Preprint of the manuscript.
Full text available at: https://www.sciencedirect.com/science/article/pii/S1364032122006785
Cite as: A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs," Renew. Sust. Energ. Rev., vol. 168, Art. no. 112794, 2022.

Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs☆

Amirkhosro Vosughi [a], Ali Tamimi [b], Alexandra Beatrice King [c], Subir Majumder [d], Anurag K. Srivastava [d,c,*]

[a] OpenEye, Spokane, WA, United States of America
[b] Amazon Web Service, Seattle, WA, United States of America
[c] Washington State University, Pullman, WA, United States of America
[d] West Virginia University, Morgantown, WV, 26505, United States of America

ARTICLE INFO

Keywords:
DER functionalities
Control architecture
Standard communication protocols for DERs
Cyber vulnerability
Security defense and mitigation
Resiliency

ABSTRACT

High penetration of renewable and sustainable Distributed Energy Resources (DER) into the traditional distribution system requires a well-coordinated control strategy for the improvement of system-wide reliability and resiliency. Implementation of such a holistic control architecture requires a flexible, near real-time, and bi-directional communication framework for facilitating the participation of various agents in a multi-vendor heterogeneous smart grid. While the sustainability of energy generation is ensured, this exposes the smart grid to extrinsic cyber threats, and appropriate defense mechanism(s) must be deployed to guarantee continued reliability and resiliency of the power grid. The comprehensive literature review presented in this paper discusses the latest trends in the DER control schemes with fast communication requirements and their accompanying cyber–physical vulnerabilities. These control schemes are compared and contrasted for various traits. A three-level DER system architecture has been depicted, facilitating the deployment of these control schemes. The current developments of standard communication protocols, key security mechanisms, and best practices along major standards and guidelines are explored. The impacts of different attack types with miscellaneous DER functions based on various control schemes and associated mitigation solutions are also provided. Finally, challenges and future research directions for limiting cyber-power susceptibility to enhance resiliency are summarized. The work presented here will help us enabling a cyber-resilient and sustainable smart electric grid.

1. Introduction

Rapid increase in the penetration of renewable distributed energy resources (DERs) in the distribution network around the globe creates a paradigm shift in the traditional generation and electricity consumption. DERs include most of the non-bulk energy generation resources, such as distributed generators (DGs), behind the meter renewable or non-renewable generators, energy storage devices (including electric vehicles), and co-generation [1]. Increasing penetration of these DERs induces a never-before-seen fast voltage and frequency alteration into the distribution grid. These intermittent generators also contribute little to no inertia into the grid, resulting in fast frequency fluctuation. These new devices cannot automatically adjust to the post-disturbance power injection [2], and they rely heavily on the communication infrastructure. Increasing penetration of these small-capacity devices extensively requires coordination among themselves. This significant evolution in the power generation scheme has propelled the utilities and stakeholders to rethink the operation and protection of the modern active distribution grid [3].

Available standards and practices, such as IEEE 1547, CA Rule 21, Hawaii Rule 14H, and NISTIR 7628, help achieve the desired coordination requirement under these new paradigm. Typically, the standards for the DER interconnection are available in IEEE 1547 document [4], and are used worldwide. The CA Rule 21 governs aspects of the interconnection between the DERs and the larger power grid in California, which includes the standard for the integration of inverter-interfaced generators at the residential point of common coupling

☆ This work is supported by the National Science Foundation CPS, United States of America award 1932574 and the U.S. Department of Energy UI-ASSIST grant DE-IA0000025. All Authors were at the Washington State University in the past.

* Corresponding author at: Washington State University, Pullman, WA, United States of America.
E-mail addresses: amirkhosro.vosughi.ee@gmail.com (A. Vosughi), ali.tamimi@gmail.com (A. Tamimi), alexandra.b.king@wsu.edu (A.B. King), subir.majumder@mail.wvu.edu (S. Majumder), anurag.srivastava@mail.wvu.edu (A.K. Srivastava).

(PCC), and metering requirements. Furthermore, the Smart Inverter Working Group (SIWG) is established by the California Public Utilities Commission (CPUC) and the California Energy Commission (CEC) to develop and continuously improve this rule [5]. The Hawaii 14H rule applies to the interconnection standards for the state of Hawaii. The United States Department of Energy is also committed to create a comprehensive set of rules and regulations for the DERs within the utility operated smart grids.

Along with other engineering challenges, the discussed communication and interaction requirements for the DERs significantly impact the security and resiliency of the grid. Most of the communication requirements originate from necessary DER control actions, and therefore, the topology of the communication network often becomes a function of control requirements. Hence, control schemes often have a one-to-one relationship with system resiliency. Lack of built-in security mechanisms makes certain communication protocols more vulnerable to cyber-attacks. Additionally, although measuring equipments like phasor measurement units (PMUs), automatic metering interfaces (AMIs) uses standardized communication protocols (details can be found at [6]), as discussed, the lack of security features in communicating these measurements can also facilitate an attacker in establishing a coordinated attack. Consequently, the utilization of communication protocols with multiple security mechanisms for the prevention and mitigation of cyber-attacks is always justifiable.

In this regard, the NISTIR 7628 lays out the premise for cybersecurity in regards to the DERs applications, where the primary goal is to achieve control over a large system consisting of DERs through communication in a secure manner [7]. The establishment of such a secure communication framework will help us preserve the confidentiality, integrity, and availability (CIA) of the critical information within the grid. Once the attacker has invaded the communication network, the operator has to utilize sophisticated intrusion, and anomaly detection schemes to separate the coordinated attack from bad data [8]. However, compared to such a reactive approach, identifying the specific vulnerabilities of each of the different control actions and associated fortification of the communication channel will facilitate proactively defend the grid. Additionally, strategic investment in cybersecurity fortification will also assist us to achieve it more efficiently.

The primary objective of this paper is a comprehensive literature review for cyber–physical vulnerability and resiliency analysis for various DER functionalities and the requisite security protocols. Such an analysis will lead to comprehensive information needed for achieving a secure, reliable, and resilient grid operation with DERs. Whilst many review papers exist in the literature that deals with each of the above-mentioned topics separately, a discussion on various cyber–physical vulnerabilities of different DER control applications, associated impact on system resiliency, and mitigation strategies, in a holistic manner have never been reported before, to the best knowledge of authors. Comprehensive analysis presented in this work allows for the investigation of DER function-specific vulnerabilities and mitigation techniques separately, which has distinguished this work from other review papers. To this end, first, DER functions and their associated control schemes and communication requirements are briefly reviewed. DER system architecture is explained next, and DER standard communication protocols are discussed. Subsequently, key vulnerabilities and threats related to DER control applications and their extensive communication requirements are summarized, and the associated impact on power system resiliency are outlined. Finally, the relation among various DER functions, control schemes, cyber susceptibility impacts, and mitigation mechanisms against adverse attacks are presented, and trends and cyber requirements of the future grid are discussed. This sequential treatment framework is pictographically presented in Fig. 1, which also illustrates the section-wise organization of the paper.

Consequently, the contribution of this review article is threefold:

- Provided a detailed literature review of various DER functions with a specific focus on their associated control schemes and communication requirements. The desired cyber-fortification demands identifying the key DER-specific control functions requiring fast communication protocols, which, if compromised, can be detrimental to the power system operation. Utilizing the insights from the detailed literature review, a qualitative comparison among alternative DER control schemes with respect to different attributes, such as communication and computational requirement, performance optimality, and cyber resiliency, are presented.
- Analyzed communication requirements for the desired mission-critical DER functions, requiring fast communication utilizing an existing five-level DER system architecture. Standard communication protocols for DERs along with their specific vulnerabilities and mitigation strategies are also reviewed.
- Analyzed cyber-attacks and associated preventive security mechanisms with alternative DER standard communication protocols based on the CIA triad. Subsequently, risks, impact level, and recommended mitigation and cyber fortification solutions are compared and contrasted for different DER functions with available control schemes. Based on the detailed analysis presented in this work, we have also identified key challenges and directions for future development to enable a cyber-secure and cyber-resilient DER-rich power grid.

2. Requisite control functions to support distribution system through DERs

The primary reason behind the integration of renewable-interfaced DERs is to displace the existing conventional generators and incentivize the utilization of clean energy resources. Furthermore, DERs can also improve the distribution network operation significantly and support the grid [9], and in this regard, different ancillary services provision from the DERs are discussed in [10]. For example, since DERs enable the local generation of power, local load-generation imbalance, vis-á-vis, power losses in the distribution network are significantly reduced. Generally speaking, in contrast to bulk power producers, the rated capacity of these DERs are minuscule; however, with increasing penetration of DERs, the control of these devices has also become challenging [11]. Furthermore, the inherent intermittency of renewable-based DERs can also lead to voltage and frequency fluctuation within the future power system. In this regard, a detailed review embracing the DER integration challenges is given in [12].

Therefore, there is a need to clearly define a set of standard functionalities of the DERs and desirable coordination mechanisms that help us avoid associated drawbacks while enhancing reliability and resiliency of active distribution network. Such coordination mechanisms have also instigated new communication requirements, with the need for more flexible and bi-directional communication on the network that is detailed in IEEE-1547 [4] and CA Rule 21 [5]. In this section, some of these additional functionalities of DERs with the fast communication interface requirements are revisited. Associated requisite supervisory control actions are also discussed. Since the dynamics of the movement of entities in the electricity market are slower, this work stresses control and coordination requirements that operate faster.

2.1. DER control schemes

The coordination among the DER controllers, and coordinators is heavily influenced by the inter-DER and DER-coordinator communication framework. Broadly speaking, there exist four control schemes, defined as follows:

Local Control: This class of controllers mainly relies on “droop” characteristics among active and reactive power, voltage and frequency, as given in the IEEE-1547 standard. This control class utilizes

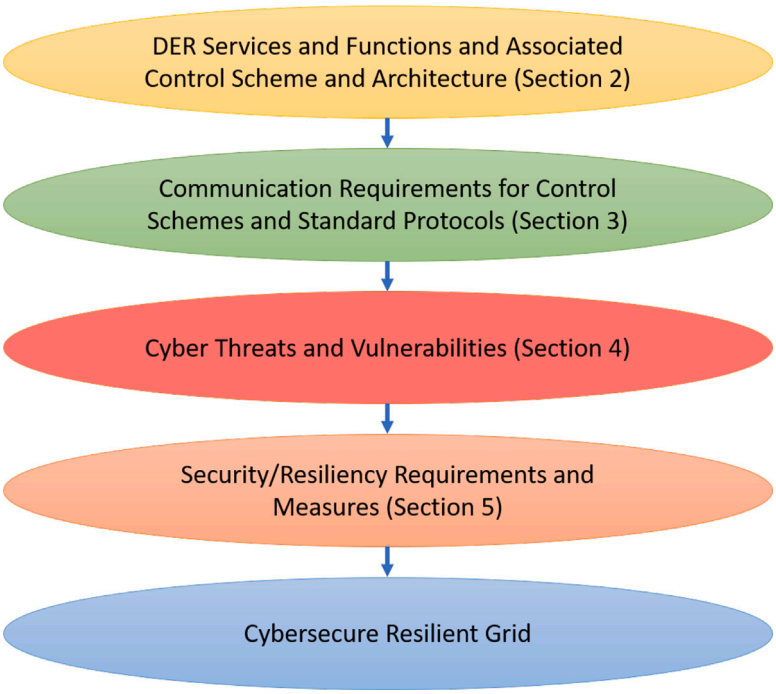

Fig. 1. Overview of cyber–physical vulnerabilities and resiliency with DER integration.

the physical relationship among power system parameters to determine the control strategy. The measurement and control actions are primarily local, with no communication required among the controllers. Nevertheless, droop-configuration set points can be obtained from one of the coordinators. Considering the control action is myopic, the controller often suffers from stability issues in a larger network, and endures susceptibility to local measurement noises.

Centralized Control: Since the electricity network's performance is reliant on the collective action of different parts of the system that are connected by power network, traditionally, all the controllers measure and communicate local information to a central controller who computes control action and informs the local controller. While the local controllers are no longer needed in this regard, the central level's computation requirement becomes enormous. Furthermore, local measurement and control action requires significant communication infrastructure, and control actions are inherently delayed.

Decentralized Control: Like centralized control, here the local coordinators also communicate with higher-level coordinators; however, all the local measurements are not aggregated at a central location; rather, a group of controllers is clustered with one coordinator and coordinators communicate among each other for the consensus. Therefore, in decentralized control, there will be two or more coordinators. Consequently, the centralized computation requirement in this control scheme will be notably reduced.

Distributed Control: Central coordinators are absent in the distributed control, and local controllers communicate with their topological neighbors to reach the consensus. Therefore, all the control entities in this scheme are autonomous at the same hierarchical level.

