Digital Object Identifier 10.1109/ACCESS.2022.DOI

On the Cyber-Physical Needs of DER-based Voltage Control/Optimization Algorithms in Active Distribution Network

SUBIR MAJUMDER[1], (Member, IEEE), AMIRKHOSRO VOSUGHI[2], (Member, IEEE), HUSSAIN M. MUSTAFA[1], (Student Member, IEEE), TORI E. WARNER[3], (Member, IEEE), and ANURAG K. SRIVASAVA[1], (Fellow, IEEE)

[1]The Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, West Virginia 26506.
[2]OpenEye, Spokane, WA
[3]Electrical Consultants, Inc., Woods Cross, Utah 84087

Corresponding authors: Anurag K. Srivasava (e-mail: anurag.srivastava@mail.wvu.edu), Subir Majumder (e-mail: subir-em@ieee.org).

This work is partially supported by the US Department of Energy UI-ASSIST project #DE-IA0000025, and NSF CPS aDaption 1932574. All the authors were previously affiliated with the School of Electrical Engineering & Computer Science, Washington State University, Pullman, WA.

ABSTRACT With the increasing penetration of distributed energy resources (DERs) and extensive usage of information and communications technology (ICT) in decision-making, mechanisms to control/optimize transmission and distribution grid voltage would experience a paradigm shift. Given the introduction of inverter-based DERs with vastly different dynamics, real-world performance characterization of the cyber-physical system (CPS) in terms of dynamical performance, scalability, robustness, and resiliency with the new control algorithms require precise algorithmic classification and suitable metrics. It has been identified that classical controller definitions along with three inter-disciplinary domains, such as (i) power system, (ii) optimization, control, and decision-making, and (iii) networking and cyber-security, would provide a systematic basis for the development of an extended metric for algorithmic performance evaluation; while providing the taxonomy. Furthermore, a majority of these control algorithms operate in multiple time scales, and therefore, algorithmic time decomposition facilitates a new way of performance analysis. Extended discussion on communication requirements while focusing on the architectural subtleties of algorithms is expected to identify the real-world deployment challenges of voltage control/optimization algorithms in the presence of cyber vulnerabilities and associated mitigation mechanisms affecting the controller performance with DERs. Finally, the detailed discussion provided in this paper identifies the modeling requirements of the CPS for real-world deployment, specific to voltage control, facilitating the development of a unified test-bed.

INDEX TERMS Cyber-physical systems, Cyber-Security, Renewable energy sources, Taxonomy, Voltage control

I. INTRODUCTION

As more and more small-scale inverter-based clean distributed energy resources (DERs) being integrated, the power distribution system is turning out to be an active distribution network (ADN). Consequently, despite the known advantages of environmentally friendly DERs, the impacts of increasing penetration are visible in the demand profile [1], [2]. The subsequent impact on the voltage profile is also prominent [3], and the resulting over-voltage condition during the day has significantly impacted the reliability of the grid. Frequent operation of traditional voltage control devices, such as on-load tap changing transformers (OLTCs), voltage regulators (VRs), capacitor banks (CBs), etc., to alleviate these over-voltage concerns would significantly reduce their life span, and a lack of proper coordination among voltage control devices [4] would be detrimental to power systems operation. While DERs can contribute towards voltage control within the ADN, these devices need to be suitably

coordinated with conventional voltage control devices.

Furthermore, with an increasing number of DERs being connected to the ADN, coordination utilizing conventional control algorithms loses scalability. From a limited list of review articles in regard to voltage control/optimization [5]–[14], it is well understood that the coordination requirements can be categorized based on the spatial location of controllers and temporal operational horizon (or, the stages of operation), which conforms to the classical controller definitions reported in the literature. The need to identify implementation architecture for performance analysis primarily drives classification requirements of existing literature. However, with the involvement of multi-device, multi-vendor, multi-technology, and multi-owner systems, classifying the controller algorithms according to the existing definitions has become complex, multi-faceted, and multi-disciplinary. Given the possible existence of multiple different algorithmic architectures within the same system of DERs executing diverse distribution system applications, these algorithms need to be architecturally inter-operable. Furthermore, the newer algorithms facilitating increased penetration of DERs must be resilient and practical enough to operate with limited information.

Consequently, there has been an increasing focus on decentralized and distributed control algorithms in the current literature. In the majority of the instances, these newer algorithms can be distributed among a network of edge-connected controllers with computation capabilities connected via communication networks. Given limited computation requirements, these edge controllers could be very inexpensive. Increased reliability of modern information and communications technology (ICTs) can also facilitate the implementation of these newer architectures. The level of coupling among these controllers separates distributed algorithms from their decentralized counterparts. Both of these algorithms facilitate the privacy of shared information. However, by definition, required data exchanges, as well as communication network architecture for distributed and decentralized control, are different. Communication would not only be limited to exchanging sensor data for decision-making as with centralized architectures; controllers may also share various other information, such as droop settings, changes in network topology, exchanging set-points across multiple control regions, etc. The priority and requirement of each of these information exchanges would be different. These architectural differences have been the basis behind classical controller definitions [5], [7]–[11], [15], [18].

With the increasing penetration of ICT devices, the probability of being susceptible to cyber-attack is also increasing. This is due to increased attack surfaces introduced by the introduction of ICT devices for DERs, automation devices, and associated software. An attacker can exploit corresponding vulnerabilities through newly introduced attack surfaces prevailing in the cyber network, communication protocols, sensors/actuators, and the requisite human-in-the-loop (in the form of an insider attack). Furthermore, both power and communication networks are subjected to physical attacks. Following attacks, compromised entities in the cyber-physical with the human-in-the-loop system (CPHS) need to be judiciously detected [20], and both cyber and physical networks may need to reorganize. Therefore, there needs to be a way to properly manage the information that the controller receives so that the exchanged information meets application requirements with proper security following confidentiality, availability, and integrity (CIA) standard. This would require the use of appropriate communication technology and interoperability, enabling data exchange with required latency, bandwidth, and jitter. Although possible vulnerabilities in a CPHS can be generalizable into broad categories, possible subtleties in smart grid communication needs to be closely looked at.

Besides these challenges, the non-linear, non-convex power flow of the system, representing the physics of the ADN, can no longer be approximated by linear approximate due to DER variability. While there have been efforts to utilize better approximation/relaxations for generating the decision variables, architectures often limit the use of certain relaxations. Therefore, it is clear that the controller performance relies on three interdisciplinary domain aspects, namely, (i) power system domain, (ii) cyber domain, and (iii) decision-making, and classical control definitions do not always capture all the aspects of a CPHS. Such a limitation inhibits the identification of controller performance based on classical definition alone, and a lack of consensus among these existing definitions has been identified in [6]. Given the closely coupled nature of the CPHS, it is imminent that an extended definition for controller classification that successively leads up to a controller taxonomy would gain significance.

From the above discussion, we also observe that architecture-specific communication requirements and associated cyber vulnerabilities would also impact controller performance. The limitation of existing review articles has been discussed in Table 1. Our primary objective would be to identify the sub-categorization of each of the domain aspects with direct implications on voltage control and the development of an extended taxonomy. The developed taxonomy would help us understand how a voltage control algorithm would fare if they were deployed in the real world with a realistic communication network.

The contribution of our paper is, therefore, two-folded:

(i) An extended classification of Voltage Control/Optimization Application through Classical-Alternative Definitions and Time-Decomposition: Utilizing the voltage control as a use-case, existing algorithms in the literature are first classified based on the classical definitions. However, it has been observed that a majority of the developed algorithms are 'hybrid' (no one architecture can completely identify an algorithm), and multiple of these algorithms operate in different time-scale or stages for the overall real-world implementation. Each of these stages is often interlinked. Therefore, the

TABLE 1: Scope of Our Research (✓: detailed commentary on the considered aspect, ✓-: limited commentary on the considered aspect, ×: no commentary on the considered aspect)

Literature	Classical Classifications for Power System Optimization & Control	Extended Definitions for Power System Optimization & Control	Power System Optimization & Control Taxonomy	Voltage Control with DERs	Communication Requirements with DERs	Cyber-Threats, Vulnerabilities & Defense Mechanisms with DERs
[5]	✓- (Limited to centralized and decentralized Approaches)	×	×	✓	✓- (Limited)	×
[6]	✓	✓	✓	✓	×	×
[7]	✓	×	✓	✓	✓- (Limited)	×
[8]	✓- (Limited to decentralized and distributed approaches)	×	×	✓	✓- (Limited)	×
[9]	✓	×	✓	✓	✓	✓- (Limited)
[10]	✓	✓- (Limited extended definition)	✓	✓	×	×
[11]	✓- (Limited to distributed Approaches)	×	✓- (Limited to distributed Approaches)	✓	✓	✓
[12]	✓	×	✓	✓	✓	✓
[13]	×	×	×	✓	✓	×
[14]	✓- (Limited to centralized, decentralized and distributed Approaches)	×	×	✓	✓	✓
[15]	✓- (Limited to decentralized and distributed approaches)	×	×	×	×	×
[16]	✓- (Limited to distributed approaches)	×	×	×	×	×
[17]	✓- (Limited to distributed approaches)	×	×	×	✓- (Limited)	×
[18]	✓	×	×	×	✓	✓
[19]	×	×	×	×	✓	✓- (Limited)
[20]	×	×	×	×	✓	✓
Our Work	✓	✓	✓	✓	✓	✓

performance analysis of time-decomposed algorithms and their inter-dependencies can be knitted together to identify the overall performance of 'hybrid' approaches. The use of varying controller objectives, power system models, algorithms, and communication architectures was observed, which implied that these subcategories, together with classical controller definitions, would better identify the performance of an algorithm. Each of the sub-categories in the taxonomy can be utilized in this regard to identify a metric for the real-world performance analysis for voltage control. Notably, the scope of the proposed taxonomy is not limited to voltage control; rather, it could be extended to other smart grid applications with DERs.

(ii) Cyber-Attack and Mitigation Taxonomy and its relation to Controller Taxonomy: Although an algorithm may require operation in multiple different time scales, the criticality of the information being carried is not often well considered. Therefore, accurate modeling of communication networks for data exchange gains immense significance. The use of suitable communication technologies, communication protocols, and ways to mitigate cyber threats along with architecture-specific subtleties are captured considering a wide area network (WAN) oriented communication for voltage control/optimization application. Subsequently, a taxonomy of various cyber-attacks, including communication and physical layer-specific vulnerabilities, and the attack mitigation strategy are also described. Therefore, there is a need to deploy specific mitigation techniques based on controller architecture. Finally, the limitation of voltage control-specific cost-benefit analysis is also presented. This detailed description is expected to help us develop a unified real-world test-bed for performance analysis of various smart-grid applications.

In this regard, Section II provides a treatment on the devices for voltage control to identify the requisite coordination requirements with DERs, typically considered voltage control objectives, the necessity of optimal control strategies, and micro-grids, wherein the voltage control gains immense significance. We identify that TSO-DSO coordination gains increasing significance with increasing penetration of DERs, but such consideration is majorly absent in the reviewed literature. The primary objective of this section is to provide a background facilitating for further discussion on the developed taxonomy of voltage control in an ADN. In Section III, the existing algorithms for voltage control are first categorized using classical architectures, and their limitations are pointed out. Extended definitions have been introduced for better classification, which results in the voltage control

taxonomy. The use of decomposition for the analysis of hybrid approaches has been discussed along with specific cyber-infrastructure requirements for voltage control. Section IV provides an extended overview of communication technologies for voltage control with DERs, communication protocols, associated vulnerabilities, and possible mitigation techniques. Section V identifies the limitation of cost-benefit analysis considering DERs and voltage control/optimization application alone, and VI summarizes this paper.

II. VOLTAGE CONTROL WITH DERS

According to range 'A' of the ANSI voltage standard C84.1-2020 [21], the voltage profile is required to be maintained within $\pm 95\%$ of the operating band for 98% of all the operating hours. Increasing penetration of variable renewable-based DERs would affect ADN-wide voltage profile [3], and traditional slow-acting regulation devices would be unable to mitigate associated impact [7]. Additionally, the new IBRs have vastly different dynamics than traditional synchronous machine-based generators [22]. Enabled by the recent IEEE 1547-2018 standard [23], DERs can contribute to ADN-wide voltage profile improvement alongside classical control devices. It can be achieved through Var injection (during heavily loaded conditions) or Var absorption (during the lightly loaded condition) with increasing energy production from these DERs. If Var absorption is unable to control the voltage within the bound, active-power curtailment (also known as volt-watt control) would be necessary [24].

The scope of voltage control is not limited to the normal operation of the system but also to ensure that the quality standard is maintained when the system undergoes contingencies. In the context of the ADN, the majority of faults are temporary [25], and fuse-saving protection mechanism [26] is often deployed for the fault to clear itself -— the requisite coordination among the protection devices results in voltage sags. In the post-fault system operation, the system may require excessive reactive power, delaying the return to the steady state. The network can also suffer from transient over-/under-voltages, known as swells or sags, originating from lateral feeders/upstream networks. In this regard, DERs can also provide voltage support when the system is undergoing contingencies.

Typically, the control problem aims to regulate the operating point to the desired state, considering the dynamics of the system. Optimization problems deal with static snapshots of a system, while optimal control bridges the gap between the optimization and control problems. If the accurate prediction of voltage dynamics within a system is not essential, consideration of static snapshots may be sufficient in voltage control/optimization. Associated problems are generally classified as optimal power flow problems (OPF), which either utilize forecasts or other ways to account for the stochasticity of renewable generation. Deploying settings to regulating devices for system-wide voltage regulation, considering forecasted data-set, obtained through supervisory control and data acquisition (SCADA) systems, comes under the purview of industrial control system [27]. Therefore, the academic literature often uses voltage optimization and control synonymously. This paper uses voltage control, optimization, and regulation interchangeably without loss of generality.

This section describes (i) various classical and modern voltage control devices, (ii) voltage control objectives, (iii) the optimality of voltage control techniques, (iv) the need to integrate the transmission and distribution system operation, and (v) voltage control vs. stability. These discussions would facilitate further discussions in the following section.

A. DEVICES FOR VOLTAGE CONTROL

1) OLTCs

OLTCs in the distribution substations control the ADN-wide voltage profile by adjusting the tap ratio. Hence, their control action is primarily discrete. These devices raise/lower voltage profiles across the entire ADN. Typically, OLTCs are equipped on the primary side of a transformer because of lower load current [28] and equipped to respond to the secondary side of the voltage profile as an automatic voltage regulator (AVR) [29], [30]. OLTCs could also be equipped with additional controllers to respond to both primary and secondary side voltages to avoid voltage collapse, as was observed in the Swedish grid in 2003 [29]. OLTCs could be operated through remote terminal units (RTUs) in a SCADA system. Requisite motorized gear operation implies that OLTCs are slow-acting devices and can suffer from mechanical wear and tear [31]. Therefore, their operation is restricted to a few times a day. However, to circumvent mechanical operation, electronic OLTCs have recently been thoroughly researched [28]. Manual tap changing operation of the transformers, although offers a substantial reduction in investment cost, requires isolation during tap operation. OLTCs can suffer from circulating currents if tap operations of parallelly connected transformers are not suitably coordinated. ADN-wide voltage control by OLTCs is typically utilized in conservation voltage reduction for the utilities.

2) VRs

Like OLTCs, VRs utilize auto-transformers [32] with mechanical or electronic taps to raise/lower the downstream voltage. Hence these devices are also susceptible to increased mechanical wear and tear, and their control action is primarily discrete. However, electronically controlled VRs are also being extensively researched. Given the unbalanced nature of the ADN, these regulators are able to adjust set-points on a per-phase basis. However, such an operation requires additional control equipments [33], making them expensive. Being mechanically controlled implies that these devices are inflexible to control DER-induced voltage fluctuations [34]. VRs can either facilitate line drop compensation (LDC) with local voltage measurements or control ADN-wide voltage based on remote sensing and SCADA data. As for LDCs, time delays are necessary to avoid oscillation among multiple regulating devices. To facilitate controlling VRs via RTUs,

the control center needs to coordinate the operation of other regulating devices [4], [35].

3) CBs

Traditionally, CBs within the ADN substation facilitated power factor correction. Like OLTCs and VRs, control of these devices is also inherently discrete. Switching of these CBs ensured avoidance of the reverse flow of reactive power in the transmission system during low-loading conditions. Given the voltage quality often used to be poor at the far end of the long distribution feeder, which can be beyond the capabilities of OLTCs, a few large CBs could be placed along a feeder [36]. The operation of substation CBs could be manual, requiring the dispatch of operational crews if needed. Like other conventional devices, operations of CBs could be based on local measurements, which are required to be deployed with suitable delay and based on a certain threshold of the state variable to facilitate desirable voltage control. Alternatively, switching of CBs could be facilitated by the RTUs, while suitably coordinating with other devices. Although carrying out per-phase voltage correction is possible, the controller could become very expensive. Switching of CBs may lead to transients, which limits their frequent operation with increasing penetration of DERs [37].

4) DERs

Traditionally, DERs were expected to operate at unity power factor [38]. Facilitated by the recent IEEE-1547 standard [23], DERs can actively participate in voltage control. Devices that may be classified as DER include PVs, wind turbines (WTs), fuel cells, energy storage systems (ESSs), microgenerators (e.g., microturbines), diesel generators, electrical vehicles (EVs), and controllable loads (CLs). CLs typically respond via demand response mechanisms. Control action of all of these loads is in a continuous domain. The majority of DERs are inverter-based resources [39] with dynamics different compared to traditional synchronous machine-based resources. These IBRs are also a major cause of power quality concern within an ADN [37]. Also, as these devices are getting cheaper with technological innovation, if suitably remunerated, these can be a more reliable way of controlling voltage on distribution feeders than conventional devices [34]. However, it is notable that DERs serve many other services in addition to providing voltage support; the most important of them is providing access to clean energy resources.

5) Other Smart Devices

Smart devices, including DERs, are electronically operated, contributing towards an intelligent distribution system [40]. Recent advancements in power electronic devices have put forth a plethora of other smart devices, such as solid-state transformers (SSTs) [41], distribution-STATCOMS (DSTATCOM) [42], dynamic voltage restorers (DVRs) [43], [44], static var compensators (SVCs) [45]. These devices are also known as custom power devices. Here, DSTATCOM and DVRs are typically considered as power quality improvement devices but could be utilized for voltage control. Unlike OLTCs, VRs, and CBs, these smart devices facilitate continuous control of voltage profiles instead of discrete tap operations. Furthermore, depending upon the underlying topology of power electronic converters, these devices are expected to inject harmonics into the ADN, like other DERs and power electronics interfaced loads. However, the use of a harmonic voltage controller for the compensation of selective grid harmonics is notable [46]. The ADN could also be equipped with switches coupled with RTUs, manual switches, and reclosers, which could facilitate reconfiguration of the ADN for the voltage profile improvement [47].

Discussion on Requisite Coordination for Voltage Control: While we have limited the scope of discussion for each of the devices in this subsection to voltage control application, it is notable that these devices can contribute towards multiple other services. For example, OLTCs and VRs can protect the bulk power system from voltage instability. CBs, DERs, and smart devices can provide long-term voltage support to the transmission grid. Switching operation gains immense significance when the ADN is faulted, especially during resiliency events. Therefore, as we will discuss in a later section, a direct cost comparison of each of these control devices may not be justifiable. Furthermore, the operation of traditional devices for voltage control is primarily discrete, and inappropriate coordination of these devices would have an adverse effect on the ADN operation. This includes switching transients, voltage oscillations, and exhausted tap operations. Contrarily, smart devices, including DERs, have to coordinate with traditional discrete control devices. Therefore, these available devices for voltage control can be classified based on discrete/continuous control actions. With the increasing penetration of power electronic converter-based devices, harmonics and associated impacts on voltage measurement need to be accounted for in developing voltage control laws.

B. VOLTAGE CONTROL OBJECTIVES

Alongside compensation for the line drops, many objectives can be found in the literature that directly affect the voltage profile. Due to the high R/X ratio of medium and low voltage ADN [9], the voltage profile is not entirely decoupled with active and reactive power. The injection of reactive power is not generally compensated. Therefore, the cost of reactive power injection is typically measured in terms of lost opportunity cost due to not supplying active power [48]. Notably, the lost opportunity cost definition doesn't imply active power curtailment; it is typically a way of accounting for the cost of reactive power production. Related analysis from the planning point of view will be discussed in Section V. Objective functions discussed in the following paragraphs could be suitably accounted for in the identification of these opportunity costs. If accurate identification of cost function is challenging or mathematical approaches are difficult to implement, rule-based approaches could also be utilized.

