less effective if the DoS does not impact all enclaves. DER enclaving does not mitigate DoS attacks on a centralized control center. To protect against DoS attacks, a central server would need to implement additional mitigation tactics, such as a firewall that only accepts communication from allowlisted hosts, e.g., members of the aggregator's fleet of DERs.

A moving target defense (MTD) that reconfigures a communication network by strategically and periodically reassigning IP addresses and ports can prevent malicious attempts to establish communication. Onunkwo et al. test several techniques to mitigate a wide array of cyberattacks, including network segmentation, encryption (TLS), and MTD, and calculate the communication latency incurred by each [57]. Network segmentation, implemented with hardware proxies close to each DER enclave, increases latencies by fractions of milliseconds. Encryption, on average, increases latencies ranging within a couple of milliseconds (this varies with the encryption standard used). MTD latencies vary but are on the order of milliseconds, and decreases in reliability are observed. These results likely depend on the specific implementation of the MTD, the parameters of which can be tuned to balance security with performance [59].

Preventing unauthorized access to DER systems by ensuring that only the proper users can access the data and command functions they need is essential to ensuring system-wide security. Access control systems should provide authentication of user identity, manage the authorization of each user to access permitted system functions, and ensure accountability and non-repudiation in case of an adversary intrusion [62]. In this work, Johnson emphasizes that access control policies must be dynamic to suit the changing roles and responsibilities of each stakeholder. Although different access control schemes can be used and should be explored, role-based access control has been identified as well suited to DER ecosystems, in which much of the system complexity can be defined in the user roles held by the many stakeholders (e.g., residential DER system owners, grid operators, and aggregators) [61]. Johnson provides an example of a role-based access control scheme, including a roles-to-rights mapping with specific variations depending on the communication protocol used (IEEE 1815, Modbus, and IEEE 2030.5) [62]; see Section IV-D for more details on these communication protocols. Johnson also outlines suggested requirements for future implementations, including authentication via unique user identifications and strong passwords, support for account lockouts, no password display under any circumstances, automatic logout due to user inactivity, and support for access control lists or role-based access control. Centralized and decentralized access control schemes for DERs have been investigated, with the decentralized scheme using smart contracts in the Ethereum blockchain to store and retrieve the access control model [61]. In these implementations, the decentralized scheme introduces latency, but it has different security contributions and weaknesses than the centralized scheme.

Zero trust architecture in grid operations is an emerging area that Hupp et al. identify as essential to security when users, such as residential DER owners, have remote access [66]. The national Cyber-Informed Engineering (CIE) Strategy released by DOE describes zero trust architecture as an approach that is inherently secure by design and calls for designs that ”implement a zero-trust architecture to the greatest degree possible” [67]. Unlike traditional access control schemes that assume all users operating within a certain network boundary are authorized to perform permitted functions within that boundary, trust must be continuously evaluated [68]. This dynamic evaluation of trust adds complexity but increases security. Implementation of zero trust access control schemes for DERs should be further investigated as DER devices become increasingly interconnected.

D. DER Communication Protocols

The communication protocol chosen for connection to a DER device has security implications that an entity such as an aggregator will need to consider. Here, we briefly review the security features, or lack thereof, of the three DER communication protocols specified in IEEE 1547-2018: SunSpec Modbus, IEEE 1815 (DNP3), and IEEE 2030.5 (SEP 2.0). Each protocol specifies how information is transmitted and received between hosts at every layer of communications [9].

Of the three protocols designated for DER communication, SunSpec Modbus is the most prevalent [9] and provides no inherent encryption or authentication [8]. The security of Modbus can be improved with bump-in-the-wire encryption technologies, such as those described in [7], or via protocol translation [9]. Encryption and authentication with Transport Layer Security (TLS) and Internet Protocol Security (IPsec) as well as network monitoring for unusual traffic is recommended [9].

The Common Smart Inverter Profile (CSIP) recommends IEEE 2030.5 (the default protocol for California) for communications between DERs and utilities, whether the communications occur via aggregators or over a direct connection [69]. IEEE 2030.5 requires message encryption and authentication, node authentication via digital certificates, and key management via Diffie-Hellman Ephemeral (DHE) key exchange, the classic and state-of-the-art asymmetrical public key exchange. PG&E selected IEEE 2030.5 to implement a DERMS design (see Section IV-B) and found that extensions to the protocol were required to support all targeted grid service use cases [52].

IEEE 1815 supports TLS, application layer encryption, and even mitigations for packet spoofing [9]. As with other protocols described, TLS and IPsec are recommended.

Although the aforementioned protocols can use TLS and IPsec [9], all but Modbus require X.509 certificate authentication [69]. In all cases, TLS and device authentication is encouraged [62]. Redundant encryption—i.e., encryption at multiple layers including the device or application level, the transport layer, and the network layer—enhance end-to-end security.