Fig. 2 provides the schematic diagrams of the above-mentioned schemes and contrasts the arrangement of the controller and sensing nodes with coordination and management nodes on those schemes. The sensing and controller nodes and coordination and management nodes are clearly identified. It can be clearly seen that in the case of centralized control, all the local measurements are brought to single coordination and management node through bidirectional communication, while local control does not require coordination (communication needed only for parameter update). Decentralized control derives some of the benefits of a central controller but is made resilient through clustering. In the absence of a leader–follower structure, each node needs

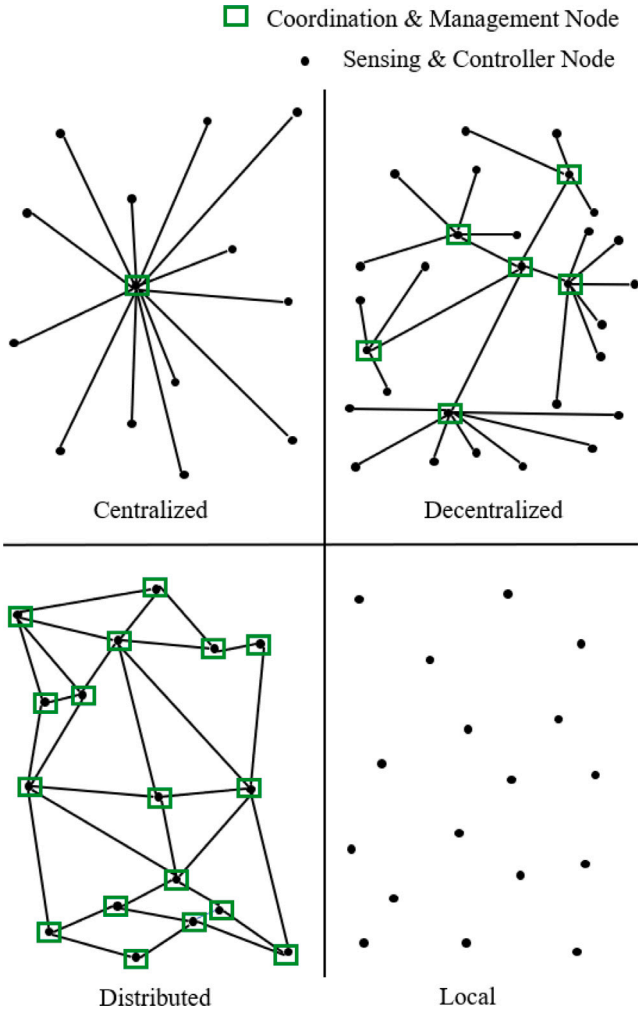

Fig. 2. Centralized, Decentralized, Distributed, and Local Control Schemes.

to have sensing and coordinating capability in distributed control. The coarseness of the communication is, of course, driven by the control function. The use of these control schemes for various DER functions is discussed next.

2.2. DER for voltage support

Increasing variability in the power injection with the high penetration of renewable-interfaced DERs directly translates into voltage fluctuations [13]. Traditional relationship among network voltage and reactive power injection motivates us to use conventional devices, such as on-load tap-changing transformers (OLTC), capacitor banks and voltage regulators to inject reactive power into the grid for voltage control; yet, the use of mechanical switches prohibits continuous control of these devices. While the fast voltage variation induced by renewable energy resources could have been absorbed by reactive power provision from inverter-interfaced resources, the older IEEE 1547 standard prohibits the same. However, enabled by the IEEE 1547-2018 standard, while utilizing computing, sensing, and communication capabilities of the DERs, one can limit voltage variations within desired limits using local DERs. Various recently developed control frameworks utilized for voltage control are discussed in the following paragraphs:

2.2.1. Local voltage control

As discussed, the primary benefit of this control method is its communication agnostic nature [14]. The local Volt/VAR control scheme based on the droop control strategy proposed in IEEE 1547-2008 standard is provided in [13,15,16]. The integration of a droop-based voltage control loop within the PV inverters to limit the generated transient is considered in [16]. A volt/var control algorithm has been discussed in [15], where, the objective function is shown to be Lyapunov function, implying its global asymptotic stability. Furthermore, a higher R/X ratio of the distribution network also enforces the use of active power for voltage control [17,18]. Voltage control for simultaneously controlling of both active and reactive power output from battery storage devices has been considered in [13,19]. Droop-based network-wide overvoltage protection has also been considered in [20,21].

However, it has been shown that droop-type controllers (especially [15]) suffer from instability and inefficiency issues, especially when the network is large [22]. Two different types of controllers have been chosen in [16], and, among them, instantaneous reactive power injection based on droop characteristics result in instabilities. Such instabilities can be mitigated if the controller characteristics mimics first-order response. In the controller designed by Varentec Inc. [23], control actions are taken by the edge devices with set-points received from the central location. Based on the received set-points with the OPF problem, each controller designed by [24] acts to limit voltage variation. Based on the coefficients received from the centralized power measurement unit local DER controllers nodal voltages are controlled in [25].

2.2.2. Decentralized voltage control

A fully decentralized approach, where the central controller generates possible future scenarios in terms of load and renewable power generation and solves stochastic control problems to determine possible control actions, has been considered [26]. Nevertheless, the drawback of this method arises from the finiteness of the computational operating horizon. A strategy that limits over-voltage through injection or extraction of reactive power from diesel generators has been considered in [27]. [28] shows that the decentralized control performs very well to control voltage profile in a wind power plant in the presence of non-negligible communication delays. Multiple cluster formation and voltage sensitivity factor-based control mechanisms in each cluster representing decentralized nodes are given in [29]. Higher data-rate requirements with decentralized control are observed in a hardware-in-loop arrangement, and the bandwidth requirement increases with increasing network size [30].

2.2.3. Distributed voltage control

Typically, the distributed voltage control is based on consensus-based method. Although voltage control is usually carried out through the injection of reactive power, due to higher R/X ratio of distribution network, control of voltage through active power injection from battery storage devices also gains significance. Active control of distribution network voltage profile through a consensus-based algorithm is discussed in [31]. Here, a weighted consensus algorithm decides proportional sharing of power, and dynamic consensus control prevents over-extraction of charge from the depleting batteries. In another work, consensus-based sharing of information about active power shortage in the batteries, and convergence of power production from individual devices are considered in [32]. A two-level voltage control mechanism, consisting of droop-based control action in the lower-level and consensus-based control action upper-level, is discussed in [33]. Another active power injection-based voltage control strategy based on the leader-following method has been discussed in [34].

Duality-based approaches for distributed volt–var control has also been considered in the literature. Typically the alternating direction method of multipliers (ADMM) requires the presence of a coordinator for the convergence of the algorithm. A consensus-based ADMM approach has been considered in [35] for regulating the voltage profile through reactive power injection. Recently discussed distributed control methods are based on primal–dual iterative methods [36]. A two-stage distributed voltage control algorithm, where the second stage deploys distributed communication and control for over-voltage prevention, has been considered in [37]. Additionally, in the controller proposed by Panasonic Corp., the control action is selected by each of the controllers based on the information (in terms of active and reactive power dispatch) from other peers [38].

2.2.4. Centralized voltage control

Ref. [39] acknowledges that the typical implementation of centralized voltage control is inadequate when the power generation fluctuation level is too high. To combat conventional VAR generators' infrequent operational requirements, they have used satellite-measured solar irradiation data for simultaneous forecasting and calculating the desired control actions. However, it is crucial to note that the accessibility of satellite-observed data is both limited and expensive. Improvement of voltage profile through simultaneous injection of active and reactive power in a centralized framework is discussed in [40]. The controller extensively relies on the forecast, and optimization is carried out by a heuristic-based approach, which may not be suitable from a real-time control point of view. A model predictive control-based centralized controller for determining OLTC and DER set-points are discussed in [41], where, operation of OLTCs is suitably adjusted to combat frequent switching problems while achieving desirable response. While [28] claims that decreasing communication delay in a centralized communication framework can significantly improve system response, it is well-known that centralized control heavily relies on the communication protocol and reduction in the delay is unlikely, other than in a small system.

Improvement in voltage profile through centralized control of both active and reactive power is considered in [42] for a three-phase unbalanced system. While the authors claim that the controller performance remains unaffected by computational and communication delay of 1 min, they remain silent on intra-minute power fluctuation. Furthermore, it is imminent that in addition to the discussed pitfalls, the amount of data collection and over-reliance on the central database makes this control architecture an easy target for cyber-security threats. Furthermore, failure in the central supervisor equates to the loss of control in the entire system [29]. From the industry side, the controller designed by Mitsubishi Electric Corp. [43] is designed to operate voltage within bound and the one designed by Dominion Resources, Inc [44] utilizes AMI data. Centralized voltage and frequency control in a microgrid are considered in [45].

2.3. Frequency support with DER

The frequency of a power system is closely related to the load-generation balance within a network, and it must be regulated around the associated nominal value. In the conventional power system, the inertial constant is relatively high, and the system frequency is regulated by the built-in automatic generation control (AGC) [46]. In an active distributed system, DER can contribute to the frequency regulation and is essential if the network is required to be operated as a microgrid. However, the integration of renewable-interfaced DERs introduces new challenges for frequency control because of the lack of inertial support. Furthermore, with increasing penetration of clean energy DERs, while replacing conventional generators, the rotational inertia of conventional power system is on the decline along with the introduction of increasing fast-variation due to renewable penetration [47]. The resulting power system suffers from the higher rate of change of frequency (ROCOF), lower frequency nadir, even with a small power imbalance. However, unlike conventional generators, DERs are of faster dynamics, making them suitable for quicker reserve provision.

Typically, a phase-locked loop (PLL) is utilized to synchronize the DERs into the grid. In the grid-connected mode, unless specifically designed, DERs may not be responsible for responding to system frequency; however, they should actively participate in the frequency regulation during the islanded operation. The decentralized frequency control method can reduce dependency on the communication layer [48], but, solely relying on local frequency measurement for ROCOF detection may be expensive, and often lead to false triggering with inverter-interfaced resources [49]. Although, traditional centralized frequency control has an excellent transient response, due to the need of a wide-area data acquisition system and associated communication delays, the system can move to instability, especially in a reduced inertia system [50].

As in voltage control, different controller design types for frequency control are also available in the literature and a few recent literature is discussed in the following paragraphs.

2.3.1. Local frequency control

In the conventional power system, all the synchronous machine-based generators simultaneously respond to system-wide frequency deviation by the virtue of its inherent rotational inertia. The droop-based mechanism is a feedback control that synchronously responds to such frequency deviation, and is a widely used technique to control system frequency. In the current AGC-based mechanism, conventional generators participate in the regulation market, and their regulation set points are frequently adjusted [51].

Unlike voltage, it is imminent that frequency has a system-wide implication, and all the control action needs to be coordinated by a central controller through set points. Stabilizing system frequency following disturbance gains the highest priority, and researchers have focused on local control strategies to inject the optimal amount of power from wind turbine-based generators [52,53]. While frequency control utilizing inverters in [54] is solely based on local measurements, they are silent on consequences of pollution in local frequency measurements. Similarly, droop-based local frequency control and frequency reference set by a central controller in microgrid settings are considered in [55].

2.3.2. Decentralized frequency control

Local control methodologies are mainly suitable for synchronous machine-based generators since they inherently respond to system frequency imbalance through speed governor. To avoid using polluted local frequency measurement (as a substitute for the lack of speed-governor action) for determining the control action, the local frequency is calculated based on multiple local measurements and directly communicated with DERs for frequency control [56–58]. However, centralized frequency measurement and communication make primary frequency response to become inherently delayed, which is further complicated by reduced system inertia with increasing penetration of inverter-interfaced DERs. If these delays are significant, the system can quickly move towards instability [50]. Furthermore, reliance on communication networks induces an additional point of vulnerability into the power system. Nevertheless, decentralized control with DERs has been widely discussed in the literature, but in most cases, their application is limited to tuning PID parameter gains for the secondary frequency control loop [59–61]. Additionally, such secondary frequency control frameworks can be suitably adjusted for multi-autonomous microgrid power-sharing [62].

2.3.3. Distributed frequency control

Unlike distributed voltage control, distributed frequency controllers participate in the hierarchically upper level. Typically, local generators with built-in primary control respond immediately after a disturbance, which inherently results in steady-state frequency error. To induce the steady-state frequency error to become zero, the secondary control loop with AGCs kicks in. Typically, AGCs consists of PI controllers with the inputs being area frequency error, and it creates a set point for individual generators. With increasing penetration of DERs, it is expected that DERs would also respond in AGC action. While distributed AGC action is preferable, considering inherent drawbacks associated with distributed PI control, in the inner control loop, frequency is controlled against a dynamic frequency reference. Here, the reference frequency is controlled utilizing a PI-controller, decreasing the steady-state error to zero [63]. The system frequency in the developed consensus protocols, in [64], with integral control action is shown converge asymptotically. In another analysis, a distributed controller with PI structure is utilized to control bus frequency [65]. In the same work, it has been shown that, although centralized controllers can achieve better performance compared to distributed control, they require detailed information consisting of power system parameters along with system-wide load-generation imbalance. This is very much communication intensive. Feasible cooperation-based distributed model predictive control has been employed in [66] to achieve cooperation for power-sharing to achieve zero area control error. However, the distributed-ness of the control algorithm is limited to large generators, and DERs can only participate through local energy management system.