DER operators could also be offered monetary benefits for voltage profile improvement [49].

Usually, the operators would like to achieve an improved voltage profile with the least amount of reactive power injection [24], [48], [50]–[58]. Active power curtailment may be necessary for lightly loaded ADN with high DER penetration and is also a widely considered objective [50], [56], [59]–[62]. Notably, active power within an ADN is typically remunerated, and volt-watt control is not typically exercised unless under circumstances where the reliability of the ADN will be threatened. This is a middle ground compared to the traditional tripping of DERs in the advent of over-voltage conditions [63]. Given that the distribution networks are typically unbalanced, associated mitigation is also used as an objective for controlling voltage [64].

Another well-considered objective for voltage regulation is the minimization of the second norm of voltage deviation from the voltage at the substation end (or some prespecified voltage) [49], [53], [54], [58], [60], [65], [65]–[71]. The correlation among line losses and voltage profiles and the quadratic nature of the associated objective function make line loss minimization a well-researched objective [49], [60], [67], [72]–[81]. Furthermore, operating the ADN at lowered voltage while satisfying ADN standards can be utilized for ADN-wide demand reduction due to the underlying voltage-active power sensitivity. This is known as conservation voltage reduction (CVR), which is a well-researched topic [11], [37], [82]. As for the traditional mechanically operated devices, tap operation is required to be minimized to improve the lifespan of the associated device [53], [69], [83], and switching operations also need to be minimized to reduce possible transients.

Devices utilizing local measurements are expected to operate according to prespecified droop characteristics or designed to follow rule-based algorithms. These droop characteristics are expected to mimic the inherent relationship among active/reactive power injection and voltage profile, fixed power factor mode, or any control objectives mentioned earlier [50], [84]–[90]. Furthermore, many other control objectives exist in the literature that is a combination or an extension of the objectives discussed here.

C. OPTIMAL VS. NON-OPTIMAL APPROACHES FOR VOLTAGE CONTROL

A typical complex decision-making problem involves cost and benefit functions while capturing the underlying physics of the system. Although the underlying physics could be represented with sufficient mathematical rigor, associated (time and computational) complexity forbids us from using them in a real-world deployment. While the use of approximations may lead to tractable algorithms, unless an appropriate model is selected, the resulting solution may not be feasibly deployed. Additionally, cognitive oversights and lack of consensus often lead to simplifications of both the cost and benefit functions [91]. Many benefits are often indirect and hard to quantify [92]. Given the complexity, a system is often systematically broken down into multiple subsystems that operate independently or with limited coordination. However, such an action may not always lead to system-wide optimality.

Voltage control in the power system also suffers from similar issues and could be the reason behind diverse solution approaches in the literature. For example, the power system is broken down into the transmission and distribution system through spatial decomposition to be operated with limited coordination [93]. However, as it will be discussed in II-D, such decomposition may not always be justifiable, especially with the increasing penetration of DERs. Furthermore, the voltage control is mostly driven by standards, which limit the use of complex decision-making algorithms by the utilities. Despite these challenges, there exists a rich literature on this topic, and there has been a wide amount of literature that focuses on ensuring a steady-state voltage profile stays within the limit by solving an OPF problem. Multiple approximations and relaxations techniques for the OPF problem [94], such as decoupled power flow, DC approximation model, Shor Relaxations, Jabr's Relaxations, Flow Relaxation, Copper Plate Relaxation, McCormick Relaxations, and Baradar–Hesamzadeh Approximation can be referred to in this regard. The power distribution system could be AC, DC, or hybrid AC/DC, which would affect the modeling requirement of the ADN. However, it would have little to no impact on the deployability of relevant voltage control approaches.

Control techniques, as available in the literature, can be primarily divided into (i) rule-based, (ii) mathematical-optimization-based, and (iii) meta-heuristic approaches. LDC is one of the major examples of rule-based voltage control. The AVISTA 60-40 rule described in [95] is another example where CBs are turned on if there is a 40 percent imbalance of reactive power, and capacitors can provide more than 60 percent of the requirement. These rule-based controllers can stem from physics-based rules [96] or based on operational characteristics [74], [97]. These rule-based approaches alleviate the need to account for complexities within the system in great detail. Droop control could be another example of the rule-based approach that actively exploits the physics of the ADN. However, these rule-based methods suffer from several limitations. For example, LDCs are unsuitable for ADNs, and the droop rules designed based on one operating condition suffer severe limitations at different operating conditions, especially with a network with a high R/X ratio.

Furthermore, depending upon the needed accuracy, different approximated/relaxed mathematical models [94] could be used. Consequently, the OPF problem could be classified as linear programming (LP), quadratic programming (QP), mixed-integer linear programming (MILP), mixed-integer quadratic-constrained programming (MIQCP), mixed-integer non-linear programming (MINLP), semi-definite programming (SDP), second-order conical programming (SOCP), mixed integer SOCP (MISOCP), etc.

Mathematical programming techniques, including the interior point method (IPM), quasi-Newton method, gradient descent methods, dynamic programming (DP), sequential quadratic programming (SQP), etc., could be used for voltage control. The problem would be of mixed-integer type depending on the scope of control variables. Additionally, the ACOPF problems could be broken down into hierarchical sub-problems utilizing the natural decomposability [93]. The computational capability could be further distributed, where each cluster solves its problem while coordinating with other clusters — which ultimately has led to the development of distributed algorithms. These methods include [16]: (i) distributed consensus-based methods (sub-gradient methods, gradient-tracking, consensus-based self-optimization), (ii) dual methods (dual decomposition, alternating direction method of multiplier or ADMM, proximal atomic control or PAC-X), (iii) constraint exchange methods.

Genetic algorithms (GA) [54], [98] and Particle Swarm Optimization (PSO) [53], [76], [99], [100] are also two of the most well-known meta-heuristics algorithms used in the context of voltage control. However, the optimality of the solution obtained using these methods may not be provable. Given the underlying complexity of the power system physics and requisite speed of control action, meta-models (such as Kriging meta-model [101]) have been utilized. Recently, artificial intelligence (AI)-based techniques, specifically reinforcement learning approaches, have widely been used in this context [102]–[104]. These AI-driven algorithms could also be utilized for determining hyper-parameters for distributed or local algorithms. However, the machine learning approaches inherently rely on available data. The limited availability of the dataset for training and the use of offline simulators (OpenDSS, GridLab-D, or real-time simulators) to generate these datasets implies that the accuracy of the simulator will decide the applicability of AI-driven approaches.

D. NEEDS FOR TRANSMISSION AND DISTRIBUTION OPERATION COORDINATION

As discussed earlier, with the increasing penetration of DERs and resulting possible power flow reversal, power transmission and distribution network voltage profiles no longer remain decoupled [105]. The assumption that the power transmission network voltage is stiff and the traditional argument that the voltage control is a local phenomenon [106] may oversimplify the developed voltage control algorithms. Multiple grid operators recommended the requisite coupled simulation requirements [107]–[109] following multiple demonstration projects around the world [110]–[112]. Furthermore, mandated by IEEE 1547-2018 and quick response time, the DERs could provide the power transmission networks with long-term voltage support [54], [113], which is under the purview of the transmission system operator (TSO). The power system voltage control would therefore require suitable coordination among TSO and DSO, which invalidates the findings of the majority of the research conducted for steady-state voltage control. However, as discussed in II-C, the stated assumptions could still be valid under certain operating conditions, and these algorithms could be readjusted to make them operable in the integrated TSO-DSO context. Given the availability of rich literature, in this paper, the focus would be limited to ADN-wide voltage control.

E. VOLTAGE CONTROL VS. STABILITY

Typically, voltage stability is referred to as the ability of the power system to return to steady state operating conditions following a major disturbance/contingencies (during emergency operating conditions). Voltage control literature, especially with the power distribution systems, typically focuses on getting voltage within the allowed range through local control or by solving OPF problems considering dynamic loading conditions. Ignoring system dynamics ensures the identification of a possible solution without a clear explanation of how the system state would evolve — under the assumption that the network does not operate near its operating limits (line limits, generation limits, etc.). Therefore, as discussed, the voltage control literature focuses on the power system as a *quasi-static process*. In an ADN with short line lengths, the voltages could be tightly coupled. Due to a lack of complete decomposability of voltages and frequency in an ADN with a high R/X ratio, voltage control gains immense significance [114]. Limited available resources coupled with being a weak grid in a microgrid setting implies that the voltage and frequency can be contorted in an isolated microgrid [115], [116]. Nevertheless, in regards to voltage stability for the ADN [114], one can refer to the following phenomenon, (i) fault-induced delayed voltage recovery (FIDVR), (ii) proper coordination among DERs to ensure the absence of circulating currents among the DERs, (iii) inability to use droop-control in the ADN with high R/X ratio, (iv) operating the network close to its loading limit, and (v) undamped voltage ripple in the DC-link capacitor of the DER. While modeling the system as a quasi-static process help in approximate voltage stability analysis, a dynamic model will be needed for accurate prediction of system state [117]. Nevertheless, as discussed in Section III, the available model often determines the suitability of a given algorithm and architecture.

Architectural Needs for Voltage Control with DERs: It is imminent from the literature above that the scope of voltage control literature is exceptionally vast. The operation of control devices needs proper coordination, which gains additional significance with the increasing penetration of DERs. This implies the performance of an algorithm would also be limited by the available communication infrastructure, how data flows through the communication network, and how the necessary computation is being carried out. In regard to the computational aspects, the availability of various models representing the power system can be observed, which are required to be judiciously used based on the operating condition of the system. Given algorithmic and communication limitations, not all models can be equally applicable,

which may impact the optimality of the control action. To understand the architectural differences in the algorithmic implementation of voltage control approaches, in this paper, we would limit our focus to *voltage control with DERs to control voltage profiles within an ADN under the modeling assumption of a quasi-static process to account for dynamic loads utilizing classical mathematical approaches*, which is under the purview of a DSO.

However, the said scope does not limit the contribution of the paper. Rather, the analysis presented in this paper is sufficiently generalizable, where, as we shall see, the challenges in the categorizations for voltage controllers, as well as the communication requirements, exist for classical control devices as well. In the subsequent section, we will focus on specific vulnerabilities in the communication network, how they will impact each of the control architectures, and the ways to mitigate the associated vulnerabilities.

III. TAXONOMY OF VOLTAGE CONTROL APPROACHES

A. CLASSIFICATIONS BASED ON CLASSICAL VOLTAGE CONTROL DEFINITIONS

As discussed in the existing literature [9], the algorithm classifications are primarily driven by the relative locations of sensors/actuators, the controllers, and the methods of internal information exchange — the physical architecture. Classical controller definitions include (i) local, (ii) centralized, (iii) decentralized, and (iv) distributed architectures. Notably, speed of communication and computation/coordination requirements at the controller/coordinator level is implicitly accounted for within the controller definitions.

In light of these definitions, a relatively detailed review of the current body of literature has been performed. As shown in Table 2, we classify these algorithms based on the existing definitions. Subsequently, these control architectures are subdivided from the methodological point of view. The resulting architectures are then sub-classified based on requisite control devices. Broader voltage control objectives are then included stressing the algorithm and modeling techniques. Secondary objectives, if needed, are also highlighted with specified goals.

Based on the conducted review, the specifics of each of the control schemes are highlighted next.

1) Local Approaches

Local approaches primarily rely on physical relationships among local measurements and control variables (e.g., voltage and reactive power droop, voltage and active power droop, etc., through simplifying assumptions) or entirely rule-based heuristics for decision-making. This way, the controllers avoid real-time communication requirements and hence, do not suffer from cyber vulnerabilities. Based on the literature, control-based approaches actively utilize PI controllers for decision-making, with the controllers tuned utilizing system-wide responses (OPF-based approaches). Lack of coordination implies the simplicity of these approaches. Depending upon the level of data processing utilized at the controller node, the performance of these approaches can be extremely fast [160]. The controllers generally rely on the 'measure-compute-deploy' approach and actively utilize the power grid itself to satisfy the physics of the ADN. Therefore, these approaches are often dynamic or feedback-based. Lack of coordination implies that these approaches seldom achieve performance optimality (for the specific control objective if there is any). Furthermore, lack of coordination can result in the conflicting operation of multiple voltage regulating devices or racing conditions [35]. Therefore, local algorithms could result in unstable system operation, and parameter tuning would be necessary [119]. Lack of communication may also result in a lack of robustness of the controllers — one of the potential drawbacks of these approaches. However, the controllers could be provided with algorithms to isolate noisy measurements for decision-making.

Due to the inherent non-linearity of the power system, the droop characteristics need to be modified based on system loading conditions. Therefore, the droop characteristic curve is required to be periodically updated at a slower time scale. Therefore, as shown in Table 2, local approaches, a majority of the time, require a secondary controller located at the ADMS for the determination of (i) droop settings, (ii) set-points, and (iii) sensitivity factors, implying these methods are inherently hybrid. Furthermore, if the control of conventional devices is involved, their set-points are primarily rule-based or come from a central controller. Decision-making in the secondary objectives may utilize centralized, decentralized, or distributed controllers. Given the secondary controllers share critical information with the local controllers, this component is inherently cyber-vulnerable and can significantly impact controller performance.

Decentralized approaches involve situations where multiple clusters are weakly coupled, and therefore, decentralized approaches can degenerate into local approaches if the control area for decentralized approaches is limited to one node. Therefore, local and decentralized techniques are often used interchangeably in the literature.

2) Centralized Approaches

Centralized approaches require the power system state measured by the sensors, including the topology of the ADN [145], to be communicated to the ADMS. The controller may employ grid computing to generate the control signal utilizing mathematical optimization algorithms or meta-heuristic methods. Subsequently, the ADMS communicates the set-points to the corresponding actuators throughout the ADN. The computation process assumes a static snapshot of the power system – or often, these approaches actively utilize forecasts. Alternatively, if the algorithm is fast enough, including communication, these algorithms can participate in a faster time scale. Therefore, these algorithms could be both static and dynamic. Given the collocatedness of the necessary information, stochasticity within the power distribution system can also be suitably incorporated. Given extensive reliance on the non-ideal communication network with (i)

TABLE 2: Classified Recent Voltage Control Schemes with DERs

Architectures	Methods	Control Devices	Voltage Controller Objectives	Secondary Objectives
Local Approach	Droop/ Sensitivity based	PVs	Maintain the voltage within limits through reactive power injection [50]	Centralized control for active power curtailment
		WTs	Sensitivity-based injection of reactive power, with minimal curtailment of active power generation [59]	Offline determination of sensitivity curve needed
		IBRs	Obtains a piece-wise P(Q) characteristic curve for a PV-inverter that aims to inject suitable Q for varying P-injection [118]	Centralized optimization for fixed Q(P) determination
			Droop itself is adapted based on historical voltage profile while ensuring zero steady-state error and control system stability [84]	Centralized optimization for periodic droop update
			Considered cost function to be minimized isolates the problem to be solved locally; local control is based on the gradient of the cost function [51], [86], [87], [119], [120]	No communication needed
			Parameter estimation technique is applied to obtain Q-V characteristics of inverter for droop-control [85]	Centralized optimization for inter-day Q-V determination
		DERs	Distribution network partition using sensitivity-based analysis, Q-V curve parameters are updated in decentralized control through forecasts, real-time reactive power injection in a droop-control [88]	Distributed ADMM is used for tuning Q-V characteristics for multiple areas
			Local control is carried out per-second basis follows Q-V curve [121]	Central controller provides corrections based on Multi-time-step optimization
			Sensitivity-based control of active and reactive power, with the introduced damping factor to limit reactive power oscillation among DERs [122]	Sensitivity factors are based on system parameters
			Local Q-V droop control is carried out [123]	Centralized clustering based on R/X-ratio and Z and successively with K-means clustering to identify droops
			Local Q-V droop control with deadband is carried out [124]	Centralized stochastic quadratic programming for droop-characteristics determination
			Lower level controller acts based on local voltage measurement and regulates terminal voltage and power output [125]	Centralized controller solves both frequency and voltage control
		DERs and OLTCs	Autonomous control of DERs around a preset operating point and droop [126]	Preset operating point along with OLTCs settings provided be centralized optimization
		DERs, OLTCs and CBs	Local DER controller with piece-wise Q-V and curtailment characteristics [60]	Centralized minimization of the weighted sum of the loss, voltage deviation and active power curtailment
	Control-based	DERs	Discrete time local PI controller aims to minimize deviation from set-point [72]	Centralized controller solves loss minimization on a periodic basis; PI controller parameter is also tuned
			The controller uses the physics of the system to device the control law, with built-in linear disturbance observer facilitates accounting for system level uncertainties [127]	No communication needed
Centralized Approaches	Mathematical Optimization	PVs	Minimize the difference of ADN losses for a robust (column-and-constraint generation based) voltage optimization using MISOCP model [73]	Optimizer is self-sufficient
			Optimal self-adaptive dynamic optimization to minimizing voltage deviation from associated reference [66]	
		PVs and SSTs	Minimizes system level losses utilizing a combination of rule-based and gradient-based approach [74]	Optimizer is self-sufficient
		OLTCs and DERs	Minimizes second-norm of weighted control variables, with linearized constraints based on sensitivities to limit voltage within bound using QP approach [128]	DERs are coupled with AVRs with reactive power set-points from central controller

continued . . .

TABLE 2: Classified Recent Voltage Control Schemes with DERs (cont.)

Architectures	Methods	Control Device	Voltage Controller Objectives	Secondary Objectives
			Receding horizon problem with prediction, considering an unbalanced three-phase system, the problem broken into integer programming and non-linear programming [129]	Optimizer relies on the predictor accuracy
		OLTCs, CLs	Minimize set-point adjustment for loads and tap settings, and linearized voltage deviation [130]	DSO identify congested area, and demands within sensitive area are controlled
			Minimize the objective consisting of CVR, line losses, and inverter losses considering the power system model as SOCP [131]	No additional communication needed
		RCS, OLTC, Shunts, and DERs	minimize the weighted sum of active power curtailment, reactive power injection, and deviations from the control mean from current values; compared two models, namely MINLP-RC and MIQC [61]	Optimizer relies on state estimators
		OLTC, CBs, and DERs	Determining DER outputs based on multi-period stochastic optimization with MIQP model at a centralized location for a given OLTC and CBs setting [132]	Centralized MIQP model solution for determining OLTCs and CBs set-point
	Meta-heuristic based	DERs, EVs	Solve a multiobjective optimization problem considering impacts on neutral current, power loss, voltage imbalance, and bus voltage from average ADN-wide voltage utilizing differential evolution to coordinate EV charging [133]	Coordinates with DSO operations
		DERs, OLTC, and CBs	Minimize voltage variation within local ADN, while minimizing reactive power injection from the transmission grid using GA [54]	Power transmission and distribution network coordinated operation
		VRs and ESS	Multi-period, multi-objective optimization using PSO to minimize tap operation and reactive power injection along with other objectives [53]	Optimizer is self-sufficient
Decentralized Approach	Mathematical Optimization	DERs	Based on over/under-voltage condition, communicate influential DERs to device local control [134]	Fixed ϵ-partitioning is carried out to identify influential DERs
			Each area minimizes power losses using an SDP-based method while coordinating in a distributed (ADMM) fashion [80]	ADN partitioning is static and pre-provided
			Minimize second norm of voltage deviation given Thevenin-equivalent of the rest of the system [135]	Kalman filter is used for Thevenin equivalent calculation with electrical distance used for identifying zones
		ESS	Controller within an area minimizes voltage and own ESS SOC level subject to power distribution network condition, and share boundary information with neighbor [68]	ADN is divided using sensitivity based approach with fixed boundary
		Microgenerators	Minimization of reactive power loss based on available local measurements within a cluster, and inter-cluster information exchange [136]	Overall coordination is facilitated by a leaderless gossip-like technique
		DERs, Transformers	Reactive power injection for voltage control while maximizing EV charging capability [137]	Fixed clustering with substation agents are hierarchically controlled
		DERs, OLTCs	Coordinated voltage control in primary controller for each zones [75]	Adaptive zone-division clustering
		PVs and VRs	Each area minimizes a combination of power losses and active power curtailment with SOCP has been used for relaxation with each area coordinates using distributed (ADMM) and VR set-points are updated using branch and bound method [138]	ADN partitioning is static based on the location of the VRs
			PV-inverters solve local voltage control based on predetermined V-Q sensitivity factors and communicate their measurements to regulators [139]	Regulators identify tap settings that minimize long-term voltage deviation; ADN partitioning is static based on the location of the VRs

continued . . .