E. Impacts of Communication Latency on Grid Stability

The control of power system resources benefits from real-time operation. As DERs are introduced that rely on the Internet to communicate with aggregator control centers, the latency and the reliability of the Internet is also introduced to the system. Communication latency includes delays resulting from the transmission of measurements from DER devices to centralized control, the transmission of commands from centralized control to DER devices, and the subsequent time required for the devices to react to commands. Traditionally, communications from centralized control to generation occurs over dedicated networks in which latency and reliability are better understood than the stochastic nature of the public Internet. If grid services are to be performed by aggregated DERs, as discussed in Section III, this communication latency can be detrimental to the efficacy of these services because communication that can typically rely on subsecond latency might now be executed with latency on the order of seconds. A number of studies simulate the impact of communication latency on DER response in emergent conditions, e.g., mismatches in generation and load that could be caused by faults, sudden load changes, or a sudden loss of supply from a generator.

Wang et al. demonstrate that there exists a threshold beyond which AGC signals sent to DERs will result in an unstable system [70]. This threshold is on the order of a few seconds and would vary depending on the system topology and generation mix. In this instance, it is 4 seconds, which is within the typical 5-second communication latency referenced in DOE's *Modern Distribution Grid Decision Guide* [71]. Zwartscholten et al. investigate the impact of communication latency between a controller and a cluster of DERs, defined as an active distribution network [3]. DER power output is adjusted in response to disturbances of varying sizes. The authors find that for a sudden load change, a communication latency of 1.31 seconds can lead to instability in the system. Li et al. similarly examine the impacts of communication latency but look at a range of percentages of variability in latency rather than an absolute value of a specific length of time [72]. System destabilization is demonstrated as more DERs are impacted, and the authors note that network latencies would impact the control of all DERs if the control were centralized. Reno et al. examine the effect on communication latency in the centralized control of voltage-regulating functions [65]. They find that a constant power factor can contribute to voltage variability because voltage can be sensitive to the quick ramps in the reactive power output of PV systems. Voltage is stabilized if power factors can be dispatched at 1-second intervals. When volt-var functions are dispatched from a central controller, communication latencies of up to 10 seconds do not have a noticeable impact on the simulated distribution feeder.

Aggregators can mitigate the detrimental effects of communication latency by maintaining awareness of network latency and how it impacts time-sensitive communications. Lai et al. recommend such a resource assessment for DER cybersecurity [9]. Aggregators might be able to gauge which grid services can be offered via communications and how they will be implemented with an evaluation of the portion of the network they control. As shown in [3], [65], [70], and [72], a threshold for latency will depend on the type of signals being sent between the aggregator and the devices in the field as well as the network size and topology. An aggregator could leverage their familiarity with the network (from physical measurements, possibly from BTM advanced metering infrastructure data, and from measured communication latencies) to determine the best practices and protocols particular to their territory. More research is required to determine the feasibility of an aggregator producing effective protocols on a case-by-case basis, depending on each aggregator's unique set of resources.

F. Resilient Communication

IEEE 2030.11 recommends fail-safe settings for DERs [30]. If DERs can detect a loss of communication and autonomously switch to a preprogrammed mode of operation, optimized operation modes triggered by such contingencies could be an area of interesting future research. The concept of a fail-safe mode for DERs that lose connection to centralized control has not been thoroughly explored [73]. FAST-DERMS describes the need for fail-safes [45]; however, there is little work on characterizing DER aggregator performance in the case of communication loss in the presence of additional physical hazards.

V. SOCIOECONOMIC IMPLICATIONS

DER aggregators will necessarily operate within—and affect—existing U.S. economic and social structures. Following FERC Order No. 2222, the main economic question for aggregators is whether a business case exists for large-scale adoption. Important social questions also surround DER aggregators, from issues of societal resilience to best practices for equitable implementation. In this section, we first examine existing and potential market structures for DER aggregators before turning to broader social implications for resilience and equity.

A. Market Structures

From an economic perspective, DER aggregators are fundamentally market players. FERC Order No. 2222 implementation could help make aggregators key stakeholders in future electricity market bidding and energy system operations [18], [29]. Although recent policymaking helps set the stage for DER aggregator integration into the wholesale electricity market, there is much work to be done before aggregation becomes mainstream.

Following FERC Order No. 2222, the main market question is whether aggregation is economic. DER aggregators have typically operated on slim profit margins, an operating model that introduces financial challenges given the costs associated with aggregation. These costs include customer acquisition, complex equipment installations, and operations-and-maintenance costs associated with developing and maintaining management software. There is also always the risk of financial exposure as a result of nonperformance should DER aggregators fail to perform to contracted or market requirements [74].