2.3.4. Centralized frequency control

Although local controllers' response in the traditional grid is based on local droop, the reliance of local generators on the centralized market makes them centralized [67,68]. Furthermore, since droop alone would introduce steady-state frequency error, the proportional–integral (PI) control loop is generally deployed to reduce the frequency error to zero, and is also a widely accepted technique. However, a PI controller's gains rely on system operating point and need to be properly tuned; one of such coordinated techniques to tune PI controller gains optimally based on particle swarm optimization algorithm is available in [69]. Furthermore, in a microgrid architecture, centralized frequency controller can be used to control demand responding (DR) loads [70–73]. In all of these cases, control action is communicated remotely to all of the DER controllers.

2.4. Emergency control action

Accidents happen. With the increasing penetration of DER in the smart grid, while it is intended that the DERs should continue to operate as a microgrid even during disasters, they must react to the emergency situations for the power grid's operational safety. In the following paragraphs, we discuss different requirements needed to be satisfied to avoid hazardous conditions during disasters. In this regard, a review of DER's different functions during islanded operating mode is given in [74].

2.4.1. Anti-islanding protection

Traditionally, in the radial distribution network, all the downstream nodes are automatically disconnected from the rest of the healthy part of the system in the post-fault protection mechanism operation. In the active distribution system, the disconnected system can operate in the islanded mode. While it is desirable that a part of the electricity grid should continue to operate normally when the power system is under fault, it is desirable to avoid the formation of unintentional islands, since they can threaten the safety of the repair crews. Also, lack of proper synchronization following the reconnection can lead the entire power system to instability. Therefore, it is essential to detect the formation of such unintentional islands. Many studies focus on the various anti-islanding approaches and reviews of islanding detection and protection techniques are available in [75,76]. Anti-islanding protection strategies can be categorized into two groups, (a) measurement-based anti-islanding approaches and (b) direct command-based control approaches.

1. Measurement-based Anti-Islanding Approaches: These Anti-Islanding (AI) approaches utilize local measurements for islanding detection. It can be achieved under both passive and active paradigms. Passive approaches rely on local parameters measurements at the point of standard connection and anomaly detection based on the local measurement of (voltage magnitude, frequency, ROCOF, etc.). DERs will be tripped provided that any of the local measurements surpasses the preset threshold. While this methodology is simple and inexpensive, it suffers from extensive non-detecting zones (NDZs). Large NDZs are typically caused by synchronous generator-based DGs, with high inertia, or unavailability of significant deviation in the local measurement due to small load-generation imbalance [77,78]. Consequently, local measurement based passive approaches are seldom used in practice.

Active anti-islanding approaches rely on the continuous injection of small disturbances with positive feedback in the control loop of inverter-based DERs [79]. In the grid-connected mode, these disturbances do not affect the stability of the system. However, once islanded, such small disturbances can create larger voltage and frequency excursion, leading to automatic triggering of conventional protection mechanisms. Typical active islanding detection approaches include Sandia frequency shift (SFS) and Sandia voltage shift (SVS) [80]. These techniques are inexpensive to implement and have been successfully adopted in the industry. However, since this method relies on an active injection of disturbances, improper system design can lead to instability.

The other measurement-based approaches utilizes power line communications (PLCs). A constant signal frequency is injected from upstream nodes, and the absence of which signifies islanded condition [81,82]. For example, the PLC signal of the frequency range of 250–500 kHz is utilized in [81].

2. Direct Command-based Control Approaches: Typically, a direct transfer trip (DTT) mechanism is one of the most sophisticated communication-based approaches for protecting against unintentional islanding [83]. This mechanism relies on continuous monitoring of reclosers, and upon detection of an island, all the downstream DERs are turned off. However, such a method is very expensive, has higher implementation complexity, and is vulnerable to cyber-threats.

2.4.2. Voltage and frequency ride through (V/FRT)

The majority of the faults occurring within the distribution network are temporary and can automatically clear themselves without requiring manual intervention. Therefore, it is not desirable that DERs to become immediately disconnected following a surge/fault; instead, DER should remain connected into the grid for a finite duration, expecting the fault to clear itself. This is supported by the fact that DERs have limited capability to feed the faults contrary to the main grid [84]. However, the situation becomes complicated with increasing penetration of DERs, because, if DERs are immediately disconnected after the temporary fault is cleared, it is expected that both local voltage and frequency would fall after fault clearing, resulting in cascaded failure. This phenomenon is majorly observed in wind power plants, and to combat this challenge, the ride-through capability requirements were first implemented by E.ON-Netz [85]. Fault ride-through capabilities are specific to DERs and are implemented locally. The grid code in this regard can be available from [86]. The technical implication of existing V/FRT standards is also available in [84].

2.5. Power quality support functions

While it is desirable that the voltage and frequency at the PCC remains at the nominal magnitude, and are purely sinusoids, imperfection of the power system made them deviate from such requirements [87]. Additionally, the integration of inverter-interfaced DERs forces the system to significantly deviate from such a nominal standard. The lines' impedance make the drooped voltage to be perceivable further away from the fault location, and the typical regulation devices are unable to improve such dropped voltage significantly. Furthermore, even if it occurs only for a very short duration, such low-voltage can lead to the shutting down of susceptible equipment [88]. Typically, power quality (PQ) issues are categorized into: (i) voltage sags, (ii) voltage fluctuation and flicker, (iii) voltage and current unbalance, (iv) voltage and current harmonics and (v) overvoltages. Impact of power quality issues do not remain limited to the power system, rather, the high-frequency voltage and current components can interact and create interference in the nearby telecommunication lines [89].

2.6. Monitoring and support functionalities

Monitoring of DERs is important to determine systems' capacity to operate at its designed potential during an abnormal condition, while enabling us to carry out future analysis. Furthermore, the reliability of the system is enhanced notably when the situation of the system and associated control action are frequently monitored. One of the widely monitored DER parameters is the system operating temperature. It is well known that the operating condition of the system will be dynamically rated, if the system operating temperature is beyond the set point. To mitigate the problem of false alarm, information from multiple neighborhood DERs are required to be cross verified, and therefore, control action should not be local. Often times, additional disconnection of one or more communication channels are considered as the consequence of an actual event. Furthermore, as the edge devices are growing to become intelligent, they can detect and send alert for anomalies [90]. A remote temperature monitoring algorithm has been proposed in [91,92] as a part of predictive condition monitoring tool. Automated shutoff and alert monitoring following a fire event along with the remote operation of automatic fire extinguishers has been considered in [93]. While, the requisite monitoring for the proactive response to the evolving cyber-threats has been considered in [94], it is also to be noted that requisite monitoring can also make the system vulnerable to cyberattacks, and recommended DER cybersecurity functionalities are discussed in [95].

2.7. Typical hierarchical control architecture for a microgrid

As indicated earlier, in addition to being operated in a grid-connected mode, DERs allow the grids to operate as islands while increasing the resiliency of the entire power system [96]. However, control of an islanded microgrid can be daunting [97] and often requires specialized control hardware. Although the microgrids are designed to operate in the islanded mode, it is expected that the microgrids are capable to switch between grid-connected and islanded mode whenever necessary. In grid-connected mode, the DERs will usually operate in a grid-following mode; wherein, microgrid operation requires the operation of at least one DER in the grid-forming mode [98]. Change of mode from grid-connected status to microgrid,

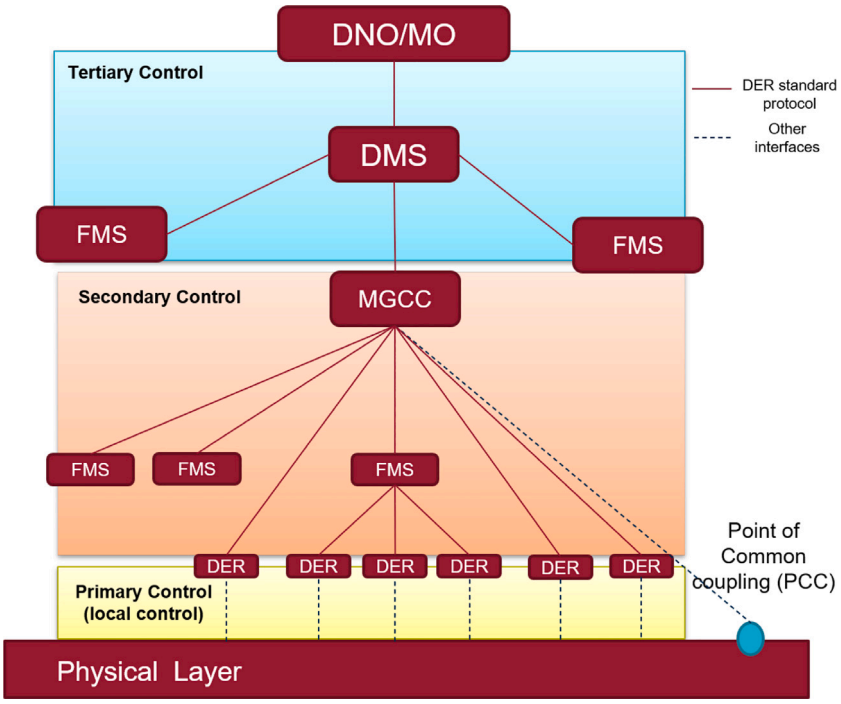

Fig. 3. A typical hierarchical architecture of DER in a microgrid.

and vice-versa, can be decided in a coordinated fashion. In the absence of synchronous machine-based DERs, inverter-interfaced DER can provide voltage and frequency reference to the entire grid [99]. Lack of speed-control requires direct communication of the local frequency information into the controller.

Operational control of grid-connected microgrids utilizing a three-layer, decentralized and agent-based control architecture based on [57, 74] is shown in Fig. 3. Such a control architecture is described as follows:

1. *Primary Control* is locally carried out by individual DERs to limit the local voltage and frequency fluctuation through the droop-based mechanism. This level is equivalent to the local layer in the distribution grid. Controllers responsible for voltage control can also utilize distributed control techniques. Additionally, since the microgrids are capable of operating in an islanded fashion, the tasks carried out by primary control also include islanding detection, voltage and frequency fault ride through, and communicating local measurements for monitoring and determining system alert condition.

2. Tasks in *Secondary Control* are coordinated by the microgrid control center (MGCC) as a part of microgrid energy management system (MEMS), and its responsibility is to ensure coordination among facility management systems (FMS) and DERs, including managing of intentional islands and load shedding. MGCC segregates the DERs into clusters through FMS and communicates the set points to each of the DERs for primary control [100]. This level is equivalent to facility layer in the distribution network.

3. In the *Tertiary Control* level, MGCC interacts with the distribution network operator (DNO) and market operator (MO) for the market participants and establishment of the set point. In the grid connected mode, the utility resides in this level. If the network becomes isolated, the MGCCs and other FMS are controlled by DNO itself. The advanced distribution management system (ADMS) and outage management system (OMS) along with supervisory control and data acquisition (SCADA) continuously monitor and maintain a smoother operation of the grid. It operates through the measurements obtained from the physical layer through an advanced metering interface (AMI) and global information system (GIS) data. When the microgrid gets isolated, some of the supervisory actions in this layer will be taken care of in the secondary control layer.

The MGCC also has to work on load-sharing (LS) optimization in addition to the discussed droop-based voltage and frequency control. LS is a sophisticated task, especially in an islanded microgrid because of multiple DERs [101]. Both the droop method and active LS methods are used in this regard. Here, the droop-based method requires minimal communication, while, active LS methods extensively relies on intercommunication infrastructure. While local droop voltage control actions are communication agnostic, low-bandwidth communication is still required for sharing the local frequency information, synchronization, and data management purposes [102].

2.8. Comparison of the requisite control methods for DERs

Conventionally, centralized and local control techniques are widely used due to their inherent implementational simplicity. Local control schemes require no communication infrastructure. Additionally, most of these schemes are derived from the physical properties of the power system, which although is less vulnerable to cyber attacks, results into sub-optimality. However, with the integration of many DERs with minuscule capacity, as discussed, overly relying on either of the mentioned methods can be both unreliable and expensive. Central controllers are computation and communication-intensive and naturally delayed, while local controllers are myopic and extensively rely on the system's physical properties. Successively, decentralized and distributed controllers have slowly started to replace existing controllers.