TABLE 2: Classified Recent Voltage Control Schemes with DERs (cont.)

Architectures	Methods	Control Device	Voltage Controller Objectives	Secondary Objectives
		PVs and EVs	Multi-time period predictive algorithm that minimizes reactive power injections from PVs while ensuring minimal deviation from the schedule for EVs is carried out for voltage control [140]	Louvain Algorithm is utilized for Distribution System Clustering that facilitates resilient performance
		DERs, ESSs, and OLTC	Predictive preventive and corrective mode, where DERs are expected to operate at MPP in the preventive and active power curtailment in the corrective mode, is devised to ensure second norm of voltage deviation is minimized with proper coordination with OLTCs [141]	Zones and critical bus selection with electrical distance
		Dispatchable DERs, ESS, OLTCs	Hierarchical controller ensures DERs respond to control area voltage variation [142]	ADN is adaptively divided into multiple zones, the centralized controller sets OLTCs
	Meta-heuristic based	PVs	Requisite clusters solve reactive power injection and active power curtailment minimizing problem using PSO [99]	Dynamic partitioning using modularity index upon detection of low voltage condition
			PSO is deployed in the daily operating horizon for multi-objective loss minimization, and voltage profile improvement [76]	ADN is partitioned into fixed cluster sets using spectral clustering method
		DERs	GA is deployed for multi-objective voltage deviation, and reactive power injection minimization for each control area [98]	Fixed ϵ-partitioning is carried out to identify the clusters; centralized controller also acts as backup
			Three-phase cluster-wide loss minimization with reactive power using PSO [100]	ADN is decomposed based on eigenvalues
		PVs, VRs, OLTCs, and SCs	Rule-based control is utilized for var-injection based voltage profile improvement [143], [144]	Clusters are identified based on tap-based voltage regulators
	Rule based	DERs	The controllers operate based on the broadcasted mode of operation, and associated capability curve of DERs [97]	Centralized entity decides the mode of operation
		VRs, CBs and DERs	Rules developed based on the physics of the ADN [96]	Control areas are divided based on locations of voltage regulators
Distributed Approach	Consensus based	DERs	Primary controller responds according to droop [89]	Secondary cooperative controller generate primary control law in a distributed fashion
			Cooperative controller facilitates distributed estimation of total power generation and utilization ratio [145]	One of the DERs communicate with SCADA
			Two stage control with the first stage iteratively control local voltage based on predetermined sensitivities with reactive power, and the second stage uses coordination among controllers with both active and reactive power [146]	No additional communication needed
			Fuzzy logic based max-min algorithm for voltage quality enhancement [147]	Consensus-based parameter estimation
		ESS	Control both active and reactive power injection from ESDs for proportional power sharing [62]	Optimizer is self-sufficient
		IBRs	Global voltage regulation with proportional load sharing, while alleviating droop-control [90], [148]	Dynamic consensus protocol for average voltage estimation
			Distributed cooperative secondary voltage control considering microgrid dynamics to facilitate droop control for primary controller [149], [150]	Distributed consensus facilitates reference voltage tracking
			ADMM-based ACOPF with inexact primal and dual update [151]	No additional communication needed
		DERs and CLs	GSPSO-based control to minimize real power loss [77]	Consensus-based parameter estimation to facilitate controller application

continued . . .

TABLE 2: Classified Recent Voltage Control Schemes with DERs (cont.)

Architectures	Methods	Control Device	Voltage Controller Objectives	Secondary Objectives
		DERs, CBs, VRs	To minimize the second-norm of voltage deviation within a microgrid with distributed consensus-based optimization [70], with CBs and VRs are operated based on the forecast while being coordinated with time delay [152]	Optimizer is self-sufficient
		PVs, WTs, ESS, CBs, CHP	To guarantee proportional reactive power sharing in the steady state [55], [153]	Uses consensus protocol to identify weighted reactive power measurements
	Dual/First-order Gradient based	IBRs	Minimize second norm of voltage deviation [58], [154] and weighted reactive power injection [58]	Built-in additional controller that seamlessly switches between local (can be droop based or otherwise) and distributed control
			Feedback-based [155] operational cost of reactive power injection minimization, with communication limited among the controller nodes [48], [156], considering relaxed unbalanced three-phase system [24], [157], [158]	Controllers need to be aware of their relative locations and cluster determination
			Minimize second-norm of voltage fluctuation with two-hop communication requirement [71]	Optimizer is self-sufficient
			Feedback-based minimization of operational cost of both active and reactive power injection [56]	
		Microgenerators	Minimizes ADN-wide losses; the problem is solved in two stages: locally dual-ascent is solved to update the dual variables, minimize the lagrangian for the determined dual variables [57], [79]	
		DERs	Minimization of QP-based weighted voltage deviation problem with unbalanced three-phase system [65]	
			Each controller gets randomly selected and solves active and reactive power-based voltage control using the interior point, with the selected controller node and its neighbor simultaneously updating the set-point [159]	Secondary controller identifying neighboring nodes upon reconfiguration
		ESS, PVs	Minimizes total ADN-wide loss in a faster time scale; the algorithm utilizes decomposability of SDP [78]	No additional coordination needed

delays, (ii) packet loss, (iii) outages, and (iv) cyber-attacks, often, the state estimators are involved in weeding out the bad data, and the algorithms need to account for necessary delays. Problems within the communication networks could prove detrimental to the ADN operation [161], and therefore, the control approach needs to be highly robust to missing sensor information, unresponsive actuators, etc. Furthermore, users can be wary of sharing private data with the ADMS.

Centralized approaches utilize power system models to determine optimal set-points, and the level of detail in the plant model impacts the feasibility of the generated control signal. Relaxations are extensively used instead of complete ACOPF models with LP, QP, MISOCP, MINLP-RC, SDP, etc., to guarantee fast convergence. Approximated models such as branch-flow and bus-injection models are specifically used for the ADN power flow equations. Combinatorial optimization techniques, such as branch and bounds, relaxations, projections, or proximal methods, are used to control conventional devices with discrete set-points. Metaheuristic methods are able to accommodate both discrete and continuous variables but do not guarantee the optimality of the algorithms. Predictive algorithms (and hence prediction accuracy determines the validity of deployed approach) are extensively used in this paradigm, given the limited scope of control of conventional devices. Centralized approaches provide a means to be properly coordinated with slower-acting conventional devices. Therefore, as seen in the table, prediction and coordination are part of the secondary objective. Notably, all other architecture can devolve into centralized ones, where all the computations are performed at a centralized location. Therefore, centralized techniques are just representationally different compared to other architectures.

3) Decentralized Approaches

Decentralized approaches originate from the spatial or level decomposition of the power network [93]. In the current context, the ADN can be segregated into multiple clusters, and the sensors within a cluster communicate with the lead controller for decision-making. This way, the communication load decreases significantly, relaxing the single-point-of-failure problem. These clusters are weakly coupled; hence

they don't require fast communication. Clusterization also simplifies the original optimization problem by reducing the number of variables of the original problem. It is also introduced as a semi-coordinated approach in some literature.

Different methods of creating subsystems, or clusters, can be found in [162], and as shown in the table, methods such as ϵ-partitioning, adaptive zone divisions, sensitivity-based approach, electrical distance, modularity index, eigenvalue-based decomposition, are among a few used for clustering. Notably, these clustering methods are a part of secondary objectives and are not part of real-time decision-making. Physical devices, such as voltage regulators and tap-changing transformers, are often used to segregate clusters. Cluster boundaries can be static or will be allowed to change dynamically (determined at the supervisory level using sensitivity-based approaches or utilizing machine learning), making these approaches primarily hybrid. All of these clusters can be further coordinated via a central coordinator, making them hierarchical, or these clusters can coordinate with each other at an equal level, exchanging boundary information. Decentralized approaches are inherently hierarchical since the upper layer is implicitly in charge of clustering while the lower layer actively participates in the decision-making. Clustering, too, can be performed in a hierarchical fashion.

Decentralized approaches can utilize mathematical optimization algorithms, meta-heuristic methods, or rule-based techniques. As in centralized approaches, full AC-OPF models, their relaxations, and approximated branch-flow or bus-injection methods could be used for each cluster. These algorithms can accommodate both continuous and discrete variables. The algorithm needs to be robust enough to the delayed/missing sensor information, unresponsive actuators, unresponsive clusters, etc. The unavailability of sensor information at the central level requires database management if the boundaries are allowed to change like a holon [18], which facilitates self-organization capability. The holonic database management can facilitate changing cluster boundaries.

4) Distributed Approaches

Central coordinators are largely absent in the distributed control, and local controllers, in turn, communicate with their neighbors to reach a consensus. These approaches are relatively newer, wherein each controller is associated with a sensing, computing, and communication agent. All of these controllers are autonomous and reside at a similar hierarchical level. Unlike the decentralized approaches, the clusters are tightly coupled. The distributed approach can degenerate into a local approach without communication or into a decentralized approach with weaker coupling. One can compute the control signal utilizing a distributed algorithm at a centralized location utilizing necessary measurements. Therefore, defining a distributed approach relies on its implementation. A detailed overview of distributed control approaches is provided in [16], [17].

The computing agents associated with each of the controllers can collectively utilize the 'measure-communicate-update-deploy' approach to solve the control problem. The coordination requirement makes the bi-directional communication network mandatory for determining the control action. The communication agent of each controller facilitates inter-controller communication, wherein the communication network can be sparse or dense. If these approaches rely on multiple 'communicate-update' cycles before the control signal is deployable, these approaches become static. Alternatively, the control algorithms can dynamically solve the control problem assuming the ADN to be in a closed feedback loop. Since the availability of sensor data is limited to the local controller, the privacy of the local information is assured. Given communication will be actively needed for the determination of control action, fast-communication network availability will be crucial.

Distributed methods involving multiple computational entities may require consensus-based methods or distributed control/optimization involving the exchange of primal and dual variables. Since distributed algorithms are majorly formulated by decomposing the original centralized optimization problem, this solution can be proven to be global optimal [163]. Consensus-based algorithms involve the use of sub-gradients to determine optimal control decisions or rely on consensus algorithms to determine ADN-wide state variables for local control actions. Lack of data availability at a central location makes computing higher-order derivatives challenging [8]. Consequently, most distributed control algorithms rely on first-order approaches, utilizing gradient or duality-based methods. Hence, their convergence rate is relatively slow. Non-linear AC equations representing the ADN are difficult to solve in a distributed fashion, so utilized models are often limited to bus injection or branch flow models. The scope of secondary objectives will be limited to the determination of ADN state through dynamic consensus, cluster determination, or providing set-points to conventional devices. Given DERs are expected to be coordinated with classical control devices, it can be expected that the overall problem will be mixed-integer in nature. However, guaranteeing optimality with the MINLP problem even with first-order approaches is extremely difficult, and therefore, literature in regards to solving the MINLP problem for ADN through distributed approaches is extremely limited [164]. Furthermore, even if an algorithm is entirely distributed, network monitoring for performance analysis requires data to be aggregated in one place.

Discussion: The literature discussed above is not exhaustive; however, from Table 2 and the above analysis, it is imminent that an algorithm can seldom be represented by one particular architecture/approach. As highlighted in the column identifying secondary objectives, in a practical implementation, different architectures may operate in different timescale in parallel [14]. Given the requisite DER integration with the ADMS, monitoring data needs to be available at a centralized location. None of the approaches (including local approaches) can operate without the involvement of communication infrastructure. And the absence of communication

would dearly cost in terms of optimality and robustness of algorithms. Multiple different approaches at different timescale would coordinate and facilitate the decision-making. In terms of deployment, approaches/architectures other than centralized and the ones with fixed cluster boundaries suffer from database management challenges. Implementation of a centralized database management system can make the implementation approach federated. Alternatively, information can be stored locally, and local information can only be shared among the neighboring controllers/coordinators in a peer-to-peer (P2P) fashion. Both of these aspects can significantly affect the performance optimality of the algorithm, quickness of convergence, etc., or can even make the algorithm challenging to deploy in the real world. Holonic control facilitates dynamic database management, facilitating a power system node to switch between clusters. Such a dynamical arrangement makes these algorithms cyber-resilient. This way, distributed and decentralized approaches would provide scalability and solve the single-point-of-failure challenges of centralized approaches. Since each DERs must be connected to the local computing agent to be controlled, if suitably designed, distributed approaches can better facilitate plug-and-play capability. Although the secondary objectives often run at a slower time scale, it does not imply compromising it due to cyber-vulnerabilities won't have catastrophic consequences.

B. EXTENSION OF CLASSICAL DEFINITIONS FOR VOLTAGE CONTROL

Classical controller classifications do not make explicit comments on the needed frequency and criticality of communication and how those communicated data would facilitate decision support. Primary controller algorithms are also coupled with additional communications as a part of secondary objectives. Although such an issue is partially addressed in [10] through an extended classification, it fails to cover all the possible subtleties in the architecture, accommodate the database management system to enable the much-needed self-healing capability, and provide extended commentary on controller performance. For example, conventional distributed approaches are iterative, but they don't discriminate against static and dynamic approaches with significantly different dynamics and performance guarantees. Static approaches with distributed optimization require multiple computation cycles for decision-making compared to dynamic approaches, which can self-correct. Therefore, static approaches are more cyber-vulnerable. Contrarily, dynamic approaches rely on the power network for feedback, and hence, all the algorithmic disturbances are directly injected into the power grid. Local approaches are primarily dynamic and require communications at a slower time scale under hybrid approaches. Both centralized and decentralized approaches can be either static or dynamic. Each of these aspects significantly contributes to algorithmic performance.

In contrast to these existing definitions, from the physical point of view, the power system, the controllers, the communication agents, and the coordinators lie on three different hierarchical levels, which could also be utilized for voltage controller classification. Three domain-related objectives for classification have been introduced in [6], such as (i) Power System Domain, (ii) Cyber-Related Domain, and (iii) Decision-making-related domain. These extended definitions are further elaborated here and are crucial since controller performance relies on (i) control objectives and the model of the power system utilized that are in the power system domain, (ii) frequency of information fetched from the sensors and type of communication employed, which are in the cyber-related domain, and (iii) the utilized algorithm, which is in the decision-making (control/optimization) domain. The expected impacts of these domain-related aspects on the controller performance are described as follows:

1) Power System Related Aspects:

The modeling details of the ADN determine the convergence rate and quality of the generated control signal. Typically utilized models are branch-flow, bus-injection, and complete ACOPF models. Also, one needs to be cognizant of the modeling assumptions before utilizing them for certain applications. Once the power system model is determined, only a certain set of approaches will be feasible. Depending upon monetary implication, and scope of operational implication, certain power applications for voltage control would be more vulnerable (e.g., volt-watt algorithms and ones involving switching are more vulnerable).

2) Cyber Related Aspects:

While the classical controller definitions are built around requisite communications, specifics of the communication infrastructure can often be missing. As discussed earlier, time-decomposition facilitates separate analysis of fast and slow control components, where slow-moving components are classified as 'a sporadic' and fast-moving components as 'a frequent.' Furthermore, nonidealities of the communication channel: (i) delay in the communication channel, (ii) packet loss, (iii) outage of communication channels, (iv) cyber-attacks, etc., would significantly affect algorithm performance which is often not accounted for in the existing literature. Notably, these non-idealities would differently impact requisite algorithms involving aperiodic and periodic modes of communication and the criticality of the information being communicated. For example, self-organization capability or self-healing, an important component of the smart grid, involves crucial information exchange but requires on-demand aperiodic communication. Communication infrastructure is also susceptible to both physical mutilation and cyber-attacks and would directly impact algorithmic performance. Failing to isolate the compromised physical nodes may harm overall controller performance [158]. Therefore, cyber-requirements of the voltage controllers would be required to be extensively looked at.

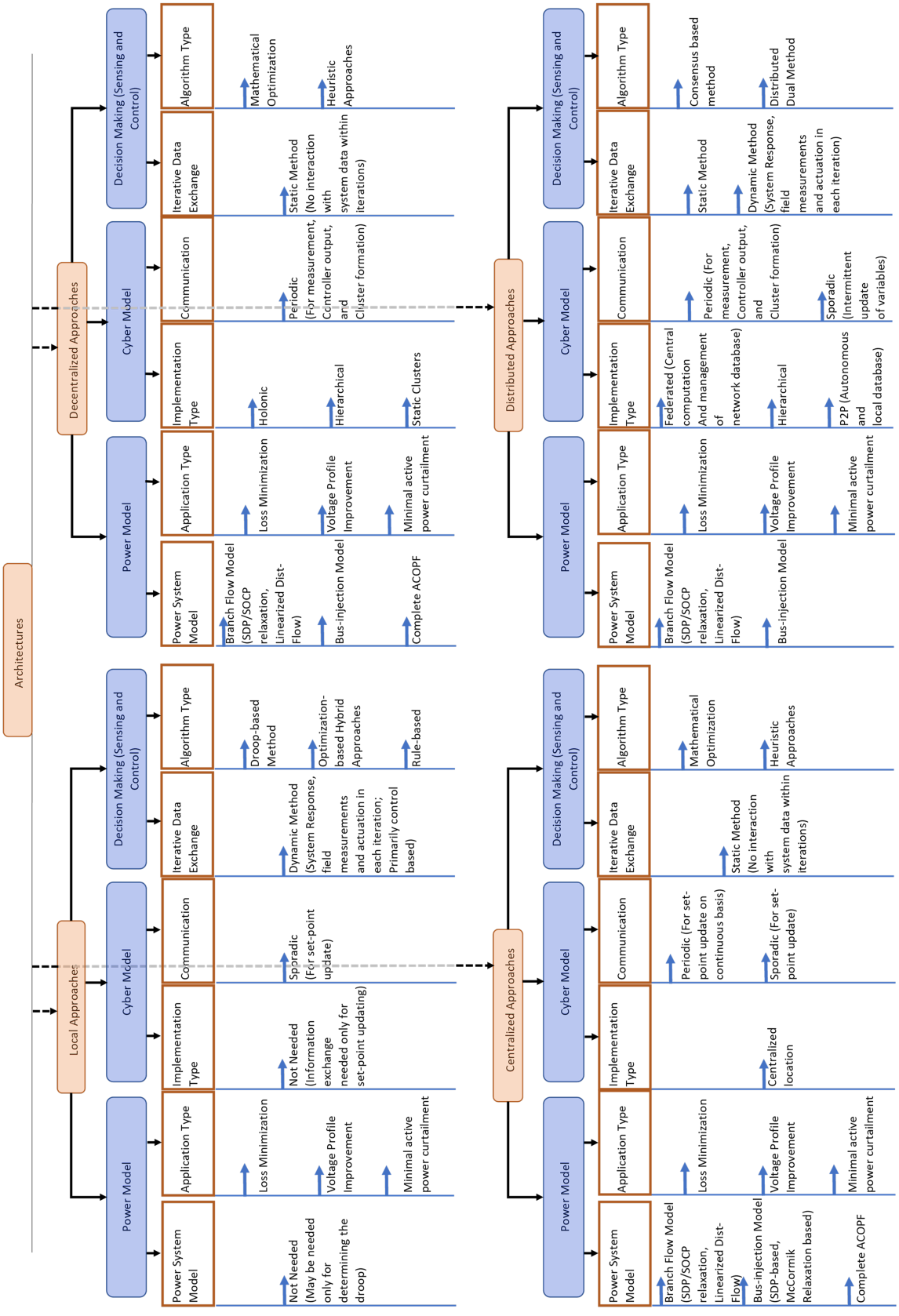

FIGURE 1: Taxonomy of Different Voltage Control Approaches.