From an end-use perspective, the most important consideration is whether aggregation benefits individual customers. The California ISO's (CAISO's) FERC Order No. 2222 compliance filing sheds light on why customers do not always perceive such benefits. In the filing, CAISO discusses the results of a 2020 survey conducted with market participants and distributed generation developers on the DER aggregator model and FERC Order No. 2222. Several respondents wrote "there is not currently a business case for DER aggregators" because of issues such as net energy metering incentives, resource adequacy ineligibility, and lack of efficient aggregation technologies [14].

Differences between retail and wholesale electricity rates are also a significant factor in California. In 2019, for example, the average retail price of electricity in the state was \$168.90/MWh—compared to an average CAISO wholesale rate of approximately \$41/MWh [14]. Small DERs that would make up a DER aggregation thus tend to prefer participation in net energy metering programs when eligible. California also presents a special case because individual, small DERs can participate in wholesale markets without the need for an aggregator model. This points to the policy challenges associated with implementing a national order across fifty U.S. states and multiple territories with a patchwork of different rules and incentives.

Customer-related aggregation issues, however, are not unique to California. In Cook et al.'s study of utility-led aggregation programs in the United States, residential recruitment and customer acquisition posed a major challenge for utilities across the nation [19]. Customer outreach, developing appropriate compensation mechanisms, and aligning DER aggregators with existing DER incentive structures are all essential pieces of the economic puzzle.

In customer outreach programs, DER aggregators need to emphasize the benefits that aggregation can bring to end users. These benefits include enabling the participation of individual or small-scale DERs in electricity markets, the potential for DERs and prosumers to engage in energy-saving and energy-efficiency programs, and the provision of demand response and load-shedding services [17]. DER aggregator models must also build in incentives such that both DER asset owners and aggregators benefit from providing regulation services to the utility [24].

Beyond articulating ratepayer cost savings, DER aggregators need to consider potential operational impacts on consumer benefits. For example, as discussed in [49], aggregator voltage regulation services could possibly induce solar energy curtailment. For DER aggregators to provide voltage and frequency regulation, any solar PV would need to operate at a power factor of less than one, meaning that production is less than the maximum amount of potential active power. This operational arrangement could result in value losses for customers, either from reducing the amount of energy they can export to the grid or from increasing the amount of energy they need to import from the grid. A potential mitigation strategy in this situation could be the use of demand response programs to lower the voltage at the customer meter, thus reducing the activation of inverter grid support functions like voltage regulation [49].

Alternative business models could help set the stage for broader and more efficient DER aggregator adoption. Potential market approaches exist for grid-integrated vehicles (i.e., EVs) to provide grid services, including: 1) leasing cars to customers, 2) providing subscription services for charging, 3) contracting with fleet owners, 4) contracting with ride share services, and 5) contracting with car rental services [75]. When asked to score the value of each of these approaches from 1 (least valuable) to 5 (most valuable), respondents in an expert survey selected "aggregators contracting with fleet owners" as the most valuable approach for aggregators to deliver grid services. In the future, grid-integrated vehicles might be an important target for aggregators as another source of DER components to integrate into their fleet. The vehicle owner will consume electricity from the grid as well as export power from the EV battery to provide grid services.

B. Social Resilience and Equity

Aggregators also have important social implications to consider, including questions of equitable implementation. The largest social resilience question relates to the impacts of extreme weather events or human-driven hazards, including a large-scale cyberattack (or ripple effects from a smaller-scale, more targeted attack). Social resilience and grid resilience are interconnected given the centrality of grid infrastructure in people's everyday lives, but we can also think about social resilience as a set of broader capacities, such as social capital, community functions, and the ability to cope with grid-related and other disruptive events [76]–[78]. Beyond the potential health and safety impacts associated with long-duration power outages from a large-scale hazardous event, there are also psychological and financial consequences. Psychological consequences might include mass panic or distrust of services, while financial fallout could occur from increased spending to restore downed systems or to secure critical services such as life-saving healthcare and emergency response, or from people being displaced and assuming economic burden [26], [79].

DER aggregators can play an important role in mitigating the effects of physical or cyberattacks on energy infrastructure. Aggregators can help maintain the security of the electricity supply, in large part by reducing any potential negative impacts of DERs on distribution networks [18]. As discussed in sections II, III, and IV, resilient DER aggregator implementation and operation can reduce risks from cybersecurity and physical threats and strengthen the capacity of aggregators to support resilient grid operations.

Cybersecurity and equity clearly intersect, as do resilient system design and equity. If a cyberattack or physically disruptive event were to occur on critical infrastructure that leads to the loss of power supply, research has shown that these outages would disproportionately affect the most socially vulnerable [79]–[81]; thus, electricity supply affects all facets of society—from the broader-scale societal system's resilience to impacts on the livelihood of the individual consumer.