In this regard, Table 1 shows the comparison of these control schemes for different traits, which is consolidated from the discussed existing literature. The pros and cons of each of the traits for the discussed control schemes are reported, and subsequently, a qualitative rank of each of the schemes is provided. It is clearly seen from our discussion, and the proposed qualitative rank that none of the control schemes unilaterally perform well across the discussed four traits, and therefore, it is expected that a mix of all four different kinds of control scheme will achieve the greater good. The discussed literature also indicates the limited use of all the four different types of control

Table 1
Comparison between different types of control schemes (VH: Very high, H: High, M:Medium, L:Low, VL: Very Low)

Traits	Centralized	Decentralized	Local	Distributed
Communication Requirement	Each DG node communicate with the central coordinator following a star topology (for n nodes in the distribution network requires $n-1$ bi-directional communication links). It is possible that the data transfer can take place through other nodes. The back up links between nodes can also be present in another centralized topology. In this case, if a link is broken, the data can be transferred through the back up link [H,VH]	Number of communication links can vary depending upon existence of computation nodes. Each of the cluster member nodes communicates with associated coordinators — each of these coordinators are also connected through high speed links [H,VH]	Local controllers are reliant on central controllers only for the set-points/ can compute set-points in a distributed way; but associated communication requirement is comparatively lower — each of the controller operate autonomously based on local measurements [L]	The sparsity of the communication requirement among central controllers determines the requisite number of communication links — in a distribution network with n nodes there will be at least $n-1$ links — if the intra-nodal link availabilities are coarse enough then each node communicates with $n-1$ other nodes, totaling $\frac{n(n-1)}{2}$ communication links — the computational coordination requirement requires the links to be very fast [M,VH]
Computational Requirement and coordination	• Central node: Requires multiple servers with high computations. Computation is also needed to handle coordination among the back up links [VH] • Edge devices: Each of the edge devices reports local measurement to the central agent, who in turn computes the control action for all the DGs — edge devices has lower computation requirement [L]	• Cluster lead node: Needs to compute the control action for the cluster's DGs. [H] • Edge devices: Computational requirement is similar to that of centralized — each DG node reports the data to the cluster lead [L]	• Edge devices: Each of the DGs operate autonomously based on local measurements. They do not require any coordination [L,M]	• Edge devices: Each the DG-controllers need to be intelligent enough to coordinate with its topological neighbors [M]
Performance Optimality	Reliance on all the local measurements in real-time makes this control type to be the optimal [VH]	While the DGs are separated into several clusters, and each of the cluster-coordinator computes the control actions for the DGs; the clusters need to coordinate among themselves for overall optimality [H]	The controllers, based on their local measurements, acts on their own to determine control actions — hence, optimality is not guaranteed; traditional literature utilizes topology of the distribution network for the coordinated control action [VL]	Although this type of controller ensures optimality, it is overly reliant on communication network for information exchange; unlike other methods this controller is a gradient-based method, and hence convergence can be very slow; one needs to continuously deploy control actions to be in close-loop which makes the controller often prone to failure [H]
Cyber Resiliency	• Communication: Since the number of back up links is low, failure of a link may lead to the failure of the corresponding DGs [VL] • Computing: All the computations are executed at one node for deciding the control action [VL] • Propagation impact of attack: Any of DGs can be a potential entry point for an attack to the centralized node — since a DG is directly connected to the centralized node (in some topology with a few more links), by compromising it, it is possible to take over the centralized node [VL]	• Communication: The failure of one of the communication link makes associated cluster to be out of service — existence of back up links reduces overall failure probability [L] • Computing: Computation are done in the lead nodes. [L,M] • Propagation impact of attack: Any of DGs within a cluster is a possible attack entry point — by compromising a DG, an attacker can take over the lead node of the cluster [M]	• Communication: No communication links between DGs. [VH] • Computing: Computations are completely independent for each of the node. [VH] • Propagation impact of attack: Since there is no communication between DGs, compromising a DG can only impact on it (not other DGs) — network performance can be impacted — the DGs can be compromised through the supervisory node [VH]	• Communication: Result of a communication link failure, a few nodes can become out of service (depends on link topology). [H] • Computing: Computations are coordinated through other nodes. [H,VH] • Propagation impact of attack: If an attacker is able to compromise a DG, it is possible to take over the neighbors — the distance between a DG and compromised DG has inverse relation with the probability of the attacker access. [H]

schemes for various DER functionalities. The risk and the recommended security mechanisms to be deployed for these control schemes have later been discussed in this paper, and are required to be used alongside Table 1 to compare the performance of these control schemes.

Since the discussed control and frameworks are majorly supported by communication systems; and in this regard, various communication and data exchange framework will be discussed in the next section.

3. DER communications and data exchange framework

The requisite communication protocols must have the capability to support the desired DER functionalities while providing the data exchange interfaces. This will be in conjunction with enough measures to avoid unwanted intrusions. Such interfaces are required to be regulated under interconnection standards and agreements, such as, IEEE 1547 and CA Rule 21. Based on these standards [103], the main communication requirement for DER-interfacing can be summarized as follows:

1. Availability of fast peer to peer (P2P) communication
2. Should be networkable throughout the utility enterprise
3. Network availability should be high
4. Should ensure guaranteed delivery times
5. Built on well-established standards
6. Capable of interoperability among various vendors
7. Ensures support for voltage and current data-samples
8. Capable of intra-DER file exchange
9. Has the capability of auto-configuration during communication failure
10. Compatible with standard security protocols

In this regard, a technical report available in [104] provides a comprehensive review of communication requirements and standard protocols for the DERs. In the following paragraphs, we first review the DER system architectures. Subsequently, standard communication protocols for data exchange will be introduced.

3.1. DER system architecture

DER's integration has instigated new communication requirements with the need for more flexible and bi-directional communication architecture [105]. As discussed, one uses a mix of the decentralized agent-based framework, local control, distributed control architecture, along with centralized supervisory monitoring and control in the modern electricity grid. The control action is often implemented through the communication infrastructure, and, this way, communication infrastructure mimics control architecture. In this regard, the EPRI report on *Cyber Security for DER Systems* is notable for introducing a five-level hierarchical DER architecture for coordinated DER operation [106]. This report also discusses associated security requirements for reliable deployment. Inspired by this architecture (see [106]), we readjust it to cover the aforementioned DER functionalities (discussed in Section 2) that require fast supervisory and communication infrastructure, and, the three levels of such a hierarchical architecture is illustrated in Fig. 4. Different levels in this architecture leverage the high abstraction and alternative hierarchical DER communications which are enumerated below. The discussion of each of the levels is also partially borrowed from [106].

1. Autonomous Cyber-Physical DER Generation and Storage
2. Facility DER Management Systems
3. Distribution Utility Operational Analytics

3.1.1. Autonomous cyber-physical DER generation and storage (local level)

As seen in Fig. 4, this level resides at the lowest hierarchical level and primarily consists of different DERs, such as distributed generators, storage devices, and controllable loads, that interact with the grid-based on local measurements. Often, the pre-adjusted set-points are obtained from higher levels. These autonomous DERs can regulate the system's dynamics instantaneously and while reacting to emergencies, such as islanding detection, V/FRT. The local controllers can also coordinate among themselves to lead the system to a desired operating point. Local controllers are also responsible for sending local measurements to upper layers for supervisory control, monitoring, and providing an alert when required. Based on the communicated set points these local controllers may deploy local/distributed control actions. Alternatively, these local controllers may be entirely reliant on the upper level for the control action in a centralized/decentralized control framework.

3.1.2. Facility DER management system (facility level)

The Facility DER management system in Fig. 4, regulates the operation of the autonomous cyber–physical DER layer by sending necessary supervisory/direct control actions. The facility's boundary might be as small as a residential home, or as sizable as business and industrial establishments such as campuses, shopping centers, industrial combined heat and power (CHP), hospitals, even a microgrid, and virtual power plant (VPP). The facility management system can also compute and communicate necessary control actions while being coordinated by the distribution utility. Here, DER's configuration is adjusted by both facility operator, utilities and retail energy providers (REPs) for regulating local energy management systems (EMS) outcome and grid coordination respectively. Thusly, connection of these DERs to the facility management system is usually the gateway for integrating DER to the utility. Wireless protocols, such as Zigbee or LoWPAN, are popular for easy and cheap installation in a small-sized facilities like homes. Residential DERs might also be connected to smart meters through Home Area Network (HAN) which is located on the residential home side. HAN might also provide other home automation services, such as home energy management, surveillance control, and monitoring. Equivalent local networks utilized for business/building and industrial site is called BAN and IAN respectively [107].

A Virtual power plant (VPP) [108] shares similar kinds of functionalities as DERMS, but often connected to the distribution network for operation. A VPP consists of multiple DERs, such as conventional generators and intermittent generating resources, alongside controllable loads, electric vehicles (EV), and residential or large scale storage units, to mimic the operation of a conventional power plant [109]. Such close coupling with a conventional power plant is facilitated by communication infrastructure, and in this regard, they can be called the Internet of Energy (IoE) [105]. This way, VPP managed distribution network can remain invisible to the utility, and can operate in isolated/microgrid mode.

Utilities or virtual power plant (VPP) managers often trade into the market through partners such as REP, aggregators, or other third parties. Therefore, DERs are connected to the utilities through the associated ICT. The communication is usually implemented using standard IP based protocols, following the guidelines suggested by IEEE 1547.

3.1.3. Distribution utility operational analytics (utility level)

The DER management system (DERMS) is a software framework for facilitating the visibility of DER to the distribution system operators (DSO) for the operational coordination [110]. As shown in Fig. 4, this platform operates alongside the advanced distribution management system (ADMS) and supervises the high-level functioning of the DERs and distribution network itself. DER Management System (DERMS) determines the desired performance requirement and communicates the requisite configuration and associated command to a specific or a group of devices. This way, aggregation of the DERs facilitates efficient communication [111,112]. Typically, clustering or aggregation is carried out based on network topological, vendor-specific, or special functional requirements. Considering this, the California Energy Commission has suggested Utility-DER communication recommendations, control architectures, and DER clustering approaches [112]. While utility communication to the DERs is generally asynchronous, emergency control actions can be broadcasted or multicasted simultaneously. Frequently, when the central controller resides on the DERMS, it can also directly control individual or DER clusters. Different kinds of data might be transferred through this layer, such as, emergency turn on/off command, mode switching command, parameter configuration, providing ancillary services, and P2P communication between facility DER management systems [113].

In the grid connected mode, this layer also facilitates information exchange between Regional Transmission Organization (RTO) and Independent System Operator (ISO), and Retailers and utilities for bulk power exchange, while ensuring power quality standards. In this regard, the existing coordination schemes among the transmission system operator (TSO) and distribution system operator (DSO) are discussed in [114] for a network with high penetration of DERs.

Apart from the discussed communication architectures, among other architectural models, a hybrid communication architecture based on connecting DERs to the smart meter through the home area network (HAN) is presented in [115]. The information is collected in Data Aggregation Point (DAP), through a neighborhood network (NAN), and finally, the wide-area network (WAN) provides a communication link to the DMS and DERMS. The categorization for the requisite communication schemes of DER integration is presented in [111]. Challenges and trends in the existing communication architectures for DER integrated microgrid (MG) and distribution system is presented in [116].

As already indicated, it is imminent that the discussed DER functionalities (in Section 2) can be coordinated through either of the discussed three layers of the developed architecture. Table 2 depicts a brief account of the activities of each of the layers, which can vary significantly depending on the control objectives. The control functionalities considered in this table are partially obtained from Sandia's report for cybersecurity recommendations [117]. Here, since some of the requisite control action is addressed in the facility layer when the microgrid gets isolated, the actions of facility and utility layer are merged together in

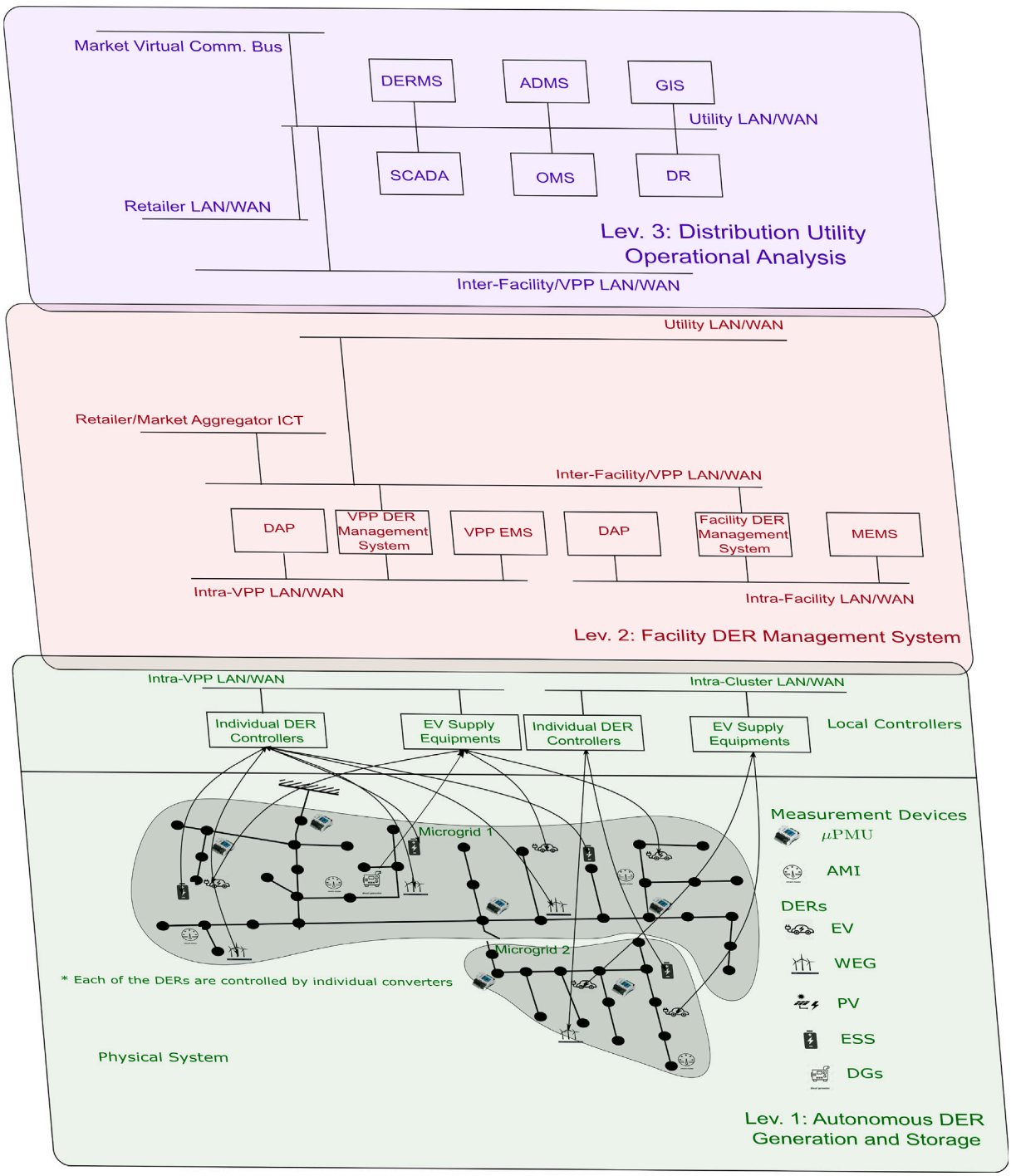

Fig. 4. Extended Three-Level Hierarchical DER System Architecture.

most of the cases. The discussed table helps us identify the essential critical communication channel requiring additional fortification, failing which the security of associated functionalities of the DER will be severely compromised.