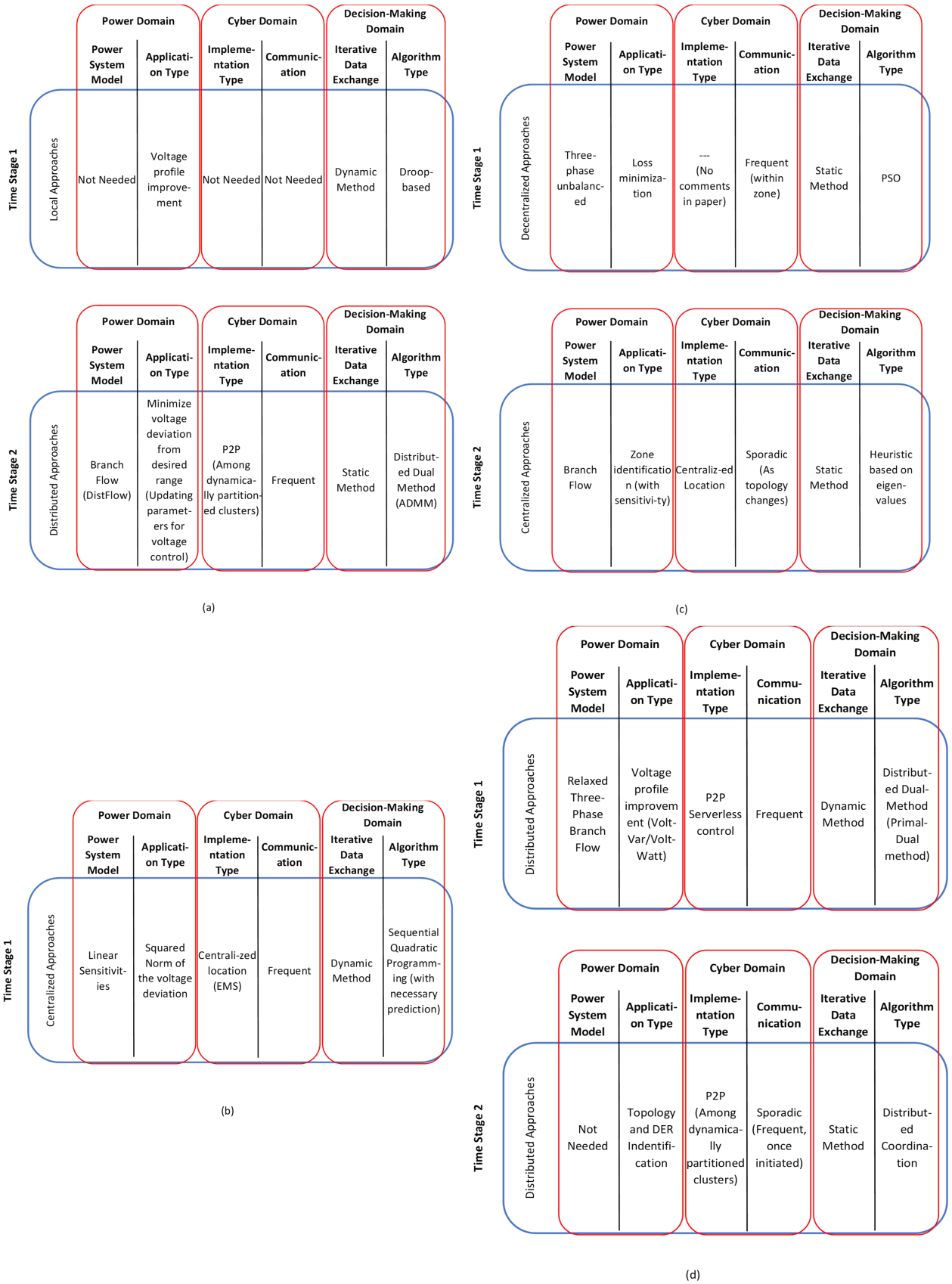

FIGURE 2: Voltage Controller Taxonomy: A Comparison — (a) Local, (b) Centralized, (c) Decentralized, (d) Distributed.

3) Decision-Making Related Aspects:

Mathematical guarantee of the underlying controller algorithm, its reliance on the communication network, efficient utilization of measurement from the power system, robustness to noisy measurements, model inaccuracies, and even cyber-attacks impact the controller performance. For example, dynamic algorithms actively utilize the power network to protect themselves against model inaccuracies; however, these algorithms should guarantee that the response of the feedback system should not be detrimental to overall power system operation. As discussed, The algorithms may include mathematical optimization problems, optimal control problems, and heuristic approaches; each has its limitations in terms of types of variables (continuous v/s integer variable), computation time, and overshoots in the plant in the case of feedback-based approach.

Discussion on Alternative Definitions: In Fig. 1, we have tried to reclassify the existing literature based on these newer definitions. Notably, sub-classifications, as shown in the figure, are not exhaustive. Rather, it is imminent that both the classical and the extended definitions together would better identify the taxonomy for classifying the controller performances. The provided readjustments do not make any commentary on the secondary objectives as highlighted in Table 2. Also, as shown, the architecture of the secondary objectives could be independent of the primary controller architecture. For example, if a controller architecture involves three different time scales (say, seasonal basis, daily basis, and real-time), each of which is implemented using different architectures, subsequently, time-decomposition could be utilized and treat the decomposed algorithms separately. Furthermore, the output of one control algorithm is used as an input for another set of algorithms. However, all of these approaches will be considered together for performance analysis. Such a methodology simplifies the treatment of hybrid approaches. Understanding the significance of coordination in different time stages would help us develop requisite metrics identifying overall controller performance.

Utilization of time-decomposability to develop the proposed taxonomy has been demonstrated in Fig. 2. Four examples from each of the four architectures, as present in the literature, have been utilized in this case. Here, local approaches is from [88], centralized approaches from [128], decentralized approaches from [100], and distributed approaches from [24], [157], [158]. As discussed in the comparative treatment, in Table 2, the decomposed problem can have multiple architectures. Also, some of the outputs of the problem being solved in a slower time scale would act as an input to a faster time scale and impact the overall operability. An algorithm could operate in a similar time scale with different architecture but in stages. For example, methodology in [77] involves GSPSO for real power loss minimization by each of the local controllers, with a consensus-based method utilized for parameter determination in the upper stage. Here, we can re-identify the local approach as local-distributed, the decentralized approach as decentralized-centralized, and the distributed approach as distributed-distributed, conforming to the decomposability of those specific algorithms. Although there have been a plethora of research works carried out in regards to the hierarchical control approach, considering [124] as an example, the said technique is classified as a local-centralized approach based on our proposed taxonomy, and it has been appropriately categorized in Table 2. The taxonomy in regard to this work is presented in Fig. 3. It can also be observed that the proposed taxonomy could be extended to account for other 'smart grid' applications, highlighting the superiority of the proposed decomposition-enabled taxonomy.

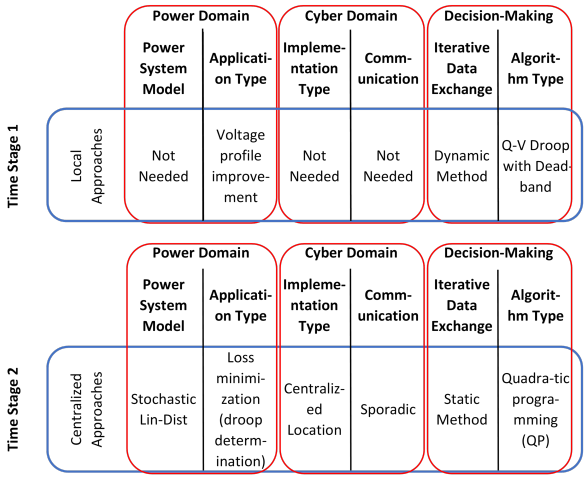

FIGURE 3: Controller Taxonomy for an example hierarchical coordinated voltage control

It is imminent that the data-flow directions, frequency of communication, and the data being exchanged considerably differ based on architecture, with possible differing cyber-impacts. The following section looks at possible modes of communications, utilized communication protocols, associated cyber vulnerabilities, and mechanisms to reduce the possibilities of cyber-attacks within a CPHS, highlighting subtleties for voltage control.

IV. CYBER REQUIREMENTS FOR VOLTAGE CONTROL WITH DERS

Increasing deployment of ICTs and advanced metering interfaces (AMIs) provide requisite communication for voltage control applications for all possible controller architectures regardless of the timescale of operation. However, even a less communication-intensive application might introduce interoperability issues due to differences in DER ownership and requisite coordination with conventional devices. Furthermore, conventional devices may require an entirely different set of communication protocols, requiring the introduction of customized middle-ware for translation. In the context of voltage control with DERs, vulnerabilities can be found on (a) poorly patched and managed conventional devices, (b) firmware/software or middleware used in newly integrated

ICT implementation, (c) communication network devices to connect the controllers and communication protocols used to exchange information. Unless the vulnerabilities within these different aspects are thoroughly mitigated and taken into account, the entire power system will remain prone to cyber-attacks.

The impact of cyber attacks on the power system has already been reported in the literature. In this regard, Iran's nuclear power plant was attacked via STUXNET worm, impacting around 200,000 computers and 1000 devices, mostly from industrial control systems in 2010 [165]. Ukraine's power grid was compromised in 2015 by a hacking group utilizing the compromised information systems of three distribution utility companies, and electricity access of 225,000 customers was temporarily disrupted. A malware named Black Energy was primarily used for remote access [166]. The US power grid was impacted by a denial-of-service (DoS) attack through the exploitation of the vulnerability within the firewall web interface [167]. Furthermore, an increasing number of reports on vandalism on the power distribution system is noted in the US power grid [168]. As smart grid device penetration in the power distribution system increases, the scope and impact of cyber and physical attacks on the ADN will also rise.

Each of the different communication technologies has limitations in terms of (i) theoretical and practical data rate, (ii) latency, (iii) coverage range, (iv) specific vulnerabilities, and (v) operational and maintenance cost. Therefore, the algorithms dictate the communication medium of choice. Even if an architecture requires sporadic communication, as and when needed, these specific information exchanges need to be prioritized over other DER-related communication in a limited-bandwidth communication channel. For example, set-point, droop, and even exchange the model database for self-healing require prioritization. If an algorithm requires real-time communication, communication protocols and associated vulnerabilities would significantly impact the controller's performance. While the voltage control application may not require frequent user intervention, the same DER could serve multiple other applications, including reporting monitoring information to the ADMS [12] utilizing different architectures, and each of these applications and associated architectures introduces an additional set of vulnerabilities. As the DERs are also subjected to periodic maintenance, firmware update, etc., in a multi-vendor, multi-user scenario, with increasing penetration of DERs, possible cyber-attack-surface are on the rise.

Therefore, it will be crucial to analyze various communication technologies leading up to voltage control, requisite standard communication protocols, possible vulnerabilities, and mitigation techniques, to understand cyber needs for the proper implementation of voltage control applications with DERs. Although the discussed majority of threats and mitigation strategies remain generic to all DER-controlled applications, our focus would be limited to the specific nuances of voltage control with DERs and relevant architectural aspects.

A. COMMUNICATION TECHNOLOGIES

The communication layer of a typical smart grid application can typically be classified into (i) Industrial Area Network (IAN)/ Home Area Network (HAN), (ii) Neighborhood Area Networks (NAN)/Facility Area Network (FAN), (iii) Local Area Networks (LAN) and Wide Area Network (WAN). IAN/HAN is typically limited to customer premises, and WAN is typically utilized for transmitting data over long distances where multiple communication networks are connected to exchange data to/from end systems or data communication over WAN. As the DER infrastructure grows to utilize WAN due to the involvement of multiple entities with conflicting interests, security, vulnerabilities, and fault tolerance gain immense significance.

If multiple behind-the-meter generators, such as PVs and BSDs, are expected to coordinate for voltage control, the use of HAN might be necessary. Notably, customer demand response (CLs) would also have an indirect impact on the voltage profile. It is envisaged that automated hierarchical controllers will take care of fine control of DERs with secondary controllers in charge of sending the set-points [169]. Even if the DERs are a part of the private area network of the public utilities, in a multi-user, multi-owner framework, remote access needs to be provided for maintaining and operating these devices [14], [170]. A comparative communication network architecture for each controller architecture has been provided in Fig. 4. Here, a smart device comprises sensors, actuators, controllers/coordinators, a database system, and communication units. Communication units would be needed even if the algorithm is local (the dataflow direction is not shown for local algorithms, for the associated communication at the slower time scale). Each of these algorithms utilizes WAN as the communication backbone.

Cisco, one of the major manufacturers of ICT devices, argues for the use of internet protocol (IP)-based networking in smart grid operations [171]. IP communication facilitates the satisfaction of requisite interoperability standards through private area networks. Therefore, DERs, vis-á-vis voltage controllers, are often built to operate with IP-based communications and open standards. Multiple communication technologies, such as DSL/ADSL, coaxial, PLCs, Ethernet, EPON/GPON in regard to wired communication, and ZigBee, Wi-Fi, Cellular (3G/4G/5G), including WiMAX and LTE facilitate IP-based communications [13], [172].

Each of these technologies comes with its own disadvantages, e.g., while the low voltage lines could be utilized for communication, their applicability is limited to a narrowband range. On the other hand, the use of a private fiber-optic network could be cost-prohibitive. Ethernet suffers from delays in the long-range and its shared access mechanism. Communication with the wireless medium can be a viable alternative depending on the voltage control applications, data rate, and distance of end-to-end devices. Wi-Fi is suitable for faster in a small range and cost-effective, but it suffers from

congestion as the participating nodes for communication increase compared to other technologies [173]–[175]. For faster data rate and long-distance exchange of data, WiMAX is more suitable; however, it's expensive and operates in a high-power range [176], [177]. Zigbee, on the other hand, might be a potential solution for cost-effective, higher efficiency and data rates in a shorter range [178]. Therefore, as discussed in the literature, although distributed dynamic voltage controller requires fast communication, it is robust to communication delays [48]. A detailed comparison of these communication technologies, in terms of their coverage range, latency, reliability, maximum data rate, and underlying protocol, is provided in [13].

From the algorithmic standpoint, we need to look at all the sub-classifications in Fig. 1 to determine the necessary communication technology. In this regard, the following questions are required to be asked e.g., (a) how is the data being stored and exchanged (implementation type)? (b) what is the needed frequency of communication? (c) criticality of the information exchange, and what if the communication could not be established? (d) how severe would it be if the communication gets compromised? Notably, implications due to the deployment of multiple applications in a single DER also get indirectly embedded within the selected communication technology. From the communication architecture point of view, ownership of the communication network matters. For example, if the communication is processed through WAN, each of the DER nodes could be publicly accessible and needs to be secured via individual firewalls. Alternatively, the communication network could be owned and operated by individual utilities or operated in a public network through a remote VPN. Given the DERs ownership would vary, alternative arrangements/ management interface needs to be in place. Additionally, if the communication medium is wireless, it will suffer from associated vulnerabilities in contrast to wired communications. The choice of private area network vs. WAN is also limited by the choice of communication medium. Notably, smart-grid communication architectures are still under development, and many possible communication architectures could co-exist [179].

Technologies that rely on wired communication have installation difficulties, while wireless communication utilizing public area networks, if not protected by advanced authentication standards, would introduce cyber vulnerabilities [180]. Wireless networks can be susceptible to evil-twin attacks, jamming attacks, etc. Also, requisite encryption can significantly impact the needed latency for appropriate control in certain architectures [181]. Both wired and wireless networks could be susceptible to theft and mutilation. The requisite protocols and middle-ware requirements and the vulnerabilities are the manifestations of the real-world deployment of a control algorithm. Notably, the DERs controllers are also vulnerable to physical damages, especially in the outbreak of natural disasters, requiring attention. Therefore, these vulnerabilities and associated mitigation techniques are discussed in the latter part of this section.

B. COMMUNICATION PROTOCOLS

Communication protocols facilitate seamless data exchange for intra-DER communication and would play a significant role in voltage controller performance. Existing standard communication protocols recognized by the IEEE 1547-2018 include IEEE 1815, IEC 61850, Modbus, and IEEE 2030.5 [182]. These standard protocols are the building blocks for the recent Open Smart Grid Protocol (OSGP) published by the European Telecommunications Standards Institute (ETSI) [183]. Notably, these protocols may not be interoperable, and different DER vendors may use different communication protocols such as SEL fast message [184]. These interoperability issues necessitate the use of protocol converters. Here, the discussion is limited to standard communication protocols for DERs:

1) IEEE 2030.5

Smart Energy Profile 2.0 has slowly become IEEE 2030.5 protocol in recent years to meet requirements of IEEE 1547 standard [185]. This protocol is being actively developed to facilitate communication among various entities within the smart grid [38], [186]. IEEE 2030.5 can be used to implement different DER scheduling algorithms, facilitating operators to control them remotely utilizing communication over IP using TCP or UDP [187]. This protocol is recommended as the default application-level protocol for California's Rule 21 [182] facilitating DERs to participate in Volt-Var support, power factor support, and provide soft-start and ride-through capabilities. This standard protocol is lightweight, has built-in security mechanisms, and could be implemented for edge-connected DER controllers. Therefore, these protocols are suitable for all possible control architectures.

2) IEEE 1815:DNP3

IEEE 1815:DNP3 is a distributed (communication) network protocol generally used for process automation and remote control in the SCADA system. It was initially developed to facilitate coordination among existing distributed (communication) network protocols and IEC 61850 and facilitate better device interoperability. Therefore, it is also widely used with DER control [188]. In [189], authors discussed real-time volt-var control tools with DERs using DNP3. It facilitates real-time communications for DERs and performs remote operations from the substation [190], [191]. Features of the DNPs include secure remote operation, addressing multiple devices over a serial or ethernet link, broadcasting messages, time synchronization, time-stamping events, getting unsolicited data from sensors, and facilitating rapid communication among DER agents.

3) IEC 61850

IEC 61850 is a set of protocols consisting of Sample Values (SV), Generic Object-Oriented Substation Events (GOOSE), Manufacturing Message Specification (MMS), etc. These protocols constitute a hierarchical architecture, facilitating object-oriented abstraction of data items. Such an abstraction

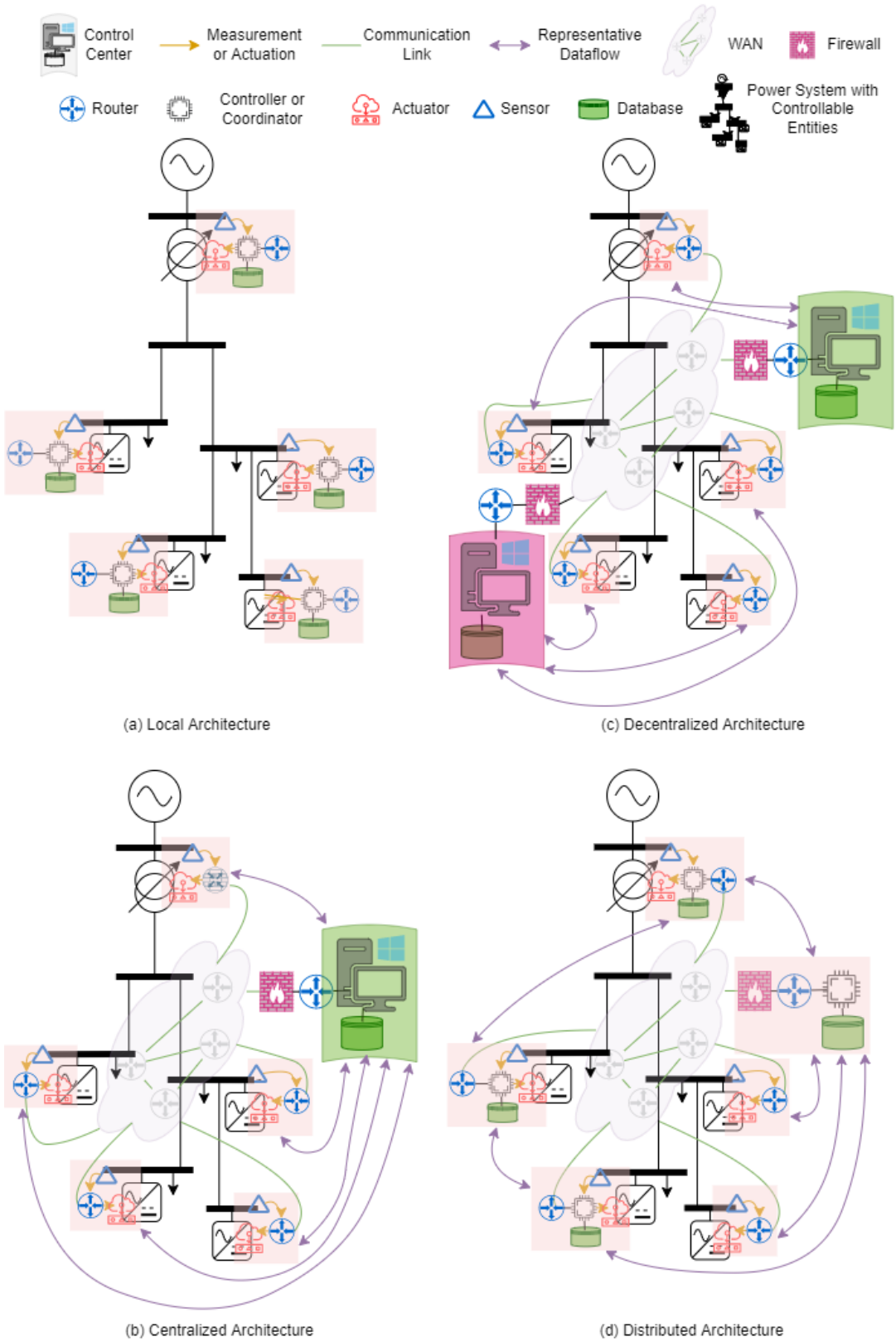

FIGURE 4: Controller Architectures for Voltage Control with Communication Architecture.

provides flexibility in communication among DER-devices [192], [193] quite significantly. Although this protocol was developed for communication within the substation, it could be suitably leveraged for voltage control application [194] as well as can be adopted for different architectures, including distributed [195], and the ones requiring both periodic and sporadic communication.