The increasing role of aggregators in electricity markets also raises other important equity questions. These questions range from issues of DER access to mapping the impacts of load shedding and other grid support functions. The role of community aggregators in place-based resilience—i.e., the focus on improving resilience in a defined geographic area and in a manner that develops and enhances local knowledge and attributes—is another topic that warrants further exploration [82].

Access to DER aggregation and the benefits it can provide is one of the most pressing equity concerns for aggregators. Consumer participation in DER aggregator programs requires time and resources that might hinder participation [19]. For example, in Utkarsh et al.'s hierarchical control system report, the authors assume that every home has a rooftop PV system; a battery energy storage system; an electric water heater; and a heating, ventilating, and air-conditioning appliance [24]. These assumptions limit the applicability of the authors' control system model in low-income and energy-burdened communities that are unable to afford these appliances [83].

One way to address issues of access and equity is to integrate these considerations into the earlier-stage design of research and implementation projects. Beginning with pilot projects in public housing units is one potential method for addressing equity issues in aggregation research, especially if these pilot projects provide the necessary technologies free of charge. For example, Tesla proposed the development of a virtual power plant in South Australia that involved installing smart meters, rooftop solar PV systems, battery storage, and computerized control systems in 1,100 public housing units [29]. Creating diverse stakeholder groups to address resilience planning [2] and ensuring that awareness of equity issues arises during planning discussions [84] are just two approaches to addressing equity issues. Further exploration is needed to understand the equity effects of aggregation and how DER aggregator models can implement equity-by-design (i.e., incorporating equity concerns into earlier-stage research) as these models become more mainstream [85].

VI. CONCLUSION

FERC Order No. 2222 is a notable step to encourage the growth of aggregators as a significant stakeholder group in an increasingly distributed power grid. The aggregation of DERs is one method that can ensure grid stability with the integration of new, clean energy resources. We have reviewed and summarized many schemes that DER technologies and stakeholders can use to contribute to power system resilience. Although a forecast of the future prevalence and capabilities of aggregators is beyond the scope of this work, there are actionable technologies and practices that aggregators can adopt to benefit the power grid in the face of increasing natural disasters and human-driven hazards. In reviewing the literature, open research questions and opportunities for standards development were revealed.

Some areas for future research are as follows:

(a) Aggregator Communication and Control Capabilities: Many of the techniques described in Section III assume that the aggregation dispatch agent can either dynamically dispatch active power control or advanced inverter function parameters or otherwise mandate specific autonomous advanced inverter functions within their DER fleet. It is unclear which portion of DER aggregators have, or will have, this type of dispatch capability. Dynamic dispatch control will depend on the communication infrastructure implemented and the individual capabilities of the DER devices registered in each fleet. Further, additional research is required to determine how an aggregator's capabilities could be impacted given the loss of communication with all, or a portion of, the DER fleet during a disruptive event. As described in Section IV-F, this is an important capability for aggregators to have, but there is a gap in the literature.

(b) Aggregator and Utility Coordination: The willingness and/or ability of aggregators and utilities to coordinate with one another is unclear. This is likely determined by socioeconomic factors that influence the strength of the business case for aggregators, such as customer engagement, willingness to share information, and incentives to initiate and complete the process of enrolling in an aggregation. This process will most likely be slow because ISOs and RTOs generally allow for utilities to take 60 days to review and approve the enrollment of DER components into an aggregation [6], [13]–[16]. As described in Section III-C, direct utility control can expand the resilience capabilities of an aggregation through the benefits of grid-awareness and forward-looking developments in the field of black-start capabilities. If an aggregation dispatch agent is not grid-aware, this will limit their ability to support resilience. An aggregator might be able to coordinate with a utility that has a high degree of grid awareness, but even this coordination leads to more questions of increased DER response latency and organization, depending on whether a grid operator can obtain direct control of an aggregator's DERs and how the operator, in turn, would implement the communication system to exercise this control.

(c) Aggregator Classification: We find that the aggregator's potential to provide security and resilience varies with the level of aggregator coordination with distribution utilities and the capabilities that aggregators design into their DER network (takeaways *(a)* and *(b)*). Work has been done that clearly delineates utility aggregators and third-party aggregators. Additional analysis to further delineate aggregator types by tech-

nical capability can support safe system operation by allowing the operator to better understand an aggregator's potential to support system security and resilience and anticipate what aggregator capabilities the operator can call on.