3.2. DER standard communication protocols

There exist a few standard communication protocols recognized by the IEEE 1547 to facilitate implementation of the discussed communication architectures. These include IEEE 1815, IEC 61850, Modbus, and IEEE 2030.5 [104]. We will briefly discuss them in the following paragraphs.

3.2.1. IEEE 2030.5

Smart Energy Profile (SEP2) or IEEE 2030.5 protocol is explicitly developed for communicating DER with other network entities in the smart grid environment [4,118]. It is the default application level protocol in California Rule 21 [104]. The evolution of IEEE 2030 to satisfy the requirements set by the IEEE 1547 standard is discussed in the technical report [119]. IEEE 2030.5 has Representational state transfer (RESTful) architecture along with an HTTP interface. SEP 2.0 supports both User Datagram Protocol (UDP) and TCP/IP, operating for IPv4 and IPv6. The overview of the IEEE 2030.5 and the utility of this protocol to ensure interoperability among DERs and various other analytics platforms are discussed in [118]. Deployment of several

Table 2
DER Functionalities and Associated Control Actions.

Example DER Functionalities	Example Control Objectives /Modes	Local Layer	Facility Layer	Utility Layer
Monitoring	Monitor DER status and output	Communicate local measurements, including individual DER alarm and supporting informations to the hierarchically upper data aggregation points (DAP)	DAP/SCADA receives signal — MEMS/ADMS processes these information to monitor overall system behavior and performance	
Voltage Control (VC)	Voltage–Watt mode	DERs operation is regulated through the settings provided from upper layer (or, DERs directly responds to the control action from the upper layer) following hysteresis and delayed action to avoid hunting — two-quadrant operation for typical generators (diesel/inverter-based) & four-quadrant operation for storage devices	MEMS issues control settings in local or distributed control (or, individual control actions in decentralized control) to DERs on behalf of the operator — control settings can be specifically designed to operate DERs in a constant power-factor mode or generate no reactive power at all during generating hours	Utility provides control settings to the DERs through MEMS
	Volt–Var mode	Local controllers coordinate (in distributed control)/ operate around the control settings (in local control)/ directly follow control actions (in centralized and decentralized control) — DERs operate on all four coordinates — DERs can be specifically instructed to operate in this mode during off-generating hours — can be designed to provide maximum reactive support autonomously during faulted condition	Coordinators may be located within MEMS/ADMS in centralized/decentralized control, or, MEMS/ADMS can provide local controller with set points in decentralized/local control to the DERs — settings provided during emergency condition should be fast — otherwise slow communication channel would suffice	
Frequency Control (FC)	Participation in AGC (multisecond basis)	DERs (under signed agreement by its operator) respond to AGC signal directed to it in a decentralized control — centralized control is not possible due to DERs are not visible to the operator — both frequency, area control error (ACE) and control settings needs to be provided — alternatively, control actions can be directly provided to DERs	MEMS/ADMS redirects AGC action in microgrid/grid-connected mode — AGC command comes from the operator in the grid-connected mode & calculated locally in the islanded mode — post-islanding, if DERs remain connected to the local distribution utility, the AGC settings are provided by ADMS, else it will come from MEMS	
	Mitigate fast frequency deviations (sub-second basis)	If registered, local controllers autonomously take decisions based on communicated droop settings in local control — the central controller can also communicate control actions directly to DERs	The droop and other control parameters are calculated by MEMS/ADMS based on individual DER ratings — operational bottleneck and fluctuating system inertia will require these parameters to be frequently updated (update frequency is slow-enough compared to requisite control action)	
Anti-Islanding protection (AI protection)	Passive Measurement-based Approach	Local DERs connects/disconnects the DERs based on discrepancies in the local measurements — in another scheme, local controller continuously monitors signal of certain frequency-band in the PLC and connects/disconnects based on the availability of the said signal	ADMS issues set points and updates them frequently based on system condition	
	Active Measurement-based Approach	Local DERs inject disturbances and respond to the resulting discrepancies in the local measurements	MEMS/ADMS continuously provides set-points to prohibit the DERs from injecting certain signals into the grid to avoid the system to go into instability when the system is in healthy condition	
	Direct Command-based Control	DERs connect or disconnect based on higher level command — no local monitoring and control are required	ADMS continuously observes recloser positions — following an event broadcasts the DER controllers to take action	
Switch from Grid Connected and Microgrid Mode and vice versa (G2MG/MG2G)	Detect and operate within an islanded microgrid and connect back once healthy condition is established	Disconnection of DERs is coordinated by other DER functionalities, such as, V/FRT and AI protection — higher level entities (MEMS) should coordinate the reconnection of DERs into the grid	Set points for the utilized functionalities V/FRT and anti-islanding protection schemes comes from this layer — MG2G scheme is always supervised by hierarchically upper layer management systems, ADMS/MEMS	
Voltage/Frequency Ride Through (V/FRT)	Ensure DERs remain connected following voltage or frequency events	Local DERs not only required to remain connected during voltage and frequency excursion events, but also provide fast VAR support (operate in a volt–var control mode) while limiting real power injection to limit feeding to the faults	VAR support control signal, maximum power injection limits and duration of remaining connected into the grid to be periodically updated by ADMS/MEMS	

IEEE 2030.5 protocol-based communication system for smart grid are underway. Implementation status of one of such projects can be found in [120]. The development of a testbed utilizing IEEE 2030.5 for cyber–physical security analysis is discussed in [121].

3.2.2. IEEE 1815:DNP3

The standard protocol IEEE 1815 enables real-time communications for DERs [122]. In this regard, DNP is specifically developed for the transmission of data and control messages, which is also capable of working in the low-speed channel. It is a master–slave protocol where the master reaches out to the slaves regularly, while also enabling slaves to initiate communication for fast data exchanges when required. DNP3 is originally developed for serial communication, but it is evolving to work in IP interface at high speed. Some of the features of DNP3 are data timestamp, message broadcasting, data clustering, setting quality flag and report-by-exception. These features make DNP3 popular for SCADA applications, and IEEE recognizes it as one of the standard protocols for rapid communication with DERs. A testbed utilizing IEEE 1815:DNP3 communication protocol for the energy storage management system application is proposed in [123].

3.2.3. IEC 61850

IEC 61850 utilizes object-oriented abstraction of data items and functions for different communication nodes by creating data/function objects to be transmitted over the communication network. It constitutes of a hierarchical architecture, accounts for communication requirement for the DERs in its information model. In this regard, [124] discusses application of IEC 61850 for DERs. The review of the IEC 61850 protocol to satisfy the new needs of the smart grid is considered in [125]. The microgrid protection system is modeled by utilizing logical nodes based on IEC 61850 in [126].

3.2.4. Modbus

Like DNP3, the Modbus is a master–slave communication protocol. It is widely used in the industrial control system due to its simplicity, speed, efficiency, and reliability. SunSpec Modbus is an implementation of Modbus that enables efficient implementation of communication protocols, while standardizing the vendor-independent application developing process, enabling interoperability. While its original version was implemented in the serial network, Modbus TCP works over IP network. However, for the deployment of this standard in the integration of DERs, one must be aware of its lack of security features. The development of the testbed with Modbus TCP for the voltage control is discussed in [127]. In [128], this protocol has also been implemented to show its efficacy in the DERs communication.

3.2.5. OpenADR

Open Automated Demand Response (OpenADR) is first developed as a research project to support California's energy policy objectives, and, there is a notable research thrust around it [129–131]. While the OpenADR requires gateway devices such as EMS or aggregators for interfacing the utilities with DERs, IEEE 2030.5 can directly connect to the DER controllers. Nevertheless, OpenADR ensures a high-security level for the communication, while allowing flexibility of information model. Furthermore, this communication protocol provides a communication interface between utilities, aggregators, and DERs.

4. Vulnerabilities and threats

One of the key points that can be observed in the discussion on DER standard communication protocols is that these protocols often lack security features, making their use cyber-vulnerable. This section will discuss various cyber vulnerabilities, types of attack, and, consequently, the defense mechanisms. The risks of several DER functionalities are also compared and contrasted.

4.1. Fundamentals of cyber security

Confidentiality, Integrity, and Availability (CIA) are the three primary pillars for analyzing the cybersecurity of a cyber–physical model [132]. The objective of any security-related policies, standards, and guidelines is to obtain the corresponding CIA. Therefore, the security of the DERs' communication infrastructure needs to be corroborated by these factors. Furthermore, the CIA of a cyber–physical system can be handled using the AAA framework that constitutes of Authentication, Authorization, and Accounting [104]. In this segment, the triad of the CIA model is introduced.

Confidentiality indicates the situation, where, access of unauthorized individuals to confidential and privileged information is prevented [133]. Primarily, access control and encryption are the security mechanisms that are employed to ensure confidentiality. Under the AAA framework, confidentiality relies on authentication, which is utilized to confirm the entities' identity and ensure that only permitted entities are granted encrypted information using the confidential keys. Authentication without encryption can suffer from eavesdropping attacks [104]. Additionally, entities' authorization to execute actions is generally regulated by access control. In view of authorization control, users are typically divided into various categories for restricting their access according to assorted privilege levels [104].

Integrity refers to the protection of cyber–physical systems and their associated data flows against malicious modifications or harms [133]. Multiple mechanisms and approaches, including the provision of mutual exclusion mechanism, error detection, correction of file systems, cyclic redundancy checking (CRC), Hardware RAID, checksums, and hash functions, ensure the integrity of a system [104].

Availability refers to granting permanent and reliable access to information by the eligible individuals [133]. Availability is conventionally enhanced by proper analysis, design, implementation, redundancy, and configuration of a system or network [104].

4.2. Threats and vulnerabilities in the DER interfaces

Miscellaneous factors that threaten the desirable operation of DER interfaces are reviewed in this subsection. These factors can be categorized into two groups. The first one concerns the system-driven factors that are related to managerial issues. The second group discusses the use of technical solutions to amend the limitation of the existing security mechanisms.

4.2.1. System driven factors

1. **Lack of Direct Supervision:** The owners primarily operate DER systems without direct supervision [106,134,135].
2. **Lack of Customers Security Expertise:** The customers, who often do not have enough security expertise, must be allowed to adjust the requisite configuration on DERs. This escalates the security vulnerabilities [106,134].
3. **Increasing Reliance on Fast Communication:** The widespread use of DERs interfaces leads to the growth in the required connections and attack entry points [106].
4. **Different Available Communication Protocols and Standards:** As discussed earlier, although various communication protocols exist that are suitable for DERs' communication, not all of them encompass built-in security features. Moreover, existence of multiple standards and their widespread use make it difficult to select the best practice [106]. Furthermore, the lack of standardized operating procedures creates misunderstandings, often leading to imprecise actions, improper situational response, and confusion during emergencies [117].
5. **General Lack of Expertise:** Lack of proficient experts in both DER functionality and cybersecurity engenders poor judgment on requisite actions [106,117]. This increases the number of incorrect settings adjustment on DERs that can significantly lessen the security [117].

6. **Several Functionalities:** DER interfaces can support a wide range of functionalities. Inappropriate configurations over these functionalities can significantly increase the security vulnerabilities [106]. Moreover, the availability of such a large number of functionalities sophisticates the system analysis [117].
7. **Utilization of the Public Internet:** Unlike bulk generators, DERs are commonly interfaced through public internet network [136], increasing the system's attack surface.
8. **Inability to Detect Loss:** The inability of DERs to detect the loss of grid, typically, results in safety issues, uncertainties, and emergency conditions. For example, DER systems must be disconnected upon islanding detection. However, their traditional anti-islanding mechanisms may fail to detect power loss because of the interference of other DERs functionalities [117].