4) Modbus

Modbus is one of the earliest protocols used for process automation and control. it is widely used due to its inherent speed, interoperability, simplicity, efficiency, and reliability. Devices utilizing the Modbus protocol communicate with each other using a master-slave technique, where only the masters can initiate communication. Modbus-TCP or the Modbus RTU protocol is expected to work, where the messages are generally exchanged over TCP/IP. Voltage control in a multi-DER environment with Modbus-TCP protocol has been discussed in [196]. However, there is no predetermined master in the distributed or decentralized protocol, and hence, Modbus would be difficult to implement. Recently, a variant, namely, Modbus Plus, has been developed, where devices can be either master or slave, facilitating the implementation of modern architectures [197].

5) OpenADR

Given Open Automated Demand Response (OpenADR) was developed to support California's energy policy objectives, [198]–[200], it is compatible with IEEE 2030.5. DERs using other protocols require gateway devices such as energy management systems or aggregators for interfacing, introducing vulnerabilities. OpenADR provides multiple security features for communication while allowing flexibility in the information model.

Discussion on Communication Protocols: Therefore, as we can observe, all of these standard communication protocols at their current state support the four control architectures and would facilitate communication over different time scales. However, these protocols can lack interoperability, and as discussed in the next sub-section, each of these communication protocols has a unique set of vulnerabilities.

C. POSSIBLE VULNERABILITIES AND THREATS

These standard communication protocols provide rule sets for intra-DER or inter-DER communication. However, inherent vulnerabilities and the lack of security mechanisms make DER communication susceptible to cyber-attacks. Vulnerabilities of a typical CPHS can be analyzed based on the Confidentiality, Integrity, and Availability (CIA) triad [201]. Here, *Confidentiality* refers to the condition where unauthorized access to confidential information is prevented. *Integrity* implies seamless communication among multiple agents where the data contents being exchanged is protected, and *Availability* refers to unhindered access to information by eligible entities. Generally, the access control mechanisms such as the Authentication, Authorization, and Accounting (AAA) framework facilitate the establishment of the CIA triad.

Gaining access to DER controllers by a malicious agent exploiting improper implementation of the CIA triad with the AAA framework can have dire consequences. While an agent can penetrate into the DER system by exploiting vulnerabilities in any of the applications running within, once intruded, an attacker can gain access to multiple operating modes of the DERs through further exploitation such as privilege escalation, or enumeration [202]. Once compromised, an attacker can have the required administrative privilege to manipulate multiple DER applications such as retail electricity market operation, frequency control, emergency control, remedial actions, etc. If the controller design is not robust enough, it can take down an entire ADN. Cyber vulnerabilities could result from numerous communication networks, physical devices, and host-related factors. What makes it worse is other external factors helping attackers to exploit those vulnerabilities, such as improper system design, lack of security-related training by the management personnel, irregular communication network and device health checks, not following required defense standards, etc. These added external factors on top of the vulnerable systems, networks, or hosts help adversaries gain access to a system.

Such a broader class of impact requires consideration of both communication networks, associated protocols, and vulnerability mitigation techniques to understand the real-world performance of the controller. In conjunction with physical threats to controllers in the advent of natural events (e.g., measurement error and subsequent bad data, faults and subsequent ADN reconfiguration, outage of controllers themselves during natural events or vandalism, etc.), which is widely discussed in the classical literature, possible cyber threats also require attention. Both physical and cyber vulnerabilities can co-exist, and mitigating one's impact does not guarantee overall performance improvement. Notably, most of these attacks cannot exist in isolation — rather, it is a combination of different methods and steps that can be taken to carry out an attack successfully. Given the vastness of the associated literature, for the architecture-related comparison, we would limit the discussion to smart grid communication through WAN. The identified differences could be suitably extrapolated for other communication mediums as well. The taxonomy of various attacks performed by a malicious agent is given below:

1) Network Reconnaissance:

Network Reconnaissance is a generalized mechanism through which an attacker gathers more information on the devices connected to the communication network, vis-á-vis the power network. Here, in terms of DER-based voltage control, the attackers can find information about the DER communication network architecture, number of network devices, device vendors, number of smart DER sensors and their vendors, software running on each of them, open ports to get access to, the application running on the DERs, corre-

sponding IP and MAC addresses, etc. [203]. Notably, it will be easier to exploit vulnerabilities in the isolated controllers than in a control center (for both centralized and decentralized schemes) with multiple perimeter security. Alternatively, discussed possible human-in-the-loop increases also introduce the chance of an insider attack within a control center or the ADMS. Given local controllers also require sporadic communication, these can be exploited for reconnaissance. Given that distributed controllers require mutual coordination, one needs to be careful about the needed security, which does not significantly impact the implementation cost.

2) Spoofing:

Spoofing attack involves the adversary who tries to mimic a legitimate user. A spoofing attack can exploit multiple vulnerabilities in the device or network configuration to spoof a legitimate MAC address or IP address. One of the prevalent and existing spoofing attacks is spoofing through address resolution protocol (ARP) and redirecting the traffic from the victim's machine, which is also the first step for a kind of Man in the Middle (MiTM) attack. Individual DER nodes could be spoofed easily compared to the control-center node. Also, the probability of gaining access to multiple DER nodes gets negligible (a DER user can get compromised along with all the DERs it operates, but not all users can simultaneously get affected). In our context, spoofing can appear in two different forms: (i) exploiting the vulnerabilities in human-to-DER-controller communication, (ii) exploiting the vulnerabilities in the human itself. Once gained access, the attacker can subsequently expand their access to DER system services for launching future attacks [204]–[206].

3) Denial of Service (DoS):

In a DoS attack, an adversary attempts to flood the open port of a DER controller with unwanted packets, effectively disabling its operational capability. This can happen via exploiting the open port for DNP3 or Modbus communication or any other open port, such as the port used for file transfer protocol (FTP) for device patch upgrade. The adversary can gain access over multiple nodes in the cyber network to launch an attack, making it very difficult to block the said adversary, which is classified as distributed DoS attack. In the case of a centralized or decentralized architecture, the attacker has much incentive to DoS the control-center node itself. Since the chances of DoS-ing, multiple control-center nodes will be very small, and consequently, a decentralized scheme with multiple control-center would fare much better compared to centralized architecture. If a DoS attack impacts an individual DER node, both centralized and decentralized architectures would be able to reconstitute the missing information with the support of other applications. The impact of a DoS attack on local control would also be limited, and the associated performance of distributed voltage control architecture has been presented in [158]. It has been shown that in the case of distributed dynamic control, isolating a controller node segregates the controller into multiple clusters. Here, impacts would vary depending upon the algorithm selected.

4) Eavesdropping:

Eavesdropping could be utilized by a malicious actor to listen to the traffic containing DER set-points used in voltage control as well as for other applications. Once a particular DER node is compromised, the attacker thwarts the confidentiality of information exchange among the DER controllers. Subsequently, the attacker can access legitimate information about the ADN and its behavior which in turn can be used as input for other attacks [204]–[206]. Eavesdropping begins with reconnaissance. Therefore, compared to the control center, vulnerabilities within individual DER nodes could be exploited first for eavesdropping.

5) Packet Replay:

Replay attack aims to intercept the valid transmission of data, record it and re-transmit it later to disrupt normal communication among different entities [204], [205]. In power system applications, a replay attack might occur when DER chooses to communicate event information related to protection via the GOOSE protocol in the IEC 61850 protocol suite. GOOSE protocol doesn't use TCP/UDP and IP and runs based on MAC address, and is vulnerable to replay attacks [207]. This way, an attacker can confuse intelligent sensors involved in the DER communication system. Notably, TCP/IP-based communication can decrease the DER vulnerabilities from packet replay cyber-attack [206], [208] due to mandatory 3-way handshaking and acknowledgment mechanisms. Therefore, a lack of security mechanisms would lead to replay attacks. The architectures requiring sporadic communication (e.g., local controllers or providing updates to traditional voltage controllers) may involve exchanging information in this way and could be vulnerable to replay attacks. Impacts of replay attacks on the distributed dynamic controller performance have been depicted in [24]. This shows the significance of requisite security mechanisms in DER voltage control.

6) Man in the Middle (MiTM):

MiTM attack is possible if the confidentiality of the DER-controller communication is compromised, and its possible impact is the integrity of communicated data. Here, the adversary poses as the legitimate controller and redirects the traffic through the malicious device to gather information about the type of data and, in the worst case, change the data contents (sometimes referred to as False Data Injection attacks) before sending them to other controllers. This can be done via ARP spoofing on a LAN where all the DER devices are communicating [205], [206], [208], [209]. Notably, even if a power system node has been compromised by a MiTM, especially in a centralized scheme, the possible malicious/bad data can be filtered out, providing much-needed resiliency. The algorithms could be made robust to work under a limited dataset. Also, it will be highly unlikely that a control-center node

will become a victim of a MiTM attack. The scope of MiTM for the local controllers is limited, given that communication happens only sporadically. MiTM on the distributed voltage controller could be prominent, and controller performance in the presence of this attack is shown in [24], [158], where the optimizer is unable to converge. MiTM could be prevented by strong authentication and tamper detection.

7) Modified Firmware Upload:

This is another possible attack surface in DER communication. If the regular version and patch upgrade for DERs, (communication) hosts, communication protocols, etc., are not frequently provided, one might introduce new vulnerabilities such as buffer overflows or any other unrecognized modification. Even the attackers might modify the firmware separately, and upon implementation of that on DER devices, one can exploit those DER devices [208]. Modified firmware upload could have multiple purposes, such as further reconnaissance and capturing logs, to jeopardize the operation of the entire controller network. They can access processes running within the DERs, gaining more insights about the roles of DERs in ADN operation. Compromised DERs, independent of the applications running within them, are vulnerable to modified firmware upload. Although the DERs expect communications from certain nodes depending upon the underlying architecture, due to the presence of human-in-the-loop, nodes from which firmware could be uploaded may not be predefined. This makes modified firmware upload attacks stealthy. Therefore, access control may not be sufficient to prevent further attacks. Alternatively, as discussed later, privilege protection by patching all opened ports could significantly reduce these attacks.

8) Log Manipulation:

To preserve the bandwidth, all possible DER-operational logs may not be possible to be communicated to a remote database, and these logs will be accessed on demand. This is also important in modern distributed or decentralized architectures, where user privacy necessitates a no-log policy. In regard to voltage control, there are two potential ramifications: (i) from the maintained logs (if unsecured), the adversary would be able to identify potential applications running within the DER controllers, and (ii) if the logs have been tampered, DER operators won't be able to perform root-cause analysis. There are other potential implications if the logs are compromised [208]. This type of attack is generally carried out in the control center from where the DER devices are being monitored, and the corresponding logs are being saved in the Historian and/or other databases or the individual DERs in the cases of distributed or local architecture.

D. MITIGATION OF CYBER-THREATS IN VOLTAGE CONTROL

Independent of the architecture, communication is essential for the performance optimality of the voltage controller. Disrupting or creating disturbances in the communication network via any means of the previously mentioned attack has dire consequences where rapid communications are needed, and computational resource is also limited [209]–[211]. Alternatively, exchanging messages in plain text would lead the controller to remain vulnerable to adversaries. The vulnerabilities would extend to voltage control applications that require infrequent but crucial, on-demand information exchange. Performance impact on the voltage controller depends on the criticality of the exchanged information, which, in a way, determines the level of encryption and needed measures.

Over the years, various organizations such as the National Institute of Standards and Technology (NIST) [212], North American Electric Reliability Corporation (NERC)/Federal Energy Regulatory Commission (FERC) [213], IEC [214], IEEE, Internet Engineering Task Force (IETF) [215], and DOE [216] have come up with several cyber-security enhancement strategies with DERs. Frequently, in a multi-vendor DER penetration, updated security patch deployment can be beyond the capabilities of one organization. Therefore, potential zero-day vulnerabilities will remain unpatched for a significant period, which could lead to subsequent attacker exploitation. Given there will not be any one-size-fits-all solution, possible classified mitigation measure includes: (i) selective encryption of exchanged data [217], (ii) limit access to system entries through well-defined access control mechanisms. [209], [210], (iii) utilizing both Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) [218], [219], (iv) communication network segmentation through VLANs [202], [220], [221], (v) maintaining and securing traffic and action logs [211], [222], (vi) provide authenticated [223] patches and version upgrades [204], [217], (vii) securing unused ports and perform configuration analysis [211], (viii) utilize Transport Layer Security (TLS) for an encrypted communication link [204], [205], [217], (ix) utilize multiple Certification Authorities (CA) for authentication [182], [206], [217], (x) use sTELNET/sFTP for transferring any file into smart sensors within ADN. [208], [224], [225], (xi) encourage the use of complex passwords [205], [211], (xii) enforce the principle of least privileges [182], [208], [211], [226], (xiii) utilize VPN (Virtual Private Network) [18], [208], [227], (xiv) use multi-factor authentication [211], (xv) implement zone-based firewall rules in boundary networks to prevent unauthorized access. A detailed description and possible impact analysis corresponding to these best practices are provided in [12]. Resiliency analysis in a DER-based smart grid considering a combination of the above-mentioned mitigation techniques has been discussed in [228]–[230]. Suitable mitigation mechanisms corresponding to attack taxonomies have been discussed in Table 3.

Typically network architecture, device vendors, DER applications, and controller's data exchange requirements affect cyber-attacks, and there does not exist any one mitigation technique which can prevent a class of cyber-attacks. In a similar line as shown in Table 3, the mitigation techniques are divided into two parts, (i) mitigation techniques with △ can

TABLE 3: Mitigation Measures Applicable to Attack Taxonomy – △ : Directly helps attackers to initiate the attack, □ : Help attackers to exploit further vulnerabilities to launch an attack.

	Mechanism (i)	Mechanism (ii)	Mechanism (iii)	Mechanism (iv)	Mechanism (v)	Mechanism (vi)	Mechanism (vii)	Mechanism (viii)	Mechanism (ix)	Mechanism (x)	Mechanism (xi)	Mechanism (xii)	Mechanism (xiii)	Mechanism (xiv)	Mechanism (xv)
Network Reconnaissance	△	△	△	□	□	□	△	△	△	□	□	△	□	□	□
Spoofing	□	△	△	□	△	□	△	□	△	□	□	□	△	□	□
Denial of Service (DoS)	□	△	△	△	△	□	△	□	△	□	□	△	□	□	△
Eavesdropping	△	△	□	□	□	□	△	△	△	□	□	□	△	□	□
Packet Replay	△	△	□	□	△	□	△	△	△	□	□	□	□	□	□
Man in the Middle (MiTM)	△	△	△	△	△	□	△	△	△	□	□	□	□	□	△
Modified Firmware Upload	□	△	△	□	△	△	△	□	△	△	△	△	□	△	□
Log Manipulation	△	△	△	□	△	□	△	□	□	□	□	△	□	△	□

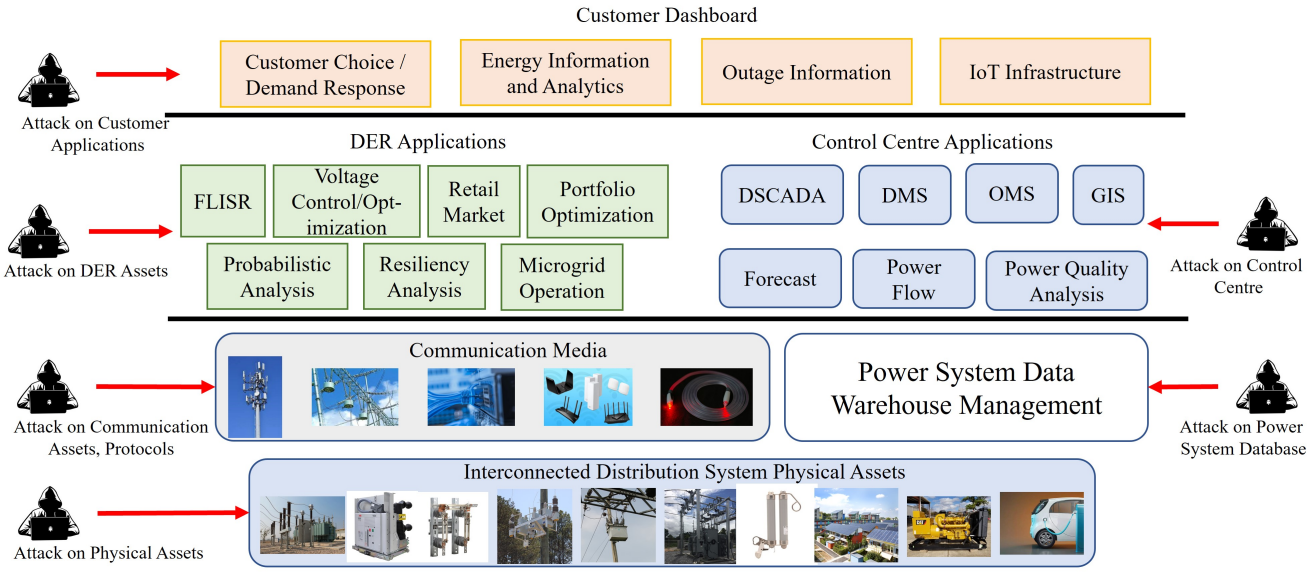

FIGURE 5: Grid Components to Applications: Ways to Attack the CPHS.

directly impact the specific attack taxonomy and (ii) as for the mitigation techniques with □, unless mitigated, it can help attackers to access/stay or escalate privilege in the network and look for further vulnerability to launch an attack. For example, for Network Reconnaissance, mechanism (ii) states to enforce access control in the network directly, which prevents attackers from gathering more information. Additionally, implementing mechanism (v), where logs are managed, and alerts are created based on the rules, prevents attackers from staying in the network and looking for access control flaws to start (communication) network reconnaissance. Also, if patching and version upgrading at regular intervals, according to the mechanism (vi), is not regularly implemented, the system doesn't get compromised immediately. However, if the controller firmware is not patched, attackers can open a potential backdoor to get into the system and look for other attack surfaces, such as weak passwords, open ports, weak access control, etc., for launching an attack.

Although these cyber-security best practices are generic, some gain immense significance from the DER control perspective. For example, given a multitude of DER controllers are required to be provided set-point from the system-operators organization, limiting access to system entries and the principle of least privileges for the system operators is important. Segmentation can be done based on running applications on the DERs using VLAN to prevent the impact of cyber-attacks on a single DER from propagating through the whole ADN. If it is difficult to implement, from the voltage control point of view, limiting access to system entries and securing traffic and action logs are important to avoid a coordinated attack. Process and memory virtualization ensures that even if one of the DER applications is compromised, its effects will not spread across other applications.