(d) Harmonization of Standards, Protocols, and Certification: Although there is no one-size-fits-all approach to the aggregator's provision of resilient operation, the interoperability and interconnection of DERs can benefit from comprehensive cybersecurity standards—such as encryption, authentication, verification, and defined roles and responsibilities—to support a heterogeneous system of diverse DER devices and stakeholders. There is no clear definition of an aggregator's responsibility in using cybersecurity best practices or in enforcing them in their customer-owned fleet (i.e., there is no comprehensive, universally accepted set of cybersecurity best practices for DERs or DER aggregators). There is a lack of universal and harmonized standards at every level, including communication protocols, access control schemes, certification of devices or aggregator communication networks, and grid services and collective DER responses to disturbances. Many efforts are being made to amend this, but much work remains to navigate the changing landscape of aggregated DER integration [38], [62], [66], [69], [86].

(e) Equitable Implementation of DERs: Significant research is needed in market structures, aggregation creation, and the services that can be provided to support vulnerable communities and address environmental justice issues. Ensuring that equity challenges are not inadvertently created requires the involvement of those who would benefit most from DERs in their communities. Stakeholder engagement and understanding the consequences of social burdens and social vulnerabilities are key to DER aggregation design and operation. Creating structures to provide services that support historically underserved or vulnerable communities will benefit society writ large. Researching and creating design criteria or guiding principles for the equitable implementation of DERs would be significant.

(f) Value of Resilience and Security: Valuing the resilience and security that DERs can provide can help with business justifications for new investments by DER aggregators in different communities to serve different customers. Understanding the components that are important to prioritize, invest in, and address within the complex DER aggregator landscape to enhance resilience and security is key. This paper summarizes a few challenges and solutions to enhancing both physical and cybersecurity within DERs; however, much more research is needed on the value that these solutions would provide.

Although the ability to increase aggregation and implement DER technologies is moving the needle forward to a clean energy future, there are opportunities for additional research. Understanding the challenges and opportunities will foster the implementation of clean energy technologies in a resilient, secure, and equitable manner. Understanding the aggregator's role in power system security and resilience is the first step on a long road to DER aggregation across the nation.

ACKNOWLEDGMENTS

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported as a planning and assessment project at NREL and by the U.S. National Science Foundation (NSF) under Grant NSF 1847578. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes. The authors wish to thank the time and expertise of the reviewers of this paper, Dr. Fei Ding, Dr. Adarsh Nagarajan, Dr. Jaquelin Cochran, and Jesse Dugan (Mines/NREL Advanced Energy Systems Program). In addition, feedback and guidance were especially appreciated from Dr. Jeremy Keen and Dr. Mohammed Ben-Idris.

REFERENCES

[1] K. Zitelman, "Advancing Electric System Resilience with Distributed Energy Resources: A Review of State Policies," National Association of Regulatory Utility Commissioners (NARUC), Tech. Rep., Apr. 2020.

[2] E. L. Hotchkiss and A. Dane, "Resilience roadmap: a collaborative approach to multi-jurisdictional resilience planning," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.

[3] J. Zwartscholten, M. Klaes, D. M. Gonzalez, F. Subhan, A. Narayan, and C. Rehtanz, "Impact of increased ict latency on active distribution network control," in *2020 6th IEEE International Energy Conference (ENERGYCon)*. IEEE, 2020, pp. 864–869.

[4] I. Pérez-Arriaga and C. Knittel, "Utility of the Future," Dec. 2016. [Online]. Available: https://energy.mit.edu/wp-content/uploads/2016/12/Utility-of-the-Future-Full-Report.pdf

[5] S. Burger, J. P. Chaves-Ávila, C. Batlle, and I. J. Pérez-Arriaga, "A review of the value of aggregators in electricity systems," *Renewable and Sustainable Energy Reviews*, vol. 77, pp. 395–405, 2017.

[6] FERC, "Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators," 2020.

[7] D. Saleem, A. Hasandka, C. Lai, D. Jose, and C. Howerter, "Design considerations of a cryptographic module for distributed energy resources," *Proceedings of the CyberPELS*, 2019.

[8] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for der cyberattacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 3, pp. 240–249, 2019.

[9] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for der vendors, aggregators, and grid operators," *Tech. Rep.*, vol. 12, 2017.

[10] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[11] R. Singh, P. D. Hines, S. E. Howerter, and J. T. Reilly, "Beyond derms: Demonstration of automated grid services, mode transition, and resilience," Argonne National Lab.(ANL), Argonne, IL (United States), Tech. Rep., 2022.

[12] J. Johnson, I. Onunkwo, D. Saleem, W. Hupp, J. Peterson, and R. Cryar, "Distributed energy resource cybersecurity standards development-final project report." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.

[13] "New York Independent System Operator, Inc.; Compliance Filing and Request for Flexible Effective Date," Jul. 2021.

[14] "California Independent System Operator CorporationTariff amendment to comply with Order No. 2222," Jul. 2021.

[15] "Revisions to ISO New England Inc. Transmission, Markets and Services Tariff to Allow for the Participation of Distributed Energy Resource Aggregations in New England Markets," Feb. 2022.