4.2.2. *Limitation of existing security mechanisms*

1. **Insufficient Protection against Backdoor Access:** DER vendors typically reserve a communication endpoint or keep certain port open for future updates and maintenance. Nonetheless, this backdoor port exposes the DER-interface software to external cyber-threats [117].
2. **No Encryption:** Inadequate processing capabilities in remote DERs prevent implementation of some conventional security mechanisms such as encryption [136].
3. **Poor Password Management:** After a grid emergency, utility operators need to access DERs remotely and handle the operations to avoid network collapse. The operator may fail to access the DER interface upon unavailability of the password [117].
4. **Poor Certificates Management:** Certificate necessitates being renewed prior to the expiration regularly. If a system does not meet this requirement, DERs will stop responding to the coordinators' commands [117].
5. **Software Updates and Patches Management:** Inadequate validation, checks, and tests before the software and patches update, pave the way for attackers to inject malicious codes into them.

4.3. *Attacks*

The cyberattacks on DERs can have tremendous impacts on their cyber–physical functionalities. As discussed before, although, increasing modern DER systems' reliance on communication interfaces enhances the system's operation remarkably [137], this usually increases attack surface from the security point of view [138,139]. Attackers can potentially target various operating modes of DERs, which result in a diverse range of physical ramifications. For example, an attack to deviate the set-point from the unity in the constant power factor mode possibly leads to increasing system loss and create voltage regulation issues. In the active power mode, fabricating the upper limit of DER's allowed active power, results in a mismatch between power consumption and scheduled generation and affects the grid's frequency. By the same token, manipulating the DERs' scheduled injected reactive power destabilizes voltage magnitude [140]. Likewise, network voltage can be compromised through modification of voltage-reactive droop curve in (volt–var) mode or similar setting in (volt–watt) mode. Furthermore, if the attacker manipulates characteristic curve in active power-reactive power (watt-var) mode of DERs, it might lead to disconnection of corresponding DERs. Compromising frequency droop (frequency-watt) mode degrades frequency and it might result in frequency collapse [95,141]. The side effects of these attacks can also be magnified provided that the attacker gains access over the multiple operating modes of DERs [142].

In the following paragraphs, various attack types are discussed.

4.3.1. *Network reconnaissance:*

The initial phase for an attacker to acquire the knowledge about the cyber–physical system is network reconnaissance [143]. The adversary can utilize different tools such as Nmap and OpenVAS, to gather information about the DER-interfaces, like, open ports, various services running on the devices, IP, MAC addresses, operating services, etc. [144].

4.3.2. *Eavesdropping:*

Eavesdropping is known as a passive attack where an attacker attempts to obtain legitimate data and information about the system. This data is subsequently used for other cyberattacks or malicious objectives [95,141,145].

4.3.3. *Packet replay:*

Packet replay targets the data transmission in a communication network. In this attack, data packets among DER client applications and the devices are recorded by an adversary. Then, the packets are altered with malicious code, and eventually are re-transmitted. The primary purpose of this attack is to introduce a delay in the communication [95,141]. An example of this attack is presented in [144]. TCP/IP-based communication can decrease the DERs' vulnerabilities from packet reply cyberattack [143,145]. This is the result of a three-way handshaking method implementation in TCP/IP protocol, which means the attacker requires access to the unique session ID generated during an initial three-way handshake by DER devices.

4.3.4. *Spoofing:*

In the spoofing attack, an adversary utilizes fake security certificates to falsify the ownership of public keys. By acquiring unauthorized access over public-key certificates, an attacker can expand their unauthorized access to DER system services and initiates future attacks [95,141,145].

4.3.5. *Man in the middle (MITM):*

MITM attack in the DER system refers to the modification of communicated data between the DER devices and client applications where confidentiality and integrity of the data are targeted and can lead to modification or deletion of the data. One way an adversary can implement the MITM is through eavesdropping on communications among the DER clients and the devices [95,143,145,146]. Detailed explanations along with examples can be found in [144,147,148].

4.3.6. *Denial of Service (DoS):*

DoS is a type of attack in which an adversary disrupts legitimate users' access by occupying the resources or communication bandwidth. This attack leads to severely increased latency of legitimate users, disruption of information flow, and intermittent connections that impact the availability of the communicated data linking the DER applications and devices. This attack is applied by overwhelming the DER device's open ports with injecting abnormal fast traffic continuously [117,143–145]. Detailed example of the DOS attack are presented in [95,149].

4.3.7. *Modified firmware upload:*

This attack targets the authentication and integrity of updating the firmware of DER embedded systems to corrupt the DERs' functionality with injecting malicious codes into the firmware of the DER interface [143]. It is typically performed through a telnet session or FTP.

Table 3
Direct impacts of attacks on Confidentiality (C), Integrity(I), and Availability (A).

Attack	C	I	A
Network Reconnaissance	✓	×	×
Eavesdropping	✓	×	×
Packet Replay	×	✓	×
Spoofing	×	✓	×
Man in the middle	✓	✓	×
Denial Of Service	×	×	✓
Modified Firmware Upload	×	✓	×
Maintained Logs per device	✓	×	×
Password Handling	✓	×	×

4.3.8. Maintained logs per device :

Appropriate and precise logs facilitate the process of attacks or security events monitoring on the DER interfaces. Commonly, a log captures various features of the devices, including but not limited to the external connection of devices, self-test summarization, modification on DER configuration notice, and grid situation. Logs can provide accurate information about the events, along with the date and timestamp, type, and source of the event. Archiving the logs is inescapable considering memory efficiency requirements. Failing to provide appropriate access control for data log can induce large security ramifications [143].

4.3.9. Password handling:

Exchanging password in a plaintext format among DERs is prone to the password handling attack. Intruders can take advantage of obtained access for unauthorized login and manipulate of the operational configuration of the DER devices [143].

In this regard, Table 3 analyzes the impact of various attack types based on the CIA triad. The attacks on confidentiality can be the precursor for attacks on integrity and availability. Also, compromised integrity can lead to an attack on availability.

5. Cyberattack and defense mechanisms

Grid resilience and *cybersecurity* of the cyber-power system are two key phrases that have recently acquired significant attention from policy-makers in the energy sector. Here, the grid resilience is about proactive prevention of the critical infrastructures from physical damage, if feasible, and faster recovery, and is primarily enabled by the DERs. However, coordination requirements of the large fleet of the DERs in a smart grid make them prone to cyberattacks [117,150]. Increasing cyber vulnerabilities can also have a negative impact on the recoverability of critical infrastructure, following a disaster.

The techniques and standards that enhance grid resiliency by improving the system's capabilities against cyber-attacks are presented in this section.

5.1. Techniques and best practices

The techniques to lock down access to the information (through the utilization of encryption of device-level information, authentication based access to the devices, encrypted communications, enforcement of security through utilization of various protocols, and continuous monitoring) have severe limitations. Locking down the access to the devices is mainly reactive. Moreover, finding the security holes are beyond the capabilities of an organization, leading us to the slower deployment of patches. The use of these advanced security-enforcing techniques is also computationally expensive due to extensive memory, processing requirements, and networking overhead [136]. A description of various security techniques that defend the system against cyberattacks are detailed as follows.

SM1 The use of cryptography can encrypt data exchange, thus limiting transmission of information as plain text [143]; enforcing confidentiality [104]. However, the large computational requirement will add processing delays [140,146] of applications embedded within DER-devices, while significantly increasing deployment expense. The use of selective encryption can solve both of these challenges [151], considerably reducing communication latency.

SM2 While encryption can protect the confidentiality of the transmitted message, it cannot ensure the immutability of transmitted messages. The use of mechanisms, such as Message Authentication Codes through cryptographic control, can guarantee the integrity of the transmitted data [151]. The use of Message Authentication Codes for DER communications are presented in [140,145].

SM3 Access Control Lists (ACL) are developed to limit access to the systems' entities [104,117]. Role-based access controls can be used to strictly enforce access to the resources of a system [136,146]. This way, one can ensure that access to a specific database or application remains limited to authorized users. Furthermore, in a role-based control, only predecided finite set of user with particular objectives are allowed application access. The use of ACL to access information from advanced metering infrastructure is presented in [152].

SM4 Network Address Translation (NAT) can isolate the external entities from direct access to the DER-devices [104,117]. In this regard, [151] recommends locking down each DERs using a .252 sub-net mask. Refs. [153–155] suggest the use of NAT for the DERs.

SM5 Intrusion monitoring is one of the key requirements to detect the presence of malicious and illegal traffic and prevent them from accessing DERs devices [156,157]. Both Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) can help us in this regard [140], and IPS specifically blocks and prevents additional traffic from suspected IP address from accessing DERs [104,117,146,151].

SM6 Network segmentation using multiple VLANs can prevent direct access among Operational Technology (OT), Information Technology (IT), and management networks by building an air gap [151]. This approach can be utilized as a security mechanism for DERs [142,158,159].

SM7 In addition to monitoring network traffic, one needs to maintain traffic and action logs to enable the intrusion detection system or operators to detect anomalies in the operation of the DERs [140, 160].

SM8 As indicated, due to the reactive nature of security updates, networked software and applications are required to be regularly patched [151], to prevent the entire system from security vulnerabilities. Continuous patching enhances the protection of DER-devices against DoS and least privilege attacks [141]. Needless to mention, the source of these security updates and patches is required to be certified to avoid further security ramifications, such as malware injection [161].

SM9 All the unused ports must be disabled or secured to eliminate unauthorized access to the DERs [151]. This can be implemented by deploying firewalls, where only white-listed entities are allowed to access specific ports [140].

SM10 Transport Layer Security (TLS) guarantees the availability of a secure and reliable communication link among connected hosts. Use of TLS for communication among DERs can help our system to remain protected against MITM, eavesdropping, replay, spoofing attacks, etc. [95,141,151].

SM11 For the establishment of a secure connection, multiple Certification Authorities (CA) enables the capability to check certificates to authenticate the user. If a connection is established using an expired certificate, the certificate will be moved into the

Certification Revocation List (CRL) [145,151], and the session will be terminated. Furthermore, enforcement of session time-out policies ensures the capability to lock the connection beyond a certain period of no-activity [104].

SM12 The use of TELNET must be entirely stopped and need to be upgraded to the latest version of sTELNET for remote logins. The use of sTELNET in DER applications are suggested in [143,162,163].

SM13 The use of FTP must be upgraded to be used in conjunction with SSL [143,162,163] for enhanced security.

SM14 Since the exchange of passwords is a standard way to verify an user's authenticity, the exchange of passwords as plain text should be prohibited, and password exchange is also required to be secured for all DER users. Furthermore, the use of a password of sufficient length and complexity can prevent a malicious attacker from gaining access privileges [95,140]. These credentials can also be used to ensure privileged access to specific users [143].

SM15 Popular belief is that the use of a firewall can diminish the impacts of DoS attacks and prevent unauthorized access to the network, where, DERs are connected [143,146,164]. To properly utilize the benefits of firewalls during the DoS attack, in-line blocking devices can be used to supervise network traffic type and directions [140].

SM16 The MAC address of the DER devices and requisite port access needs to be locked to prevent access to unauthorized traffic [143].

SM17 The implementation of AAA (Authentication, Authorization, and Accounting) framework can help us to secure the communication among DER devices [143].

SM18 The principle of least privileges refers to limiting the access of information and resources for each of the modules (depending on the subject, it can be a process, a user, or a program) to its bare minimum value. Such a limited access can improve the security of a network system significantly [140]. Furthermore, if a module does not require access to a certain resource for its legitimate task anymore, access to it must be revoked [104,143,165].

SM19 Every IP packet in DER must be authenticated and encrypted. Moreover, each session should be initialized using mutual authentication [117].

SM20 The VPN (Virtual Private Network) generates a tunnel across the network, encrypts the entire IP packet, and encapsulates it. VPN improves the security of the network significantly [117,164]. The use of VPN in DER communication is recommended by [11,143,166].

SM21 The risk of unauthorized access reduces significantly if multi-factor authentication is used, and therefore, it is highly recommended in the literature to be used for accessing to DER services. In this regard, simultaneous implementation of two out of three of the following mechanisms is suggested [140]: 1) knowledge assessment (through passwords), 2) inherent assessment (through biometrics features), or 3) possession assessment (through token).

Categorization of these techniques for ensuring secure access to the DER devices, based on the CIA triad, is provided in Table 4.

Table 4
Impacts of each security mechanism (SM) on Confidentiality (C), Integrity(I), and Availability (A)

CIA	Security mechanisms
Group 1- Confidentiality	SM1, SM11, SM14, SM21
Group 2- Integrity	SM2
Group 3- Confidentiality + Integrity	SM3, SM5, SM9, SM10, SM12, SM13, SM17, SM18, SM19, SM20
Group 4- Confidentiality + Integrity + Availability	SM4, SM6, SM7, SM8, SM15, SM16

5.2. DER resiliency

Under the resourcefulness, robustness, and recovery characteristics framework, the resiliency of infrastructure can be defined based on avoidance of the operation failure, or minimization of service breaks during and after the unforeseen precarious events [167]. Resiliency can be improved in two stages: 1) avoid and mitigate, and 2) response and recover. Improved system resiliency can prevent or limit the impacts of the adverse actions, provide robust infrastructure design to lessen and restrict the impact of an unpredictable unfortunate event, and, have resource sufficiency for faster recovery into normalcy. Alternatively, resiliency can be defined by the responsiveness of a system following an unexpected event to minimize its ramification. The following points, based on [168], are essential for the resiliency management of the network with DER-devices.