Furthermore, it is extremely difficult to audit individual cyber-security mechanisms, and it can be expected that the utilities would follow standards related to the smart grid, such as NERC CIP compliance [231]. Although these guidelines are specifically designed to protect the BPS from cyber

threats, these compliance mechanisms need to be followed for the extending active cyber components of the ADN. Also, utilities can follow MITRE ATT&CK framework for adversary emulation in ADNs to validate the security and defense mechanisms in place from time to time [232]. There are other frameworks, such as the NIST cybersecurity framework, which provides the idea of best practices to manage cyber security risks in smart grid [233]. Finally, it has been noted that the scope of each attack taxonomy varies based on the controller architecture. Therefore, given the criticality of the power system, cyber-security audits [234] are required to be frequently carried out to ensure that architecture-specific mitigation measures are actively deployed.

V. VALUE ANALYSIS FOR VOLTAGE CONTROL WITH DERS

The focus of this work is to identify the cyber-physical requirements for deploying a voltage control algorithm and the identification of real-world factors that impact the controller's performance. The first step in this regard would be to deploy the controller in a realistic test-bed and benchmark it across the existing algorithms. Numerous test-beds, including [158], [184], [187], [191], [218], [219], [235], exists in the literature. However, as highlighted in this work, the availability of a highly customizable test-bed encompassing all the aspects of a cyber-power system, facilitating testing of various controller architectures across multiple stages and time-steps, incorporating properties of realistic communication network, communication protocols, and facilitating the incorporation of vulnerability mitigation measures gains immense significance.

Nevertheless, once a thorough performance analysis is conducted, one needs to carry out a thorough value analysis before the deployment of a controller. Integration of DERs in the ADN for intra-DER coordination would necessitate significant infrastructural investments. Determination of siting and sizing of the substations and feeders involves the cost [236] component of the ADN in the cost-benefit analysis (CBA), and the benefit [237] constitutes of reduction in REG curtailments, reduced congestion, loss reduction in a multiyear framework. Similarly, the CBA with DER voltage control is provided in [238], [239], where the cost involved includes ADN reinforcements, transformer replacements or exchange, and their annual maintenance costs, while benefits are tied to the annualized ADN daily operation in terms of losses, renewable curtailment, and required reactive power compensation. Here, although the PV-inverters are considered to utilize local control architecture and are expected to respond to German grid code, the optimal operation of OLTCs requires AMI data, central processors, and distributed automation infrastructure. The costs in this automation infrastructure are elaborated in [240], where the cost of communication infrastructure, information processing, and data transmission costs – essential components for voltage control – are elaborated. However, each distribution automation infrastructure can serve multiple operational objectives. In [241], the costs for ADMS development are categorized into: (i) observability improvement, (ii) providing a decision support system, (iii) increasing situational awareness, and (iv) integration of IT and OT systems. Notably, cyber-security is a continual process, and associated implementation costs will be incorporated within operational and maintenance costs for the integration of IT and OT systems. Article [169] also highlights multiple levels through which DERs can interact with the power system, and all of these externalities require suitable incorporation in the CBA. Furthermore, as highlighted in Section II-A, the scope of voltage control devices operation is not limited.

It is demonstrated that each of the distribution systems assets participates in multiple DER applications. For example, smart switches within the ADN can directly contribute to FLISR and microgrid formation and indirectly to voltage control and retail market operation. Notably, smart switches are a core reliability improvement component of the utilities. PVs and electric vehicle infrastructures could have visibility in the customer portal depending on the ownership structure and would directly participate in the retail market applications. However, if suitably compensated, DERs would participate in resilient grid operations, ADN service restoration, and voltage control [49]. Widely used CVR, as discussed earlier, utilized for energy-efficiency programs utilizing devices such as OLTCs, VRs, and CBs can also be linked with voltage control.

The informational cross-dependency of the CPHS has been shown in Fig. 5, which is adapted from [242]. The bottom layer consists of physical devices within the power system, including automation, monitoring and actuation assets, and assets owned by the DER operators, aggregators, and customers. The second layer consists of various communication (physical and virtual) media and database management system. The third layer belongs to the core ADMS applications, such as distribution-SCADA, distribution management system (DMS), outage management system (OMS), geographic information system (GIS), forecasters, power flow, and power quality analyzers. These core components are an integral part of power distribution system operation, which, in a way, helps in the deployment of DER applications. Applications running within DERs are fault localization, isolation, and service restoration (FLISR), voltage control/optimization, retail market, resiliency analysis, and microgrid operation application, which will be carried out by the ADMS, with DERs being an active part within is also a part of this layer. DER operators would also carry out various probabilistic analyses and portfolio optimization for optimal utilization of their resources. Modern utilities also provide customers with retail choices, energy information analytics, and portals for reporting outages in the top layer through the customer dashboard. Fig. 5 also highlights various ways a malicious agent can intrude on the CPHS.

Therefore, given the inter-dependency among the operational assets in the ADN, multiple ways DERs would interact with the system and other externalities, a cost-benefit analysis

of voltage control in isolation may not be wise. The possibility of cyber-attacks through human dashboards also requires investment, although end-users may not directly enjoy the benefits of an improved ADN voltage profile. A lack of thorough investment analysis would question the equitable distribution of costs in the distribution system automation. Various considerations for the CBA in detail are available in [92].

VI. CYBER-PHYSICAL NEEDS FOR DER-BASED VOLTAGE CONTROL/OPTIMIZATION: A SUMMARY

The power system can be treated as a system of systems with multiple domain-related information interplay at various levels to control the CPHS successfully. Having one standard controller and communication architecture may not be well justified with multiple levels of data exchange. Given the vastness of the existing voltage control approaches in the literature, analyzing individual controller performance can be daunting, and a performance-oriented classification of approaches gains significance. Discussion in Sections III and IV has identified that analysis of the real-world performance analysis of voltage controllers is complex due to (i) architectural complexity, (ii) needed speed and criticality of communication, (iii) complexity of models and algorithms, (iv) requisite coordination with classical control devices, (iv) integration among multi-vendor devices, along with (v) challenges of real-world communication. Oversimplification of one-or-more aspects of the CPS needs to be carefully considered and should not question the real-world deployability of the approaches. To enable the same, an extensive classification encompassing all three domains of a CPHS (namely, physical/sensor, communication, and control/coordination) are tallied across classical definitions to develop a taxonomy that could be utilized to analyze the performance of any other CPHS. Furthermore, a thorough treatment of requisite communication layers and the associated impact on the controller performance has been provided. Commentary on recently flourishing hybrid controller architectures that can be decomposed under the current taxonomy has been provided, where the performance analysis of decomposed entities can be carried out independently and combined together for overall performance.

A traditional mathematical guarantee of algorithmic robustness may not translate to cyber-robustness and vice-versa. The algorithm can be made robust to missing information and measurement errors. However, the shared information could be strategically manipulated, which can be beyond the capability of the robust controller. Furthermore, the communication exchange need not be locked down via encryption; rather, they are required to be selectively encrypted with no performance deterioration. Communication technologies for voltage control would vary based on the underlying architecture, and the use of communication protocols will be limited by not only smart-grid operators but also diverse multi-owner, multi-vendor DERs and requisite interfacing with classical control devices. There is no one cyber-infrastructure that fits all solutions. Protocols have their own vulnerabilities and subtleties in mitigation of those vulnerabilities, especially from the voltage control architecture point of view is of immense significance. Notably, the applicability of DERs is not limited to voltage control, and hence each of the applications running within DER interfaces and the possible involvement of human-in-the-loop would introduce an additional set of vulnerabilities. In a similar thread, communication systems and power system automation devices participate in a multitude of other applications in addition to voltage control, questioning the possibility of independent cost-benefit analysis for voltage control.

It can be expected that this paper will help researchers with the critical information for voltage control in the presence of DERs while addressing specific challenges for successfully deploying these algorithms in terms of cyber-physical needs. From the detailed description provided, we can identify the algorithm performance for each of the sub-layers of the taxonomy and combine them to generate a metric. The discussed taxonomy would also facilitate the development of benchmark test systems encompassing all real-world subtleties, which, together with the developed metric, would unify the performance evaluation and thorough classifications of voltage control algorithms.

ACRONYMS

Acronyms used in this paper are tabulated here.

REFERENCES

[1] "Confronting the duck curve: How to address over-generation of solar energy." [Online]. Available: https://www.energy.gov/eere/articles/confronting-duck-curve-how-address-over-generation-solar-energy
[2] CAISO, "What the duck curve tells us about managing a green grid." [Online]. Available: https://www.caiso.com/Documents/FlexibleResourcesHelpRenewables_FastFacts.pdf
[3] "Breaking the duck curve." [Online]. Available: https://www.essentialenergy.com.au/media-centre/newsletter/newsletter-3-breaking-the-duck-curve
[4] D. Ranamuka, A. P. Agalgaonkar, and K. M. Muttaqi, "Examining the interactions between dg units and voltage regulating devices for effective voltage control in distribution systems," *IEEE Transactions on Industry Applications*, vol. 53, no. 2, pp. 1485–1496, 2016.
[5] T. T. Hashim, A. Mohamed, and H. Shareef, "A review on voltage control methods for active distribution networks," *Prz. Elektrotech*, vol. 88, no. 6, pp. 304–312, 2012.
[6] S. Majumder, N. Patari, A. K. Srivasava, P. Srivasava, and A. M. Annaswamy, "Epistemology of voltage control in der-rich power system," *Elec. Pow. Syst. Res.*, 2023.
[7] H. Sun, Q. Guo, J. Qi, V. Ajjarapu, R. Bravo, J. Chow, Z. Li, R. Moghe, E. Nasr-Azadani, U. Tamrakar *et al.*, "Review of challenges and research opportunities for voltage control in smart grids," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2790–2801, 2019.
[8] D. K. Molzahn, F. Dörfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.
[9] K. E. Antoniadou-Plytaria, I. N. Kouveliotis-Lysikatos, P. S. Georgilakis, and N. D. Hatziargyriou, "Distributed and decentralized voltage control of smart distribution networks: Models, methods, and future research," *IEEE Transactions on smart grid*, vol. 8, no. 6, pp. 2999–3008, 2017.
[10] X. Han, K. Heussen, O. Gehrke, H. W. Bindner, and B. Kroposki, "Taxonomy for evaluation of distributed control strategies for distributed

AAA	Authentication, Authorization, and Accounting
ACOPF	AC optimal power flow
ADMM	Alternating direction method of multipliers
ADMS	Advanced distribution management system
ADN	Active distribution network
AI	Artificial intelligence
AMI	Automatic metering interfaces
ANSI	American National Standards Institute
AVR	Automatic voltage regulator
BPS	Bulk Power System
CAMC	Central autonomous management controller
CA	Certification Authorities
CBA	Cost-Benefit Analysis
CBs	Capacitor banks
CIA	Confidentiality, Integrity, and Availability
CLs	Controllable loads
CPHS	Cyber-physical with human-in-the-loop system (CPHS)
CVRs	Conservation Voltage Reduction
DERs	Distributed energy resources
DNO	Distribution network operator
DoS	Denial of Service
DP	Dynamic programming
DSO	Distribution system operator
DSTATCOM	Distribution-STATCOMS
DVRs	Dynamic voltage restorers
ESS	Energy storage systems
ETSI	European Telecommunications Standards Institute
EVs	Electrical vehicles
FAN	Facility Area Network
FERC	Federal Energy Regulatory Commission
GA	Genetic algorithms
IAN	Industrial Area Network
IBRs	Inverter-based resources
ICT	Information and communications technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet protocol
IPS	Intrusion Prevention System
IPM	Interior point method
HAN	Home Area Network
LDC	Line drop compensation
LP	Linear programming
MGMC	Micro-grid management controller
MiTM	Man in the Middle
MILP	Mixed-integer linear programming
MINLP	Mixed-integer non-linear programming
MIQCP	Mixed-integer quadratic-constrained programming
MISOCP	Mixed integer SOCP
NAN	Neighborhood Area Networks
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation
OLTCs	On-load tap changing transformers
OpenADR	Open Automated Demand Response
OPF	Optimal Power Flow
OSCP	Open Smart Grid Protocol
P2P	Peer-to-peer
PAC-X	Proximal atomic control
PLCs	Power Line Communication
PSO	Particle Swarm Optimization
PVs	Solar photovoltaics
QP	Quadratic programming
RTUs	Remote terminal units
SCADA	Supervisory control and data acquisition
SDP	Semi-definite programming
SOCP	Second-order conical programming
SQP	sequential quadratic programming
SVCs	Static var compensators
SSTs	Solid-state transformers
TLS	Transport Layer Security
TSO	Transmission system operator
VPN	Virtual Private Network
VRs	voltage regulators
WAN	Wide Area Network
WTs	Wind turbines

energy resources," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5185–5195, 2017.

[11] N. Patari, V. Venkataramanan, A. Srivastava, D. K. Molzahn, N. Li, and A. Annaswamy, "Distributed optimization in distribution systems: Use cases, limitations, and research needs," *IEEE Transactions on Power Systems*, 2021.

[12] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivasava, "Cyber-physical vulnerability and resiliency analysis for der integration: A review, challenges and research needs," *Renewable and Sustainable Energy Reviews*, 2022.

[13] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in han, nan and wan," *Computer Networks*, vol. 67, pp. 74–88, 2014.

[14] A. Mashlakov, A. Keski-Koukkari, A. Romanenko, V. Tikka, P. Jafary, A. Supponen, J. Markkula, M. Aro, R. Abdurafikov, A. Kulmala *et al.*, "Integrated business platform of distributed energy resources–heila," 2019.

[15] A. Kargarian, J. Mohammadi, J. Guo, S. Chakrabarti, M. Barati, G. Hug, S. Kar, and R. Baldick, "Toward distributed/decentralized dc optimal power flow implementation in future electric power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2574–2594, 2016.

[16] G. Notarstefano, I. Notarnicola, and A. Camisa, "Distributed optimization for smart cyber-physical networks," *Foundations and Trends in Systems and Control*, vol. 7, no. 3, pp. 253–383, 2019.

[17] T. Yang, X. Yi, J. Wu, Y. Yuan, D. Wu, Z. Meng, Y. Hong, H. Wang, Z. Lin, and K. H. Johansson, "A survey of distributed optimization," *Annual Reviews in Control*, vol. 47, pp. 278–305, 2019.

[18] S. Howell, Y. Rezgui, J.-L. Hippolyte, B. Jayan, and H. Li, "Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources," *Renew. Sust. Energy Reviews*, vol. 77, pp. 193–214, 2017.

[19] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen, "A survey of communication/networking in smart grids," *Future generation computer systems*, vol. 28, no. 2, pp. 391–404, 2012.

[20] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[21] "American national standard for electric power systems and equipment voltage ratings (60 hz)," American National Standards Institute (ANSI), Tech. Rep., 2016.

[22] N. Hatziargyriou, J. Milanovic, C. Rahmann, V. Ajjarapu, C. Canizares, I. Erlich, D. Hill, I. Hiskens, I. Kamwa, B. Pal, P. Pourbeik, J. Sanchez-Gasca, A. Stankovic, T. Van Cutsem, V. Vittal, and C. Vournas, "Definition and classification of power system stability – revisited amp; extended," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3271–3281, 2021.

[23] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[24] P. S. Sarker, S. Majumder, M. F. Rafy, and A. K. Srivastava, "Impact analysis of cyber-events on distributed voltage control with active power curtailment," in *Power Electronics, Drives and Energy Systems (PEDES)*. IEEE, Dec. 2022.

[25] J.-H. Lee, S.-G. Jeon, D.-K. Kim, J.-S. Oh, and J.-E. Kim, "Temporary fault ride-through method in power distribution systems with distributed generations based on pcs," *Energies*, vol. 13, no. 5, 2020.

[26] C. A. McCarthy and M. J. Meisinger, "Intelligent fuse-saving," in *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, 2012, pp. 1–5.

[27] "Industrial control system," 2022. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

[28] J. de Oliveira Quevedo, F. E. Cazakevicius, R. C. Beltrame, T. B. Marchesan, L. Michels, C. Rech, and L. Schuch, "Analysis and design of an electronic on-load tap changer distribution transformer for automatic

voltage regulation," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 1, pp. 883–894, 2017.

[29] Z. Gajic, D. Karlsson, and M. Kockott, "Advanced oltc control to counteract power system voltage instability," *ABB Power Technologies, Substation Automation, SE-721*, vol. 59, 2006.

[30] C. R. Sarimuthu, V. K. Ramachandaramurthy, K. Agileswari, and H. Mokhlis, "A review on voltage control methods using on-load tap changer transformers for networks with renewable energy sources," *Renewable and Sustainable Energy Reviews*, vol. 62, pp. 1154–1161, 2016.

[31] K. M. Muttaqi, A. D. Le, M. Negnevitsky, and G. Ledwich, "A coordinated voltage control approach for coordination of oltc, voltage regulator, and dg to regulate voltage in a distribution feeder," *IEEE Transactions on Industry Applications*, vol. 51, no. 2, pp. 1239–1248, 2015.

[32] "Voltage regulators: fundamentals of power distribution voltage regulators." [Online]. Available: https://www.eaton.com/us/en-us/products/medium-voltage-power-distribution-control-systems/voltage-regulators/voltage-regulators–fundamentals-of-voltage-regulators.html

[33] K. P. Schneider and J. C. Fuller, "Voltage control devices on the ieee 8500 node test feeder," in *IEEE PES T D 2010*, 2010, pp. 1–6.

[34] C. McEntee, D. Mulcahy, J. Wang, X. Zhu, and N. Lu, "A vsm-based der dispatch minlp for volt-var control in unbalanced power distribution systems," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[35] D. Ranamuka, A. Agalgaonkar, and K. Muttaqi, "Online voltage control in distribution systems with multiple voltage regulating devices," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 2, pp. 617–628, 2013.

[36] K. Turitsyn, P. Sulc, S. Backhaus, and M. Chertkov, "Options for control of reactive power by distributed photovoltaic generators," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1063–1073, 2011.

[37] M. H. J. Bollen, R. Das, S. Djokic, P. Ciufo, J. Meyer, S. K. Rönnberg, and F. Zavodam, "Power quality concerns in implementing smart distribution-grid applications," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 391–399, 2017.

[38] IEEE, "IEEE application guide for IEEE Std 1547(tm), IEEE Standard for interconnecting distributed resources with electric power systems," *IEEE Std 1547.2-2008*, pp. 1–217, 2009.

[39] S. Li, Y. Sun, M. Ramezani, and Y. Xiao, "Artificial neural networks for volt/var control of der inverters at the grid edge," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5564–5573, 2018.

[40] "Distribution Intelligence," 2023. [Online]. Available: https://www.smartgrid.gov/the_smart_grid/distribution_intelligence.html

[41] R. Manojkumar, C. Kumar, S. Ganguly, H. B. Gooi, and S. Mekhilef, "Voltage control using smart transformer via dynamic optimal setpoints and limit tolerance in a residential distribution network with pv sources," *IET Generation, Transmission & Distribution*, vol. 14, no. 22, pp. 5143–5151, 2020.

[42] Y. Tan, C. Liao, Y. Li, Y. Cao, M. Shahidehpour, and C. Chen, "A linear power flow model for balanced distribution network with droop-controlled dstatcom and voltage controlled dg," *International Journal of Electrical Power & Energy Systems*, vol. 117, p. 105665, 2020.

[43] A. Moghassemi and S. Padmanaban, "Dynamic voltage restorer (dvr): a comprehensive review of topologies, power converters, control methods, and modified configurations," *Energies*, vol. 13, no. 16, p. 4152, 2020.

[44] S. Majumder, S. A. Khaparde, A. P. Agalgaonkar, S. Kulkarni, and S. Perera, "Graph theory based voltage sag mitigation cluster formation utilizing dynamic voltage restorers in radial distribution networks," *IEEE Transactions on Power Delivery*, 2020.

[45] "SVC for voltage control of weak subtransmission and distribution network," 2022. [Online]. Available: https://library.e.abb.com/public/15318e8bc3c4386fc1256fda003b4cfa/A02-0131E_Eldor_LR.pdf

[46] V. L. Srinivas, B. Singh, S. Mishra, and L. Xu, "Harmonic voltage control in distributed generation systems using optimal switching vector strategy," *IEEE Systems Journal*, 2021.

[47] Y. Liu, J. Li, and L. Wu, "Coordinated optimal network reconfiguration and voltage regulator/der control for unbalanced distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2912–2922, 2019.