[16] "Order No. 2222 Compliance Filing of PJM Interconnection, L.L.C." Feb. 2022.

[17] L. Strezoski and I. Stefani, "Utility derms for active management of emerging distribution grids with high penetration of renewable ders," *Electronics*, vol. 10, no. 16, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/16/2027

[18] S. Kerscher and P. Arboleya, "The key role of aggregators in the energy transition under the latest european regulatory framework," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107361, 2022.

[19] J. J. Cook, K. B. Ardani, E. J. O'Shaughnessy, R. M. Margolis, and B. Smith, "Expanding pv value: Lessons learned from utility-led distributed energy resource aggregation in the united states," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2018.

[20] D. Mishra, "Api use-case prioritization approach and methodology," 2021.

[21] M. Alharbi, "Design and Implementation of PV-Firming and Optimization Algorithms For Three-Port Microinverters," Ph.D. dissertation, University of Central Florida, Orlando, Florida, 2018.

[22] B. Kroposki, A. Bernstein, J. King, D. Vaidhynathan, X. Zhou, C.-Y. Chang, and E. Dall'Anese, "Autonomous energy grids: Controlling the future grid with large amounts of distributed energy resources," *IEEE Power and Energy Magazine*, vol. 18, no. 6, pp. 37–46, 2020.

[23] I. Wilson, "Foundations of hierarchical control," *International Journal of Control*, vol. 29, no. 6, pp. 899–933, 1979.

[24] K. Utkarsh, F. Ding, X. Jin, M. Blonsky, H. Padullaparti, and S. P. Balamurugan, "A network-aware distributed energy resource aggregation framework for flexible, cost-optimal, and resilient operation," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1213–1224, 2021.

[25] J. Cochran, M. Miller, O. Zinaman, M. Milligan, D. Arent, B. Palmintier, M. O'Malley, S. Mueller, E. Lannoye, A. Tuohy *et al.*, "Flexibility in 21st century power systems," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2014.

[26] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, 2011.

[27] H. Zakernezhad, M. S. Nazar, M. Shafie-khah, and J. P. Catalão, "Optimal resilient operation of multi-carrier energy systems in electricity markets considering distributed energy resource aggregators," *Applied Energy*, vol. 299, p. 117271, 2021.

[28] S. M. Spina, L. Mcallister, and A. P. Ramadevanahalli, "Ferc breaks new ground with der aggregation order," 2020.

[29] I. R. E. Agency, "Aggregators: Innovation landscape brief," 2019.

[30] "IEEE Guide for Distributed Energy Resources Management Systems (DERMS) Functional Specification," IEEE, Tech. Rep., iSBN: 9781504475938. [Online]. Available: https://ieeexplore.ieee.org/document/9447316/

[31] J. T. Johnson, J. Flicker, A. Castillo, C. Hansen, M. El-Khatib, D. Schoenwald, M. Smith, R. Graves, J. Henry, T. Hutchins, J. Stamp, D. Hart, A. Chavez, M. Burnett, J. Tabarez, C. Glatter, B. Xie, A. P. Meliopoulos, P. Huynh, H. Zhu, and K. Davis, "Design and evaluation of a secure virtual power plant." 9 2017. [Online]. Available: https://www.osti.gov/biblio/1395430

[32] "Odessa Disturbance, Texas Events: May 9, 2021 and June 26, 2021 Joint NERC and Texas RE Staff Report," North American Electric Reliability Corporation, Tech. Rep., Sep. 2021.

[33] "1 , 200 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report," North American Electric Reliability Corporation, Tech. Rep., Jun. 2017.

[34] "Multiple Solar PV Disturbances in CAISO: Disturbances between June and August 2021 Joint NERC and WECC Staff Report," North American Electric Reliability Corporation, Tech. Rep., Apr. 2022.

[35] J. Smith, M. Rylander, J. Boemer, R. Broderick, M. Reno, and B. Mather, "Analysis to Inform CA Grid Integration Rules for PV: Final Report on Inverter Settings for Transmission and Distribution System Performance," Tech. Rep. SAND2016–9164R, 1431468, 647453, Sep. 2016. [Online]. Available: https://www.osti.gov/servlets/purl/1431468/

[36] "Electric Rule No. 21: Generating Facility Interconnections," Jun. 2018.

[37] R. Arghandeh, M. Brown, A. Del Rosso, G. Ghatikar, E. Stewart, A. Vojdani, and A. von Meier, "The local team: Leveraging distributed resources to improve resilience," *IEEE Power and Energy Magazine*, vol. 12, no. 5, pp. 76–83, 2014.