- The risk assessment of the products and services of each stakeholder is required to be carried out. This includes: (i) recognizing the threats that can infect certain services and products, (ii) understanding the vulnerabilities of those, (iii) evaluating the likelihood of the threats, and (iv) identifying the impacts on each product and services.
- Possible technological mitigation mechanisms to cater to those threats.
- Cost–benefit analysis: balancing the impact of threats against the implementation cost of mitigation solutions.
- Coordinating stakeholders to deploy the recommended mitigation solutions.

The impact of threats, as described in [168], can be evaluated based on the following parameters:

- **Safety Impacts:** As discussed in Section 2, DER devices should not remain energized following the grid's unavailability to which it is connected. If not satisfied, this may pose threats to the repair personnel, or lack of synchronization can lead to the failure of the grid to which the DER is to be connected.
- **Power Outage Impacts:** Prolonged outage following distribution system infrastructure damage can lead to severe financial damages to business and residential customers.
- **Power Quality Impacts:** Rapid voltage and frequency excursion can significantly damage and/or reduce DER devices' lives.
- **Financial Impacts:** The financial implication of the low-probability events can be multitude. The customers will not only lose business opportunities, but the cost of infrastructure destruction can also be high, burdening the entire society.
- **Environmental Impacts:** Each of the existing infrastructure contains a certain carbon footprint, destruction of which requires redeployment increasing carbon-footprint for the entire society. Often requisite deployment of diesel generators as a means of rapid recovery also increases carbon footprint.

Increasing reliance of the distribution network on the communication network with increasing penetration of DERs makes them vulnerable to physical and cyber-attacks. Therefore, the attack-resilient framework constitutes several layers, including the cyber (communication) layer, physical (device) layer, and management/supervisory layer. For effective management of the network, attack prevention, attack detection, and attack response for all these layers needs to be addressed [134]. The mitigation strategies of the unforeseen threats rely on both engineering and cyber solutions, and neither of these solutions alone can solve all the challenges.

5.3. Security mechanisms of the communication protocols

In this section, the discussed protocols in Section 3 are reviewed from the security standpoint. Additionally, various mechanisms for the enhancement of security are also discussed.

5.3.1. Modbus

Being a royalty-free open-protocol, the use of Modbus protocol in the industry is wide-spread. Primarily, the Modbus protocol does not come up with any baked in cybersecurity standard [169]. The lack of security mechanisms makes this protocol vulnerable against several kinds of attacks, such as DoS, MITM, and replay attacks [170]. For example, a lack of encryption leads the information exchange as a part of this protocol in the form of plain text. Consequently, this protocol suffers from the lack of confidentiality. Furthermore, the Modbus protocol does not have any integrity checks such as Message Authentication Codes validation. Thus, it is impossible to determine whether a message has been altered within the communication channel [171]. Nevertheless, an attacker can flood the bandwidth with crafted packets leading the assets unable to communicate. Therefore, this protocol cannot ensure the availability of the communication interface [171]. Lack of authentication requirement also facilitates an external adversary to communicate malicious messages for execution [172].

However, due to its popularity, several mechanisms have been developed over the years to ensure the possibility of secure communication across the network assets. Several encryption algorithms for establishing a secure communication channel can be found in [173–175], thus ensuring authentication against unauthorized command execution. Use of external devices for the encryption and decryption of the network traffic [104] utilizing bump-in-the-wire (BITW) encryption technologies [176] can ensure confidentiality of Modbus protocol. The use of TLS to provide secure communication in the Modbus protocol is presented in [177]. Furthermore, provisioning of Hash-Based Message Authentication Codes validation for secure Modbus communication is presented in [178], ensuring integrity. Also, the use of SHA2, as developed in [170], also ensures integrity. Furthermore, several other works utilizing IDS and IPS to provide secure communication for Modbus protocols can be found in [171,179–182].

5.3.2. IEEE 2030.5

According to IEEE 2030.5, five mandatory function sets, such as certificates, device capabilities, discovery, secured HTTP, and time synchronization, are required to enable the secure exchange of messages. This protocol uses TLS 1.2 for secure communications over the network [104]. TLS provides message authentication and encryption using the AES-CCM [183] algorithm. The exchange of digital certificates as a part of TLS ensures authentication [117]. Additionally, as a part of IEEE 2030.5, access control lists exist for every resource to permit using them based on the authentication level. Furthermore, a registration list also exists to validate users for authorized access to the clients. Access to each of the devices are based on the three credentials, short and long form device identifiers, and a 6-digit pin code. The built-in authentication and authorization mechanisms provide secure access to the resources/devices [184]. Also, IEEE 2030.5 utilizes native IPv6 for addressing the internet devices [185]. For devices with adequate hardware resources, it is possible to implement additional security mechanisms.

5.3.3. IEEE 1815 (DNP3)

The DNP3 protocol can provide secure authentication in both master and outstation application layers. This addresses the challenges of multiple security threats, including spoofing, firmware modification, eavesdropping on exchanges of keys, and ensuring non-repudiation. Ability to limit the connection based on specific IP-addresses, or address range, while incorporating higher-level security layer validation features helps protect DER-devices against the condition where multiple devices are simultaneously trying to connect to the same device, which may result in data loss or unintentional command execution [122]. While IEEE 1815 (DNP3) can utilize TLS to secure DER communications, the TLS support is not a necessity. Furthermore, the current revision of the DNP3 protocol ensures end-to-end application layer encryption [104].

However, there are numerous ways the security of the smart grid deploying DNP3 protocol for real-time communication can be compromised [186–189]. Among them, evaluation of the impact of Reconnaissance, Replay, and MITM attacks on different layers of the communication network deploying the DNP3 standard is discussed in [190].

DNP3-SA: DNP3 Secure Authentication (DNP3-SA) is a protocol layer introduced between the application and transport layer of the IEEE 1815 (DNP3) protocol. DNP3-SA creates a secure communication session utilizing Message Authentication Codes, ensuring authentication and integrity of communication. Furthermore, the Authorization Management Protocol (AMP) is developed to be used alongside DNP3-SA to centrally manage the devices' ability to communicate with each other [191,192].

5.3.4. IEC 61850

Although like the Modbus protocol, there is no inherent security feature in the IEC 61850 protocol, and it merely describes the information model for communication among the DER devices, this protocol can utilize other communication protocols, such as Manufacturing Message Specification (MMS), Generic Object Oriented Substation Event (GOOSE) that provides flexibility in communication among DER devices. Moreover, DERs utilizing the IEC 61850 protocol for communication can utilize security features described in IEC 62351. In this regard, security features provided by IEC 62351 includes security profiles of TCP/IP, MMS protocol, secured network and system management, key management, role-based access control, and architectural security [104]. The security features are selected based on the application requirement.

The impact of different kinds of cyber-attacks on the communication network utilizing IEC 61850 can be found in [147,193,194]. The use of different hash functions, including MD-5, SHA-1, and RSA for the integrity of communication, is prescribed in [195]. Categorization of the impact of DoS, password cracking, and eavesdropping attacks on the network utilizing IEC 61850 is discussed in [196].

5.3.5. OpenADR

As defined by the NIST standard for cybersecurity, OpenADR [197] provides a guideline to ensure the confidentiality, integrity, authentication, and message-level security requirements [104]. OpenADR 2.0 embraces existing common security mechanisms (such as, TLS). This protocol also utilizes Public Key Infrastructure (PKI) certificates (Use RSA or ECC algorithms for PKI certificates). It adopts an open architecture [198] framework, and its applicability is not limited to any specific DER technologies [197].

Multiple levels of security exist for OpenADR 2.0. *Standard* security employs TLS for providing secure communication channels. *Higher* security level additionally utilizes XML signatures for providing non-repudiation for documentation purposes [197]. Various literature for the evaluation of the security of OpenADR can be found in [131,199,200].

Based on our discussion, security mechanisms for protecting the DERs against various kinds of attacks with different communication protocols are described in Table 5.

Table 5
DER Communication protocols' security mechanisms.

Protocol	Modbus	IEEE 2030.5	DNP3 (DNP3-SA)	IEC 61850*(described in the IEC 62351)	OpenADR
Confidentiality	×	Encryption using HTTPS	using TLS (optional)	IEC 62351-9: Key Management	PKI algorithms (RSA or ECC)
Integrity	×	Message Integrity using HTTPS	use key encryption to keep session keys secure. DNP3-SA use Message Authentication Codes	IEC 62351-3 to 7: Security for TCP/IP, MMS, Peer-2-Peer, and network and system management (use TLS)	using TLS and XML signatures
Availability	×	×	×	×	×
Authentication	×	using HTTPS/certificate	in Application Layer	IEC 62351-3 covers authentication	Using PKI certificates
Authorization	×	registration list/certificate	provided by AMP	IEC 62351-8: Role-Based Access Control	×

5.4. Major standards and guidelines for cybersecurity enhancement for the DERs

5.4.1. NIST

Over the years, NIST has provided various cybersecurity standards. For example, the NIST 7628 [201] presents an analytical framework to develop an effective cybersecurity strategy of a smart grid. NIST SP 800-82 [202] provides us with the guidelines to enable a secured operation of an industrial control system, while ensuring that the system operates reliably.

5.4.2. NERC/FERC

While the typical cybersecurity enhancing NERC standard is developed mainly for the bulk power system [203], as recommended by FERC, some of the recommended practices can be suitably adapted for the enhancement of DER-devices along with distribution networks [204].

5.4.3. IEC

IEC 62351 standard [205] has mainly been developed to bridge the security challenges that remain unaddressed by other standards. Therefore, it incorporates the best security practices for information exchange in the power systems. The focus of this standard is to enhance the security of the communication network, and address the challenges of the different types of communication, such as, end-to-end communication [206].

5.4.4. IEEE

IEEE standard 1547-2018 is the main cybersecurity-related standard for DERs. Other IEEE standards for DER integration include IEEE C37.240 (cybersecurity requirements of substation automation, control and protection devices) [207], IEEE 1686 (capabilities of intelligent electronic devices for cybersecurity enhancements) [208], and IEEE 1711 (protection of SCADA interface from cyber vulnerabilities) [209].

5.4.5. IETF

While the primary scope of the Internet Engineering Task Force (IETF) is to develop standards for the effective management of the internet-connected devices [104], some of these standards are relevant to cybersecurity improvements. These standards gain additional significance with the integration of intelligent electronic devices (IEDs) in a smart grid. In this regard, the best utilization methodology of Internet Protocol Suite technologies for the smart grid design in an IP-based infrastructure is discussed in IETF RFC 6272 [210]. Other standards for cybersecurity enhancements can also be deployed to improve the security of the DER-device interfaces.

5.4.6. DOE

Two documents, desirable for the development of (i) a mechanism to evaluate the security capabilities, while prioritize and improve the cybersecurity capabilities of electricity subsector devices [211], and (ii) risk management process based on current best practices in regulatory requirements, various threat-definitions, and organizational policies, while considering future challenges [212], are developed by the Department of Energy.

6. Cessation and future trends

6.1. Summary

This paper provides a comprehensive review of control schemes, given by centralized, decentralized, distributed, and local control with increasing renewable DERs for a sustainable grid, as well as, associated communication requirements, cyber–physical vulnerabilities and defense mechanisms. These high-level control schemes were compared against various parameters to identify associated strengths and weaknesses in terms of their deployability (see Table 1). The utility of these control schemes to satisfy several functional requirements by the DERs are also detailed. Here, our objective was limited to the control applications that extensively require fast communication network, only to judge later the cyber–physical vulnerabilities introduced by such communication requirements. Our discussion was limited to monitoring, voltage control, frequency control, and other emergency control actions, requiring fast communication interface. We discussed anti-islanding detection and protection strategies and V/FRT techniques among various emergency control actions. The impact of power-system harmonics and its impact on communication lines were also discussed. This gains immense importance in the future power grid with the high-penetration of converter interfaced devices. Based on the discussed extensive control requirements, a typical facility microgrid hierarchical control architecture was also presented (see Fig. 3). Dependence of various control layers for different control objectives are also discussed (see Table 2).

Next, the existing DER system architectures were reviewed. Here, we stressed on a three-level system architecture and discussed how such an architecture (see Fig. 4) could satisfy the communication requirement of the future grid. The location of diverse decision-making entities in such system architecture and how miscellaneous controllers communicate with each other and central decision-making entities are also inspected. Subsequently, we reviewed DER communication protocols (IEEE 2030.5, IEEE 1815:DNP3, IEC 61850, Modbus, OpenADR) that can lead our desired DER communication system architecture into reality.

Typically, the security mechanisms used for standard DER communication protocols are analyzed based on CIA triad, and the CIA can be handled using the AAA framework. We have also discussed the various administrative factors and limitations of existing security

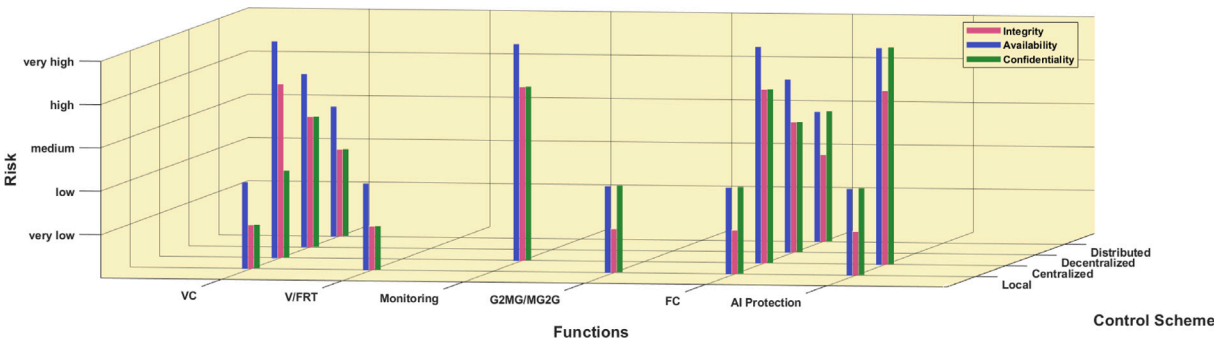

Fig. 5. Summarizing of DER functions, control schemes and security risk based on CIA.