[48] G. Qu and N. Li, "Optimal distributed feedback voltage control under limited reactive power," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 315–331, 2019.

[49] S. Majumder and S. A. Khaparde, "Revenue and ancillary benefit maximisation of multiple non-collocated wind power producers considering uncertainties," *IET Generation, Transmission & Distribution*, vol. 10, no. 3, pp. 789–797, 2016.

[50] S. Ghosh, S. Rahman, and M. Pipattanasomporn, "Local distribution voltage control by reactive power injection from pv inverters enhanced with active power curtailment," in *2014 IEEE PES General Meeting| Conference & Exposition*. IEEE, 2014, pp. 1–5.

[51] X. Zhou, J. Tian, L. Chen, and E. Dall'Anese, "Local voltage control in distribution networks: A game-theoretic perspective," in *2016 North American Power Symposium (NAPS)*. IEEE, 2016, pp. 1–6.

[52] M. Rashidi, A. Bani-Ahmed, and A. Nasiri, "Application of a multi-port solid state transformer for volt-var control in distribution systems," in *2017 IEEE Power & Energy Society General Meeting*. IEEE, 2017, pp. 1–4.

[53] R. Zafar, J. Ravishankar, and H. R. Pota, "Centralized control of step voltage regulators and energy storage system under high photovoltaic penetration," in *2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia)*. IEEE, 2016, pp. 511–516.

[54] H. Kazari, A. A.-T. Fard, A. Dobakhshari, and A. M. Ranjbar, "Voltage stability improvement through centralized reactive power management on the smart grid," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*. IEEE, 2012, pp. 1–7.

[55] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 1, pp. 96–109, 2015.

[56] S. Magnússon, G. Qu, and N. Li, "Distributed optimal voltage control with asynchronous and delayed communication," *IEEE Transactions on Smart Grid*, 2020.

[57] L. Ortmann, A. Prostejovsky, K. Heussen, and S. Bolognani, "Fully distributed peer-to-peer optimal voltage control with minimal model requirements," *Electric Power Systems Research*, vol. 189, p. 106717, 2020.

[58] H. J. Liu, W. Shi, and H. Zhu, "Hybrid voltage control in distribution networks under limited communication rates," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2416–2427, 2018.

[59] V. Calderaro, V. Galdi, G. Massa, and A. Piccolo, "Distributed generation and local voltage regulation: An approach based on sensitivity analysis," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*. IEEE, 2011, pp. 1–8.

[60] H. Ji, C. Wang, P. Li, J. Zhao, G. Song, F. Ding, and J. Wu, "A centralized-based method to determine the local voltage control strategies of distributed generator operation in active distribution networks," *Applied energy*, vol. 228, pp. 2024–2036, 2018.

[61] F. Capitanescu, I. Bilibin, and E. R. Ramos, "A comprehensive centralized approach for voltage constraints management in active distribution grid," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 933–942, 2013.

[62] G. Mokhtari, A. Ghosh, G. Nourbakhsh, and G. Ledwich, "Smart robust resources control in lv network to deal with voltage rise issue," *IEEE Transactions on Sustainable Energy*, vol. 4, no. 4, pp. 1043–1050, 2013.

[63] T. Xu and P. Taylor, "Voltage control techniques for electrical distribution networks including distributed generation," *IFAC Proceedings Volumes*, vol. 41, no. 2, pp. 11 967–11 971, 2008, 17th IFAC World Congress.

[64] A. Kharrazi and V. Sreeram, "Mitigation of voltage unbalance in distribution feeders using phase switching devices: A decentralized control approach based on local measurements," *IEEE Transactions on Power Delivery*, vol. 37, no. 4, pp. 2875–2885, 2022.

[65] B. A. Robbins and A. D. Domínguez-García, "Optimal reactive power dispatch for voltage regulation in unbalanced distribution systems," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 2903–2913, 2015.

[66] A. Cagnano and E. De Tuglie, "Centralized voltage control for distribution networks with embedded pv systems," *Renewable Energy*, vol. 76, pp. 173–185, 2015.

[67] T. Senjyu, Y. Miyazato, A. Yona, N. Urasaki, and T. Funabashi, "Optimal distribution voltage control and coordination with distributed generation," *IEEE Transactions on power delivery*, vol. 23, no. 2, pp. 1236–1242, 2008.

[68] M. Bahramipanah, R. Cherkaoui, and M. Paolone, "Decentralized voltage control of clustered active distribution network by means of energy storage systems," *Electric Power Systems Research*, vol. 136, pp. 370–382, 2016.

[69] N. Yorino, Y. Zoka, M. Watanabe, and T. Kurushima, "An optimal autonomous decentralized control method for voltage control devices

by using a multi-agent system," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2225–2233, 2014.

[70] A. Maknouninejad and Z. Qu, "Realizing unified microgrid voltage profile and loss minimization: A cooperative distributed optimization and control approach," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1621–1630, 2014.

[71] Z. Tang, D. J. Hill, and T. Liu, "Fast distributed reactive power control for voltage regulation in distribution networks," *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 802–805, 2018.

[72] S. Nowak, L. Wang, and M. S. Metcalfe, "Two-level centralized and local voltage control in distribution systems mitigating effects of highly intermittent renewable generation," *International Journal of Electrical Power & Energy Systems*, vol. 119, p. 105858, 2020.

[73] T. Ding, C. Li, Y. Yang, J. Jiang, Z. Bie, and F. Blaabjerg, "A two-stage robust optimization for centralized-optimal dispatch of photovoltaic inverters in active distribution networks," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 2, pp. 744–754, 2016.

[74] Z. Shen and M. E. Baran, "Gradient based centralized optimal volt/var control strategy for smart distribution system," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2013, pp. 1–6.

[75] Y. Li, Y. Feng, H. Zhang, Y. Cao, and C. Rehtanz, "An adaptive zone-division approach for voltage control of power grid with distributed wind farms: A case study of a regional power grid in central south china," *International Journal of Electrical Power & Energy Systems*, vol. 103, pp. 652–659, 2018.

[76] J. Ding, Q. Zhang, S. Hu, Q. Wang, and Q. Ye, "Clusters partition and zonal voltage regulation for distribution networks with high penetration of pvs," *IET Generation, Transmission & Distribution*, vol. 12, no. 22, pp. 6041–6051, 2018.

[77] K. Utkarsh, A. Trivedi, D. Srinivasan, and T. Reindl, "A consensus-based distributed computational intelligence technique for real-time optimal control in smart distribution grids," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 1, pp. 51–60, 2016.

[78] B. Zhang, A. Y. Lam, A. D. Domínguez-García, and D. Tse, "An optimal and distributed method for voltage regulation in power distribution systems," *IEEE Transactions on Power Systems*, vol. 30, no. 4, pp. 1714–1726, 2014.

[79] S. Bolognani, R. Carli, G. Cavraro, and S. Zampieri, "Distributed reactive power feedback control for voltage regulation and loss minimization," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 966–981, 2014.

[80] E. Dall'Anese, H. Zhu, and G. B. Giannakis, "Distributed optimal power flow for smart microgrids," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1464–1475, 2013.

[81] B. A. Robbins, H. Zhu, and A. D. Domínguez-García, "Optimal tap setting of voltage regulation transformers in unbalanced distribution systems," *IEEE Transactions on Power Systems*, vol. 31, no. 1, pp. 256–267, 2015.

[82] Q. Zhang, K. Dehghanpour, and Z. Wang, "Distributed cvr in unbalanced distribution systems with pv penetration," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5308–5319, 2019.

[83] S. Kawano, S. Yoshizawa, and Y. Hayashi, "Centralized voltage control method using voltage forecasting by jit modeling in distribution networks," in *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*, 2016, pp. 1–5.

[84] A. Singhal, V. Ajjarapu, J. Fuller, and J. Hansen, "Real-time local volt/var control under external disturbances with high pv penetration," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3849–3859, 2018.

[85] J. Zhao, Y. Li, P. Li, C. Wang, H. Ji, L. Ge, and Y. Song, "Local voltage control strategy of active distribution network with pv reactive power optimization," in *2017 IEEE Power & Energy Society General Meeting*. IEEE, 2017, pp. 1–5.

[86] M. Farivar, L. Chen, and S. Low, "Equilibrium and dynamics of local voltage control in distribution systems," in *52nd IEEE Conference on Decision and Control*. IEEE, 2013, pp. 4329–4334.

[87] X. Zhou, M. Farivar, and L. Chen, "Pseudo-gradient based local voltage control in distribution networks," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2015, pp. 173–180.

[88] P. Li, J. Ji, H. Ji, J. Jian, F. Ding, J. Wu, and C. Wang, "Mpc-based local voltage control strategy of dgs in active distribution networks," *IEEE Transactions on Sustainable Energy*, 2020.

[89] J. Lai, H. Zhou, X. Lu, X. Yu, and W. Hu, "Droop-based distributed cooperative control for microgrids with time-varying delays," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1775–1789, 2016.

[90] V. Nasirian, Q. Shafiee, J. M. Guerrero, F. L. Lewis, and A. Davoudi, "Droop-free distributed control for ac microgrids," *IEEE Transactions on Power Electronics*, vol. 31, no. 2, pp. 1600–1617, 2015.

[91] M. Buchanan, "Non-optimal optimization," *Nature Physics*, vol. 11, no. 12, pp. 984–984, 2015.

[92] T. Woolf, B. Havumaki, D. Bhandari, M. Whited, and L. C. Schwartz, "Benefit-cost analysis for utility-facing grid modernization investments: Trends, challenges, and considerations," Lawrence Berkeley National Lab.(LBNL), Berkeley, CA (United States), Tech. Rep., 2021.

[93] F. C. Schweppe and S. K. Mitter, "Hierarchical system theory and electric power systems," in *Proceedings Symposium on Real Time Control of Electric Power Systems*. Elsevier Publishing Company, 1972, pp. 259–277.

[94] D. K. Molzahn and I. A. Hiskens, "A survey of relaxations and approximations of the power flow equations," *Foundations and Trends in Electric Energy Systems*, vol. 4, no. 1-2, pp. 1–221, 2019. [Online]. Available: http://dx.doi.org/10.1561/3100000012

[95] S. Chanda, F. Shariatzadeh, A. Srivastava, E. Lee, W. Stone, and J. Ham, "Implementation of non-intrusive energy saving estimation for volt/var control of smart distribution system," *Electric Power Systems Research*, vol. 120, pp. 39–46, 2015.

[96] M. E. Elkhatib, R. El-Shatshat, and M. M. A. Salama, "Novel coordinated voltage control for smart distribution networks with dg," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 598–605, 2011.

[97] F. Olivier, P. Aristidou, D. Ernst, and T. Van Cutsem, "Active management of low-voltage networks for mitigating overvoltages due to photovoltaic units," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 926–936, 2015.

[98] A. Abessi, V. Vahidinasab, and M. S. Ghazizadeh, "Centralized support distributed voltage control by using end-users as reactive power support," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 178–188, 2015.

[99] B. Zhao, Z. Xu, C. Xu, C. Wang, and F. Lin, "Network partition-based zonal voltage control for distribution networks with distributed pv systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4087–4098, 2017.

[100] M. Nayeripour, H. Fallahzadeh-Abarghouei, E. Waffenschmidt, and S. Hasanvand, "Coordinated online voltage management of distributed generation using network partitioning," *Electric Power Systems Research*, vol. 141, pp. 202–209, 2016.

[101] P. Li, C. Zhang, X. Fu, G. Song, C. Wang, and J. Wu, "Determination of local voltage control strategy of distributed generators in active distribution networks based on kriging metamodel," *IEEE Access*, vol. 7, pp. 34 438–34 450, 2019.

[102] Y. Shi, G. Qu, S. Low, A. Anandkumar, and A. Wierman, "Stability constrained reinforcement learning for real-time voltage control," *arXiv preprint arXiv:2109.14854*, 2021.

[103] J.-F. Toubeau, B. Bakhshideh Zad, M. Hupez, Z. De Grève, and F. Vallée, "Deep reinforcement learning-based voltage control to deal with model uncertainties in distribution networks," *Energies*, vol. 13, no. 15, p. 3928, 2020.

[104] M. Tan, C. Han, X. Zhang, L. Guo, and T. Yu, "Hierarchically correlated equilibrium q-learning for multi-area decentralized collaborative reactive power optimization," *CSEE Journal of Power and Energy Systems*, vol. 2, no. 3, pp. 65–72, 2016.

[105] D. S. Stock, A. Venzke, T. Hennig, and L. Hofmann, "Model predictive control for reactive power management in transmission connected distribution grids," in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. IEEE, 2016, pp. 419–423.

[106] M. M. Begovic, *Electrical transmission systems and smart grids: selected entries from the Encyclopedia of sustainability science and technology*. Springer Science & Business Media, 2012.

[107] Z. Li, Q. Guo, H. Sun, and J. Wang, "Impact of coupled transmission-distribution on static voltage stability assessment," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3311–3312, 2016.

[108] N. Pilatte, P. Aristidou, and G. Hug, "Tdnetgen: An open-source, parametrizable, large-scale, transmission, and distribution test system," *IEEE Systems Journal*, vol. 13, no. 1, pp. 729–737, 2017.

[109] B. Palmintier, E. Hale, T. M. Hansen, W. Jones, D. Biagioni, H. Sorensen, H. Wu, and B.-M. Hodge, "Igms: An integrated iso-to-appliance scale grid modeling system," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1525–1534, 2016.

[110] M. Geidl, "Implementation of coordinated voltage control for the swiss transmission system," in *Melecon 2010-2010 15th IEEE Mediterranean Electrotechnical Conference*. IEEE, 2010, pp. 230–236.

[111] H. Barth, D. Hidalgo, A. Pohlemann, M. Braun, L. H. Hansen, and H. Knudsen, "Technical and economical assessment of reactive power provision from distributed generators: Case study area of east denmark," in *2013 IEEE Grenoble Conference*. IEEE, 2013, pp. 1–6.

[112] C. G. Kaloudas, L. F. Ochoa, B. Marshall, S. Majithia, and I. Fletcher, "Assessing the future trends of reactive power demand of distribution networks," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4278–4288, 2017.

[113] P. Aristidou, G. Valverde, and T. Van Cutsem, "Contribution of distribution network control to voltage stability: A case study," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 106–116, 2015.

[114] M. Farrokhabadi, C. A. Cañizares, J. W. Simpson-Porco, E. Nasr, L. Fan, P. A. Mendoza-Araya, R. Tonkoski, U. Tamrakar, N. Hatziargyriou, D. Lagos, R. W. Wies, M. Paolone, M. Liserre, L. Meegahapola, M. Kabalan, A. H. Hajimiragha, D. Peralta, M. A. Elizondo, K. P. Schneider, F. K. Tuffner, and J. Reilly, "Microgrid stability definitions, analysis, and examples," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 13–29, 2020.

[115] A. Adib, B. Mirafzal, X. Wang, and F. Blaabjerg, "On stability of voltage source inverters in weak grids," *IEEE Access*, vol. 6, pp. 4427–4439, 2018.

[116] G. Kandaperumal, S. Majumder, and A. K. Srivastava, "Microgrids as a resilience resource in the electric distribution grid," in *Electric Power Systems Resiliency*. Elsevier, 2022, pp. 181–212.

[117] K. R. Padiyar and A. M. Kulkarni, *Dynamics and control of electric transmission and microgrids*. John Wiley & Sons, 2019.

[118] S. Weckx and J. Driesen, "Optimal local reactive power control by pv inverters," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 4, pp. 1624–1633, 2016.

[119] X. Zhou, M. Farivar, Z. Liu, L. Chen, and S. Low, "Reverse and forward engineering of local voltage control in distribution networks," *IEEE Transactions on Automatic Control*, 2020.

[120] H. Zhu and H. J. Liu, "Fast local voltage control under limited reactive power: Optimality and stability analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3794–3803, 2015.

[121] H. S. Bidgoli and T. Van Cutsem, "Combined local and centralized voltage control in active distribution networks," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1374–1384, 2017.

[122] W. Haokun, L. Jian, Z. Shiqiang, and L. Yifan, "Strategies and properties of local control for distributed generation," in *2016 China International Conference on Electricity Distribution (CICED)*. IEEE, 2016, pp. 1–5.

[123] S. M. Mirbagheri and M. Merlo, "Optimal reactive power flow procedure to set up an effective local voltage control," *Sustainable Energy Technologies and Assessments*, vol. 39, p. 100709, 2020.

[124] C. Zhang and Y. Xu, "Hierarchically-coordinated voltage/var control of distribution networks using pv inverters," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 2942–2953, 2020.

[125] C. Ahn and H. Peng, "Decentralized voltage control to minimize distribution power loss of microgrids," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1297–1304, 2013.

[126] P. Cuffe and A. Keane, "Voltage responsive distribution networks: Comparing autonomous and centralized solutions," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2234–2242, 2014.

[127] H. Amiri, G. A. Markadeh, N. M. Dehkordi, and F. Blaabjerg, "Fully decentralized robust backstepping voltage control of photovoltaic systems for dc islanded microgrids based on disturbance observer method," *ISA transactions*, vol. 101, pp. 471–481, 2020.

[128] G. Valverde and T. Van Cutsem, "Model predictive control of voltages in active distribution networks," *IEEE Transactions on Smart Grid*, vol. 4, no. 4, pp. 2152–2161, 2013.

[129] D. E. Olivares, C. A. Cañizares, and M. Kazerani, "A centralized energy management system for isolated microgrids," *IEEE Transactions on smart grid*, vol. 5, no. 4, pp. 1864–1875, 2014.

[130] K. Christakou, D. Tomozei, J. Le Boudec, and M. Paolone, "Gecn: Primary voltage control for active distribution networks via real-time demand-response," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 622–631, 2014.

[131] M. Farivar, R. Neal, C. Clarke, and S. Low, "Optimal inverter var control in distribution systems with high pv penetration," in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–7.

[132] Y. Xu, Z. Y. Dong, R. Zhang, and D. J. Hill, "Multi-timescale coordinated voltage/var control of high renewable-penetrated distribution systems," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4398–4408, 2017.

[133] M. R. Islam, H. Lu, J. Hossain, and L. Li, "Multiobjective optimization technique for mitigating unbalance and improving voltage considering higher penetration of electric vehicles and distributed generation," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3676–3686, 2020.

[134] L. Yu, D. Czarkowski, and F. de Leon, "Optimal distributed voltage regulation for secondary networks with dgs," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 959–967, 2012.

[135] A. R. Di Fazio, G. Fusco, and M. Russo, "Decentralized control of distributed generation for voltage profile optimization in smart feeders," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1586–1596, 2013.

[136] S. Bolognani and S. Zampieri, "A distributed control strategy for reactive power compensation in smart microgrids," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2818–2833, 2013.

[137] S. Weckx, R. D'Hulst, B. Claessens, and J. Driesensam, "Multiagent charging of electric vehicles respecting distribution transformer loading and voltage limits," *IEEE Transactions on Smart Grid*, vol. 5, no. 6, pp. 2857–2867, 2014.

[138] Y. Liu, L. Guo, C. Lu, Y. Chai, S. Gao, and B. Xu, "A fully distributed voltage optimization method for distribution networks considering integer constraints of step voltage regulators," *IEEE Access*, vol. 7, pp. 60 055–60 066, 2019.

[139] A. Bedawy, N. Yorino, K. Mahmoud, and M. Lehtonen, "An effective coordination strategy for voltage regulation in distribution system containing high intermittent photovoltaic penetrations," *IEEE Access*, vol. 9, pp. 117 404–117 414, 2021.

[140] L. Wang, A. Dubey, A. H. Gebremedhin, A. Srivastava, and N. Schulz, "Mpc-based decentralized voltage control in power distribution systems with ev and pv coordination," *IEEE Transactions on Smart Grid*, 2022.

[141] Y. Guo, Q. Wu, H. Gao, X. Chen, J. Østergaard, and H. Xin, "Mpc-based coordinated voltage regulation for distribution networks with distributed generation and energy storage system," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 4, pp. 1731–1739, 2018.

[142] P. Pachanapan, O. Anaya-Lara, A. Dysko, and K. L. Lo, "Adaptive zone identification for voltage level control in distribution networks with dg," *IEEE Transactions on smart grid*, vol. 3, no. 4, pp. 1594–1602, 2012.