[38] D. Narang, M. Ingram, S. Widergren, S. Gonzalez, S. Alam, T. Bohn, Y. Xue, R. Brown, J. Page, M. A. Piette *et al.*, "Gmlc survey of distributed energy resource interconnection and interoperability standards," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2021.

[39] M. Emmanuel, J. Giraldez, P. Gotseff, and A. Hoke, "Estimation of solar photovoltaic energy curtailment due to volt–watt control," *IET Renewable Power Generation*, vol. 14, no. 4, pp. 640–646, 2020.

[40] J. Giraldez, M. Emmanuel, A. Hoke, and S. Suryanarayanan, "Impacts of voltage-based grid support functions on energy production of pv customers," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[41] V. Gevorgian, Y. Zhang, and E. Ela, "Investigating the impacts of wind generation participation in interconnection frequency response," *IEEE Transactions on Sustainable Energy*, vol. 6, no. 3, pp. 1004–1012, 2015.

[42] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," IEEE, Tech. Rep.

[43] M. Gautam, M. M. Lakouraj, N. Bhusal, M. Benidris, and H. Livani, "Allocating reserves in active distribution systems for tertiary frequency regulation," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2022, pp. 1–5.

[44] J. Johnson, J. C. Neely, J. J. Delhotal, and M. Lave, "Photovoltaic frequency–watt curve design for frequency regulation and fast contingency reserves," *IEEE Journal of Photovoltaics*, vol. 6, no. 6, pp. 1611–1618, 2016.

[45] F. Ding, W. Liu, J. MacDonald, J. Ogle, A. Pratt, and M. Baggu, "Federated architecture for secure and transactive distributed energy resource management solutions (fast-derms)," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2022.

[46] L. Strezoski, H. Padullaparti, F. Ding, and M. Baggu, "Integration of utility distributed energy resource management system and aggregators for evolving distribution system operators," *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 2, 3 2022. [Online]. Available: https://www.osti.gov/biblio/1867582

[47] M. Noguera, B. K. Johnson, C. Rieger, and T. McJunkin, "Enhancement of Distribution System Resilience Through the Application of Volt-Var Regulation Devices," in *2020 Resilience Week (RWS)*. Salt Lake City, ID, USA: IEEE, Oct. 2020, pp. 174–180. [Online]. Available: https://ieeexplore.ieee.org/document/9241288/

[48] A. Nikoobakht and J. Aghaei, "Resilience promotion of active distribution grids under high penetration of renewables using flexible controllers," *Energy*, vol. 257, p. 124754, Oct. 2022. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0360544222016577

[49] A. Hoke, J. Giraldez, B. Palmintier, E. Ifuku, M. Asano, R. Ueda, and M. Symko-Davies, "Setting the smart solar standard: Collaborations between hawaiian electric and the national renewable energy laboratory," *IEEE Power and Energy Magazine*, vol. 16, no. 6, pp. 18–29, 2018.

[50] J. Taft, "Electric grid resilience and reliability for grid architecture," *Pacific Northwest National Laboratory (PNNL): Richland, WA, USA*, 2017.

[51] R. J. Concepcion, F. Wilches-Bernal, and R. H. Byrne, "Effects of communication latency and availability on synthetic inertia," in *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2017, pp. 1–5.

[52] K. B. Ardani, E. J. O'Shaughnessy, and P. D. Schwabe, "Coordinating distributed energy resources for grid services: A case study of pacific gas and electric," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2018.

[53] M. Gautam, M. Abdelmalak, M. Benidris, and E. Hotchkiss, "Post-disaster microgrid formation for enhanced distribution system resilience," in *2022 Resilience Week (RWS)*. IEEE, 2022, pp. 1–6.

[54] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for der integration: A review, challenges and research needs," *Renewable and Sustainable Energy Reviews*, vol. 168, p. 112794, 2022.

[55] P. De Martini, L. Gallagher, E. Takayesu, R. Hanley, and P. Henneaux, "Unlocking consumer der potential: Consumer-centric approaches for grid services," *IEEE Power and Energy Magazine*, vol. 20, no. 4, pp. 76–84, 2022.

[56] "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid," U.S. Department of Energy's Office of Cybersecu-

rity, Energy Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy., Tech. Rep., Oct. 2022.

[57] I. Onunkwo, B. J. Wright, P. G. Cordeiro, N. Jacobs, C. F. Lai, J. T. Johnson, T. Hutchins, W. M. Stout, A. D. Chavez, B. T. Richardson *et al.*, "Cybersecurity assessments on emulated der communication networks," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); DNK . . . , Tech. Rep., 2019.

[58] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 226–231.

[59] A. R. Chavez, "Moving Target Defense to Improve Industrial Control System Resiliency," in *Industrial Control Systems Security and Resiliency*, C. Rieger, I. Ray, Q. Zhu, and M. A. Haney, Eds. Cham: Springer International Publishing, 2019, vol. 75, pp. 143–167, series Title: Advances in Information Security. [Online]. Available: http://link.springer.com/10.1007/978-3-030-18214-4_8

[60] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[61] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, "Centralized and decentralized distributed energy resource access control implementation considerations," *Energies*, vol. 15, no. 17, 2022. [Online]. Available: https://www.mdpi.com/1996-1073/15/17/6375

[62] J. T. Johnson, "Recommendations for distributed energy resource access control," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2021.

[63] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, Mar. 2014, conference Name: IEEE Transactions on Parallel and Distributed Systems.

[64] J. E. Quiroz, M. J. Reno, O. Lavrova, and R. H. Byrne, "Communication requirements for hierarchical control of volt-var function for steady-state voltage," in *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2017, pp. 1–5.

[65] M. J. Reno, J. E. Quiroz, O. Lavrova, and R. H. Byrne, "Evaluation of communication requirements for voltage regulation control with advanced inverters," in *2016 North American Power Symposium (NAPS)*. IEEE, 2016, pp. 1–6.

[66] W. Hupp, D. Saleem, J. T. Peterson, and K. Boyce, "Cybersecurity certification recommendations for interconnected grid edge devices and inverter based resources," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2021.

[67] "National Cyber-Informed Engineering Strategy," U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy., Tech. Rep., Jun. 2022.

[68] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Tech. Rep., 2020.

[74] P. de Martini, "Where have all the aggregators gone?" 2020.

[69] J. Obert, P. Cordeiro, J. T. Johnson, G. Lum, T. Tansy, N. Pala, and R. Ih, "Recommendations for trust and encryption in der interoperability standards," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Kitu Systems . . . , Tech. Rep., 2019.

[70] W. Wang, X. Fang, and A. Florita, "Impact of der communication delay in agc: Cyber-physical dynamic co-simulation," in *2021 IEEE 48th Photovoltaic Specialists Conference (PVSC)*. IEEE, 2021, pp. 2616–2620.

[71] U. OE, "Modern distribution grid: decision guide volume iii," 2017.

[72] Y. Li, D. Huang, Y. Zhang, and T. Orekan, "Resilience analysis of cyber-physical networked microgrids with communication latency," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2021, pp. 1–5.

[73] G. Švenda, I. Krstić, S. Kanjuh, M. Jajčanin, and D. Vuletić, "Volt var watt optimization in distribution network with high penetration of renewable energy sources and electric vehicles," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2022, pp. 1–5.

[75] M. A. Brown and A. Soni, "Expert perceptions of enhancing grid resilience with electric vehicles in the united states," *Energy Research & Social Science*, vol. 57, p. 101241, 2019.

[76] Y. Lin, J. Wang, and M. Yue, "Equity-based grid resilience: How do we get there?" *The Electricity Journal*, vol. 35, no. 5, p. 107135, 2022.

[77] S. L. Cutter, "The landscape of disaster resilience indicators in the usa," *Natural hazards*, vol. 80, no. 2, pp. 741–758, 2016.

[78] M. Keck and P. Sakdapolrak, "What is social resilience? lessons learned and ways forward," *Erdkunde*, pp. 5–19, 2013.

[79] J. Dugan, D. Byles, and S. Mohagheghi, "Social vulnerability to long-duration power outages," *International Journal of Disaster Risk Reduction*, vol. 85, p. 103501, 2023.

[80] E. Boyle, A. Inanlouganji, T. Carvalhaes, P. Jevtić, G. Pedrielli, and T. A. Reddy, "Social vulnerability and power loss mitigation: A case study of puerto rico," *International Journal of Disaster Risk Reduction*, vol. 82, p. 103357, 2022.

[81] D. B. Karakoc, K. Barker, C. W. Zobel, and Y. Almoghathawi, "Social vulnerability and equity perspectives on interdependent infrastructure network component importance," *Sustainable Cities and Society*, vol. 57, p. 102072, 2020.

[82] R. Salvia and G. Quaranta, "Place-based rural development and resilience: A lesson from a small community," *Sustainability*, vol. 9, no. 6, p. 889, 2017.

[83] R. Best, "Energy inequity variation across contexts," *Applied Energy*, vol. 309, p. 118451, 2022.

[84] A. L. Berka and E. Creamer, "Taking stock of the local impacts of community owned renewable energy: A review and research agenda," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 3400–3419, 2018.

[85] N. S. Dutta, E. Gill, B. K. Arkhurst, M. Hallisey, K. Fu, and K. Anderson, "Just-r metrics for considering energy justice in early-stage energy research," *Joule*, vol. 7, no. 3, pp. 431–437, 2023.

[86] D. Saleem and C. Carter, "Certification procedures for data and communications security of distributed energy resources," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.