[143] X. Zhang, A. J. Flueck, and C. P. Nguyen, "Agent-based distributed volt/var control with distributed power flow solver in smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 600–607, 2015.

[144] Y. Zoka, N. Yorino, M. Watanabe, and T. Kurushima, "An optimal decentralized control for voltage control devices by means of a multi-agent system," in *2014 Power Systems Computation Conference*. IEEE, 2014, pp. 1–8.

[145] H. Xin, Y. Liu, Z. Qu, and D. Gan, "Distributed control and generation estimation method for integrating high-density photovoltaic systems," *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, pp. 988–996, 2014.

[146] B. A. Robbins, C. N. Hadjicostis, and A. D. Domínguez-García, "A two-stage distributed architecture for voltage control in power distribution systems," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1470–1482, 2012.

[147] V. Loia, A. Vaccaro, and K. Vaisakh, "A self-organizing architecture based on cooperative fuzzy agents for smart grid voltage control," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1415–1422, 2013.

[148] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, 2014.

[149] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3462–3470, 2013.

[150] A. Bidram, A. Davoudi, F. L. Lewis, and S. S. Ge, "Distributed adaptive voltage control of inverter-based microgrids," *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, pp. 862–872, 2014.

[151] Y. Zhang, M. Hong, E. Dall'Anese, S. V. Dhople, and Z. Xu, "Distributed controllers seeking ac optimal power flow solutions using admm," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4525–4537, 2017.

[152] S. Mahdavi, H. Panamtash, A. Dimitrovski, and Q. Zhou, "Predictive coordinated and cooperative voltage control for systems with high pene-

tration of pv," *IEEE Transactions on Industry Applications*, vol. 57, no. 3, pp. 2212–2222, 2021.

[153] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "A consensus-based distributed voltage control for reactive power sharing in microgrids," in *2014 European Control Conference (ECC)*. IEEE, 2014, pp. 1299–1305.

[154] G. Cavraro and R. Carli, "Local and distributed voltage control algorithms in distribution networks," pp. 1420–1430, 2017.

[155] E. Dall'Anese and A. Simonetto, "Optimal power flow pursuit," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 942–952, 2016.

[156] Q. Li, Y. Zhang, T. Ji, X. Lin, and Z. Cai, "Volt/var control for power grids with connections of large-scale wind farms: A review," *IEEE Access*, vol. 6, pp. 26 675–26 692, 2018.

[157] N. Patari, A. K. Srivastava, G. Qu, and N. Li, "Distributed voltage control for three-phase unbalanced distribution systems with ders and practical constraints," *IEEE Transactions on Industry Applications*, vol. 57, no. 6, pp. 6622–6633, 2021.

[158] P. S. Sarker, N. Patari, B. Ha, S. Majumder, and A. K. Srivastava, "Cyber-power testbed for analyzing distributed control performance during cyber-events," in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Apr. 2022, pp. 1–6.

[159] X. Hu, Z.-W. Liu, G. Wen, X. Yu, and C. Liu, "Voltage control for distribution networks via coordinated regulation of active and reactive power of dgs," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4017–4031, 2020.

[160] M. Tahir, M. E. Nassar, R. El-Shatshat, and M. Salama, "A review of volt/var control techniques in passive and active power distribution networks," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*. IEEE, 2016, pp. 57–63.

[161] Y. Wang, K. Tan, X. Y. Peng, and P. L. So, "Coordinated control of distributed energy-storage systems for voltage regulation in distribution networks," *IEEE transactions on power delivery*, vol. 31, no. 3, pp. 1132–1141, 2015.

[162] L. Bakule, "Decentralized control: An overview," *Annual reviews in control*, vol. 32, no. 1, pp. 87–98, 2008.

[163] G. Cavraro, S. Bolognani, R. Carli, and S. Zampieri, "The value of communication in the voltage regulation problem," in *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 5781–5786.

[164] J. Adan, S. Majumder, and A. K. Srivastava, "Distributed optimization approaches with discrete variables in the power distribution systems," in *North American Power Symposium (NAPS)*. IEEE, Oct. 2022.

[165] J. Cartwright, "Europe's power grids readied against cyber attack," 2015. [Online]. Available: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/europes-power-grids-readied-against-cyber-attack

[166] M. Assante, "Confirmation of a coordinated attack on the ukrainian power grid," 2016.

[167] "Lesson learned risks posed by firewall firmware vulnerabilities," 2019. [Online]. Available: https://legacy-assets.eenews.net/open_files/assets/2019/09/06/document_ew_02.pdf

[168] V. Bergengruen, "'is there something more sinister going on?' authorities fear extremists are targeting u.s. power grid," 2023. [Online]. Available: https://time.com/6244977/us-power-grid-attacks-extremism/

[169] S. Majumder and A. Srivastava, "Resilience-driven integration of distributed energy resource (der): Holistic value analysis," *IEEE Smart Grid eBulletin*, Sep. 2022.

[170] V. Tikka, A. Mashlakov, A. Kulmala, S. Repo, M. Aro, A. Keski-Koukkari, S. Honkapuro, P. Järventausta, and J. Partanen, "Integrated business platform of distributed energy resources – case finland," *Energy Procedia*, vol. 158, pp. 6637–6644, 2019, innovative Solutions for Energy Transitions.

[171] CISCO, *Internet protocol architecture for the Smart Grid*, 2022. [Online]. Available: http://assets.fiercemarkets.net/public/smartgridnews/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf

[172] S. Ahmed, T. M. Gondal, M. Adil, S. A. Malik, and R. Qureshi, "A survey on communication technologies in smart grid," in *2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, 2019, pp. 7–12.

[173] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *IEEE PES general meeting*. IEEE, 2010, pp. 1–7.

[174] R. Ma, S. Chen, H.-H. Chen, and W. Meng, "Coexistence of smart utility networks and wlans in smart grid systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8313–8324, 2016.

[175] D. K. Sharma, G. K. Rapaka, A. P. Pasupulla, S. Jaiswal, K. Abadar, and H. Kaur, "A review on smart grid telecommunication system," *Materials Today: Proceedings*, vol. 51, pp. 470–474, 2022.

[176] F. Aalamifar and L. Lampe, "Optimized wimax profile configuration for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2723–2732, 2016.

[177] M. Ibrahim and M. M. Salama, "Smart distribution system volt/var control using distributed intelligence and wireless communication," *IET generation, transmission & distribution*, vol. 9, no. 4, pp. 307–318, 2015.

[178] E. Kabalcı, Y. Kabalcı, and P. Siano, "Design and implementation of a smart metering infrastructure for low voltage microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107375, 2022.

[179] E. Hossain, Z. Han, and H. V. Poor, "Communication architectures and models for smart grid," *Smart Grid Communications and Networking; Hossain, E., Han, Z., Poor, HV, Eds*, pp. 1–103, 2012.

[180] Aberdeen Cyber Security, "Wired vs wireless networking." [Online]. Available: https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking/

[181] "Cisa, securing wireless networks." [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST05-003

[182] 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.*, 2017.

[183] "Etsi approves open smart grid protocol (osgp) for grid technologies." [Online]. Available: https://www.etsi.org/newsroom/news/382-news-release-18-january-2012

[184] H. G. Aghamolki, Z. Miao, and L. Fan, "A hardware-in-the-loop scada testbed," in *2015 North American Power Symposium (NAPS)*, 2015, pp. 1–6.

[185] T. Basso, "IEEE 1547 and 2030 standards for distributed energy resources interconnection and interoperability with the electricity grid," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2014.

[186] F. Leccese, "An overwiev on IEEE Std 2030," in *2012 11th International Conference on Environment and Electrical Engineering*. IEEE, 2012, pp. 340–345.

[187] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller, "Cyber-physical security and resiliency analysis testbed for critical microgrids with ieee 2030.5," in *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020, pp. 1–6.

[188] A. S. Soliman, A. A. Saad, and O. Mohammed, "Securing networked microgrids operation through dnp3 protocol implementation," in *2021 IEEE Industry Applications Society Annual Meeting (IAS)*, 2021, pp. 1–6.

[189] Q. Nguyen, J. Ogle, X. Fan, X. Ke, M. R. Vallem, N. Samaan, and N. Lu, "Ems and dms integration of the coordinative real-time sub-transmission volt-var control tool under high der penetration," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*, 2021, pp. 01–05.

[190] IEEE, "IEEE standard for electric power systems communications-distributed network protocol (DNP3) - redline," *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010) - Redline*, pp. 1–821, 2012.

[191] H. M. Mustafa, M. Bariya, K. Sajan, A. Chhokra, A. Srivastava, A. Dubey, A. von Meier, and G. Biswas, "RT-METER: A real-time, multi-layer cyber-power testbed for resiliency analysis," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2021, pp. 1–7.

[192] F. Cleveland, "IEC 61850-7-420 communications standard for distributed energy resources (DER)," in *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, 2008, pp. 1–4.

[193] D. Yadav, "Application of IEC 61850 standard to the integration of der with the electricity network," in *CIRED 2020 Berlin Workshop (CIRED 2020)*, vol. 2020. IET, 2020, pp. 696–698.

[194] W. D. Pieters, "Monitoring, protection, and voltage control of parallel power transformers based on IEC 61850-9-2 process bus," Ph.D. dissertation, Cape Peninsula University of Technology, 2019.

[195] Z. Zhu, B. Xu, C. Brunner, T. Yip, and Y. Chen, "IEC 61850 configuration solution to distributed intelligence in distribution grid automation," *Energies*, vol. 10, no. 4, p. 528, 2017.

[196] X. Liu, A. Aichhorn, L. Liu, and H. Li, "Coordinated control of distributed energy storage system with tap changer transformers for voltage

rise mitigation under high photovoltaic penetration," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 897–906, 2012.

[197] W. Buchanan, "18 - modbus," in *Computer Busses*, W. Buchanan, Ed. Oxford: Butterworth-Heinemann, 2000, pp. 301–312.

[198] J. Ferreira, H. Martins, M. Barata, V. Monteiro, and J. L. Afonso, "Openadr—intelligent electrical energy consumption towards internet-of-things," in *CONTROLO 2016*. Springer, 2017, pp. 725–736.

[199] M. Kolenc, N. Ihle, C. Gutschi, P. Nemček, T. Breitkreuz, K. Goedderz, N. Suljanović, and M. Zajc, "Virtual power plant architecture using openadr 2.0 b for dynamic charging of automated guided vehicles," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 370–382, 2019.

[200] C. McParland, "Openadr open source toolkit: Developing open source software for the smart grid," in *2011 IEEE Power and Energy Society General Meeting*. IEEE, 2011, pp. 1–7.

[201] W. Stallings, "Data and computer communications," *Prentice Hall*, 2005.

[202] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki, "A multidimensional holistic framework for the security of distributed energy and control systems," *IEEE Systems Journal*, 2019.

[203] I. Onunkwo, B. Wright, P. Cordeiro, N. Jacobs, C. Lai, J. Johnson, T. Hutchins, W. Stout, A. Chavez, B. T. Richardson *et al.*, "Cybersecurity assessments on emulated DER communication networks," Sandia National Laboratories, Tech. Rep., 2018.

[204] R. Siqueira de Carvalho, "Integrating big data analytics and cybersecurity for power distribution networks with distributed energy resources," Ph.D. dissertation, Colorado School of Mines. Arthur Lakes Library, 2019.

[205] R. Siqueira de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2020.

[206] 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.

[207] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156 044–156 053, 2019.

[208] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources," in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*. IEEE, 2017, pp. 2135–2140.

[209] A. Veichtlbauer, O. Langthaler, D. Engel, C. Kasberger, F. P. Andrén, and T. Strasser, "Towards applied security-by-design for DER units," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2016, pp. 1–4.

[210] E. Ibrahim, "Disruptive ideas for power grid security and resilience with DER," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2017.

[211] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of system and interoperability impact from securing communications for distributed energy resources," in *2019 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2019, pp. 1–8.

[212] V. Y. Pillitteri and T. L. Brewer, "Guidelines for smart grid cybersecurity," Tech. Rep., 2014.

[213] K. A. Horowitz, Z. Peterson, M. H. Coddington, F. Ding, B. O. Sigrin, D. Saleem, S. E. Baldwin, B. Lydic, S. C. Stanfield, N. Enbar *et al.*, "An overview of distributed energy resource (DER) interconnection: Current practices and emerging solutions," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.

[214] S. Fries, "Security in power system automation status and application of IEC 62351 - an introduction," 06 2017.

[215] D. Meyer and F. Baker, "Internet protocols for the smart grid," in *IETF*, 2011.

[216] J. Stevens, "Electricity subsector cybersecurity capability maturity model (es-c2m2)(case study)," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, Tech. Rep., 2014.

[217] D. Saleem and J. Johnson, "Distributed energy resource (der) cybersecurity standards," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2017.

[218] M. M. S. Khan, A. Palomino, J. Brugman, J. Giraldo, S. K. Kasera, and M. Parvania, "The cyberphysical power system resilience testbed: Architecture and applications," *Computer*, vol. 53, no. 5, pp. 44–54, 2020.

[219] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, "A control system testbed to validate critical infrastructure protection concepts," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 88–103, 2011.

[220] Á. Silos, A. Señís, R. M. De Pozuelo, and A. Zaballos, "Using IEC 61850 goose service for adaptive ansi 67/67n protection in ring main systems with distributed energy resources," *Energies*, vol. 10, no. 11, p. 1685, 2017.

[221] W. Wimmer, "Determining vlan-ids for a switched-based communication network of a process control system," Apr. 28 2015, uS Patent 9,021,067.

[222] A. B. Pedersen, E. B. Hauksson, P. B. Andersen, B. Poulsen, C. Træholt, and D. Gantenbein, "Facilitating a generic communication interface to distributed energy resources: Mapping IEC 61850 to restful services," in *2010 First IEEE international conference on smart grid communications*. IEEE, 2010, pp. 61–66.

[223] J.-Y. Joo, E. Stewart, B. Salazar, and N. Yee, "Selection of ten (10) cybersecurity scenarios for project cybersecure interconnection of distributed energy resources," Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), Tech. Rep., 2018.

[224] C. Carter, P. G. Cordeiro, I. Onunkwo, and J. T. Johnson, "Cyber assessment of distributed energy resources." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2018.

[225] J. T. Johnson, "Pv cybersecurity final report." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2019.

[226] C. Powell, K. Hauck, A. D. Sanghvi, and T. L. Reynolds, "Distributed energy resource cybersecurity framework best practices," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2020.

[227] J. Schmutzler, S. Gröning, and C. Wietfeld, "Management of distributed energy resources in IEC 61850 using web services on devices," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011, pp. 315–320.

[228] V. Venkataramanan, A. Hahn, and A. Srivastava, "Cp-sam: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1055–1065, 2020.

[229] V. Venkataramanan, A. K. Srivastava, A. Hahn, and S. Zonouz, "Measuring and enhancing microgrid resiliency against cyber threats," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 6303–6312, 2019.

[230] V. Venkataramanan, A. Hahn, and A. Srivastava, "Cyphyr: a cyber-physical analysis tool for measuring and enabling resiliency in microgrids," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 4, pp. 313–321, 2019.

[231] "Nerc : Standards, compliance, and enforcement bulletins," 2023. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/default.aspx

[232] "MITRE ATT&CK Navigator," 2023. [Online]. Available: https://mitre-attack.github.io/attack-navigator/

[233] "NIST: Cybersecurity Framework," 2023. [Online]. Available: https://www.nist.gov/cyberframework

[234] V. Menghani. (2018, Mar.) Cyber security in power system. http://erpc.gov.in/wp-content/uploads/2018/03/ERPC_Cyber-Security-in-Power-system_presentation.pdf.

[235] D. J. Sebastian-Cardenas, H. M. Mustafa, A. Hahn, and A. Srivastava, "Grid-vids: A smart grid co-simulation platform for virtual device simulation," in *2022 Resilience Week (RWS)*, 2022, pp. 1–6.

[236] Z. Hu and F. Li, "Cost-benefit analyses of active distribution network management, part i: Annual benefit analysis," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1067–1074, 2012.

[237] ——, "Cost-benefit analyses of active distribution network management, part ii: investment reduction analysis," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1075–1081, 2012.

[238] B. Idlbi, K. Diwold, T. Stetz, H. Wang, and M. Braun, "Cost-benefit analysis of central and local voltage control provided by distributed generators in mv networks," in *2013 IEEE Grenoble Conference*. IEEE, 2013, pp. 1–6.

[239] T. Stetz, K. Diwold, M. Kraiczy, D. Geibel, S. Schmidt, and M. Braun, "Techno-economic assessment of voltage control strategies in low voltage grids," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 2125–2132, 2014.

[240] M. Lehtonen and S. Kupari, "A method for cost benefit analysis of distribution automation," in *Proceedings 1995 International Conference on Energy Management and Power Delivery EMPD'95*, vol. 1. IEEE, 1995, pp. 49–54.

[241] A. M. Belay, S. Puranik, R. Gallart-Fernández, H. Tuiskula, J. Melendez, I. Lamprinos, F. Díaz-González, and M. Smolnikar, "Developing novel technologies and services for intelligent low voltage electricity grids:

Cost–benefit analysis and policy implications," *Energies*, vol. 15, no. 1, p. 94, 2021.
[242] D. DSPx, "Modern distribution grid report volume i: Customer and state policy driven functionality," *Washington, DC*, 2017.

SUBIR MAJUMDER (S'17–M'21) received the Ph.D. degree under a Cotutelle/Joint Agreement between Indian Institute of Technology Bombay, India and the University of Wollongong, Australia in 2020.

From 2020 to 2021, he worked as a post-doctoral research associate at Washington State University, Pullman, WA, USA. Subsequently, he worked as an Engineering Scientist at the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV, USA, from 2021 to 2023. Currently, he is working as a TEES Senior Research Engineer I at the Department of Electrical & Computer Engineering, Texas A&M University, College Station, TX, USA. He was conferred POSOCO Power System Awards (PPSA) under the Doctoral category in 2020. His research interests include power systems modeling, operations (including operational resiliency) and planning, power system economics, distributed optimization, power quality, and the smart grid.

AMIRKHOSRO VOSUGHI (M'21) received a bachelor's degree in electrical engineering from AmirKabir University of Technology (AUT), in Iran, in 2009, and Master of Control System from Iran University of Science and Technology (IUST), Iran, in 2011, and the Ph.D. degree in System Engineering from the Electrical and Computer Science Engineering Dept, Washington State University (WSU), Pullman, WA., in 2020.

From 2020 to 2021, he was a Postdoctoral Researcher at Washington State University, Pullman, WA, USA. He is currently an R&D Engineer with OpenEye. His research interest includes control and estimation systems, data science, and machine learning algorithms.

HUSSAIN M MUSTAFA (M'21) received his bachelor's degree in Applied Physics from the University of Dhaka, Bangladesh in 2014, and master degree in Computer Science from Washington State University in 2021. He is currently working towards a Ph.D. degree in Computer Science from West Virginia University, Morgantown, WV.

He previously worked as a Data Communication & Security engineer in Huawei Technologies Co. Ltd., designing and implementing secured network topologies for telecommunication networks. He is CISCO Certified Network Associate in Routing & Switching, and Security. His research interests include cyber security and cyber resiliency of the Smart Grid, the development of real-time multi-vendor Hardware-In-The-Loop test-beds for application validation, and cyber security use cases.

TORI E. WARNER (M'21) received the bachelor's degree in electrical engineering from Washington State University, in 2021.

She is currently working as a Design Engineer – I with Electrical Consultants, Inc., Salt Lake City, Utah, United States.

ANURAG K. SRIVASTAVA (F'22) received the Ph.D. degree in power engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2005.

He is a Raymond J. Lane Professor and Chairperson with the Computer Science and Electrical Engineering Department West Virginia University. He is also an Adjunct Professor with the Washington State University and Senior Scientist with the Pacific Northwest National Lab. He is an Author of more than 300 technical publications, including a book on power system security and four patents. His research interest includes data-driven algorithms for power system operation and control, including resiliency analysis.

Prof. Srivastava is serving as Chair of PES voltage stability working group, and Vice-Chair of power system operation sub-committee, and Vice-Chair of tools for power grid resilience task force.