Table 6
Security mechanisms of each protocol against the attacks: provided(✓)/partial mechanism (✓)/no security mechanism (×)

Attack/protocol	Modbus	IEEE 2030.5	DNP3 (DNP3-SA)	IEC 61850
Network Reconnaissance	×	✓	✓	✓
Eavesdropping	×	✓	✓	✓
Packet Replay	×	✓	✓	✓
Spoofing	×	✓	✓	✓
Man in the middle	×	✓	✓	✓
Denial Of Service	×	×	×	×
Modified Firmware Upload	×	✓	✓	✓
Maintained Logs per device	×	✓	✓	✓
Password Handling:	×	✓	✓	✓

mechanisms, creating vulnerabilities in the DER interfaces. Given the existing DER interface vulnerabilities, we have discussed different kinds of mechanisms an attacker can resort to. Each of the attack types is compared against the CIA triad (see Table 3).

The cyber defense and security mechanism methods have been discussed next and explained how these mechanisms could prevent cyberattacks. Use of miscellaneous security mechanisms to reduce the cyber vulnerability of the system through CIA-triad is given in Table 4. Based on the security mechanisms that are provided by each communication protocols, protection mechanisms to defend against various confidentiality, integrity, availability, authentication and authorization-based attacks are discussed in Table 5. Table 6 identifies the available security mechanisms for each communication protocol against different cyberattacks. The security features provided by key standard communication protocols have been evaluated, and cybersecurity guidelines and standards have been reviewed.

The risk of the attack can be defined with the combination of attack surface (it has been discussed in cyber resiliency row of Table 1) and impact level of the attack, which depend on the control scheme and the DER's function respectively. In Table 1, the control schemes including local, distributed, decentralized, and centralized, are categorized into very high, high, medium, and low resiliency, respectively. On the other hand, the CIAs are measured for different DER functionalities in terms of high, medium, and low, and is derived from [117]. Subsequently, Table 7 demonstrates the computed risk level based on these metrics, which has been utilized to find out the dependencies shown in Figs. 5 and 6.

Risk levels of various DER functionalities for different control schemes and CIA triad have been summarized in Fig. 5. It is imminent that utilization of a centralized control scheme increases the overall risk in the network. On the contrary, the less communication requirement in the local scheme, the fewer associated cyber risks. However, this scheme extensively relies on the power system model. Furthermore, the utilization of the centralized approach for frequency control notably exposes the smart grid to the cyberthreats. Figs. 6 and 7 illustrate the

Table 7
Security risk level based on surface of attack of control scheme and Impact level of cyber attack for function, qualitative and quantitative score.

Control scheme	Impact Measure on CIA		
Resiliency	Low	Medium	High
Centralized (Low)	Low	High	Very High
Decentralized (Medium)	Low	Medium	High
Distributed (High)	Very Low	Low	Medium
Local (Very High)	Very Low	Very Low	Low

level of impact and recommendation of various attacks and mitigation measures respectively, for different DER functionalities and control schemes. Security mechanisms utilized by different groups, as depicted in Fig. 7, is given in Table 4. It can be concluded from these figures and tables that utilization of distributed and decentralized techniques can reduce severity of cyber risks, while enabling DERs to take advantage of grid situational awareness to regulate their performance.

6.2. Challenges and research directions

Several possible research directions exist for achieving the best security practices regarding DERs integration and thereby reducing cyber vulnerabilities. In addition to general research on cybersecurity, we need to increase our focus on the cybersecurity of industrial control systems, the internet of things, and utility applications, with a special focus on DERs. This stems from the fact that although many of the traditional security features can be easily imported for DER application, the criticality of the electricity network imposes a special challenge in the modern world, and security challenges of DERs can be unique compared to traditional IP-connected devices. Furthermore, in an electricity network, all the agents do not get equal priority, while, allowable communication latency over various functionalities can also vary widely. Coordinating numerous minuscule DER devices

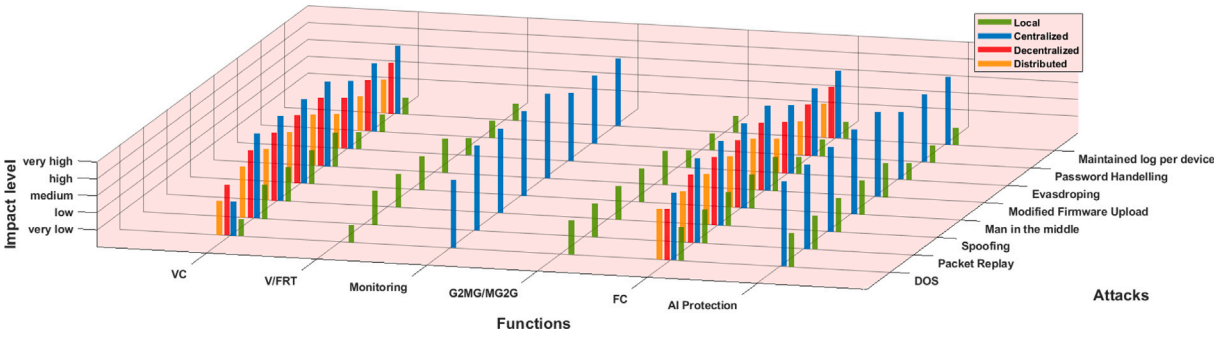

Fig. 6. Summarization of DER functions and cyber attacks for different control schemes.

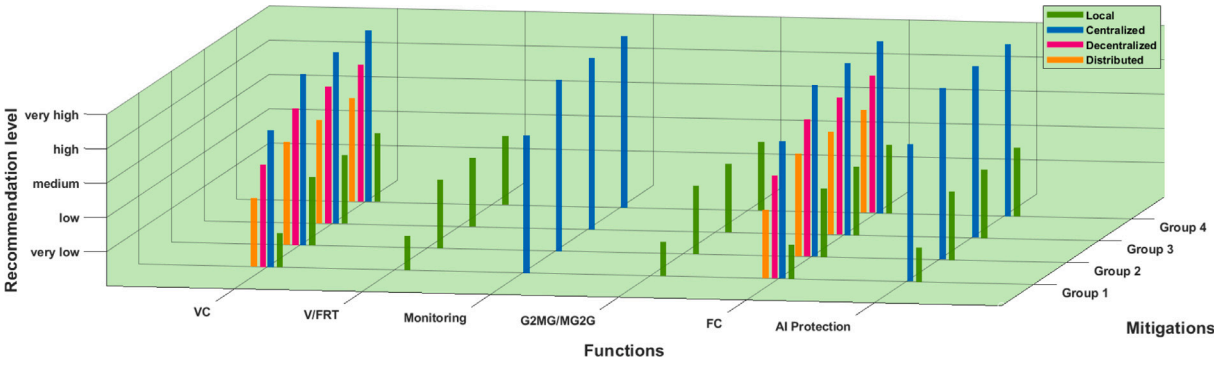

Fig. 7. Summarization of DER functions and mitigation methods for different control schemes.

with various attributes, clustering requirements, and location within the network can be challenging. Moreover, as discussed, not all the DER-operators are e-literate, increasing the vulnerabilities of the system further. Consequently, the impact of human behavior on the improvement of cyber vulnerabilities is required to be studied. This is to be done in conjunction with the development of testbeds to conduct extensive research on identifying key threats and vulnerabilities that challenge DERs security. Security research needs to be in place for the quick deployment of patches. As a conclusion, it can be stated that along with extensive research on reduction of cyber vulnerabilities, comprehensive analysis for DERs integration in cyber-power system will facilitate enabling a sustainable and resilient grid.

CRediT authorship contribution statement

Amirkhosro Vosughi: Conceptualization of this study, Methodology, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] NREC. Distributed energy resources: connection modeling and reliability considerations. Technical report, Atlanta, GA (United States): North America Electric Reliability Corporation; 2017.

[2] Chuvychin V, Sauhatas A, Gurov N, Strelkovs V. Frequency control features for increasing DER penetration in power system. In: 2007 IEEE lausanne power tech. IEEE; 2007, p. 1726–9.

[3] Driesen J, Belmans R. Distributed generation: Challenges and possible solutions. In: 2006 IEEE power engineering society general meeting. IEEE; 2006, p. 8–pp.

[4] IEEE. IEEE application guide for IEEE std 1547(TM), IEEE standard for interconnecting distributed resources with electric power systems. 2009, p. 1–217, IEEE Std 1547.2-2008.

[5] Soyoye OT, Stefferud KC. Cybersecurity risk assessment for california's smart inverter functions. In: 2019 IEEE CyberPELS. IEEE; 2019, p. 1–5.

[6] Sun CC, Hahn A, Liu CC. Cyber security of a power grid: State-of-the-art. Int J Electr Power Energy Syst 2018;99:45–56.

[7] Harvey M, Long D, Reinhard K. Visualizing nistir 7628, guidelines for smart grid cyber security. In: 2014 power and energy conference at illinois. IEEE; 2014, p. 1–8.

[8] Sun CC, Liu CC, Xie J. Cyber-physical system security of a power grid: State-of-the-art. Electronics 2016;5(3):40.

[9] Seal B. Common functions for smart inverters, version 3. Technical report 3002002233, Electric Power Research Institute (EPRI); 2014.

[10] Kotsampopoulos P, Hatziargyriou N, Bletterie B, Lauss G. Review, analysis and recommendations on recent guidelines for the provision of ancillary services by Distributed Generation. In: 2013 IEEE international workshop on inteligent energy systems. IEEE; 2013, p. 185–90.

[11] Howell S, Rezgui Y, Hippolyte JL, Jayan B, Li H. Towards the next generation of smart grids: Semantic and holonic multi-agent management of distributed energy resources. Renew Sustain Energy Rev 2017;77:193–214.

[12] Bravo RJ, Salas R, Bialek T, Sun C. Distributed energy resources challenges for utilities. In: 2015 IEEE 42nd photovoltaic specialist conference. IEEE; 2015, p. 1–5.

[13] Schmitt KE, Canha LN, Antunes MdA, Pereira PR. A smart local voltage regulator methodology for dynamic integration between volt-var control and distributed energy resources. In: 2018 IEEE PES transmission & distribution conference and exhibition-latin america. IEEE; 2018, p. 1–5.

[14] Sun H, Guo Q, Qi J, Ajjarapu V, Bravo R, Chow J, et al. Review of challenges and research opportunities for voltage control in smart grids. IEEE Trans Power Syst 2019;3CSI4(4):2790–801.

[15] Farivar M, Chen L, Low S. Equilibrium and dynamics of local voltage control in distribution systems. In: 52nd IEEE conference on decision and control. IEEE; 2013, p. 4329–34.

[16] Jahangiri P, Aliprantis DC. Distributed Volt/VAr control by PV inverters. IEEE Trans Power Syst 2013;28(3):3429–39.

[17] Tonkoski R, Lopes LA, El-Fouly TH. Coordinated active power curtailment of grid connected PV inverters for overvoltage prevention. IEEE Trans Sustain Energy 2010;2(2):139–47.

[18] Wu D, Tang F, Dragicevic T, Vasquez JC, Guerrero JM. Autonomous active power control for islanded ac microgrids with photovoltaic generation and energy storage system. IEEE Trans Energy Convers 2014;29(4):882–92.

[19] Baker K, Bernstein A, Dall'Anese E, Zhao C. Network-cognizant voltage droop control for distribution grids. IEEE Trans Power Syst 2017;33(2):2098–108.

[20] Chalise S, Atia HR, Poudel B, Tonkoski R. Impact of active power curtailment of wind turbines connected to residential feeders for overvoltage prevention. IEEE Trans Sustain Energy 2015;7(2):471–9.
[21] Wang Y, Zhang P, Li W, Xiao W, Abdollahi A. Online overvoltage prevention control of photovoltaic generators in microgrids. IEEE Trans Smart Grid 2012;3(4):2071–8.
[22] Zhu H, Liu HJ. Fast local voltage control under limited reactive power: Optimality and stability analysis. IEEE Trans Power Syst 2015;31(5):3794–803.
[23] Divan D, Dillon A. Systems and methods for edge of network voltage control of a power grid. 2015, US Patent 9, 014, 867.
[24] Varma RK. Use of distributed generator (DG) inverters as statcoms for decreasing line losses. 2016, US Patent 9, 436, 200.
[25] Dall'Anese E, Bernstein A, Simonetto A. Real time feedback-based optimization of distributed energy resources. 2020, US Patent App. 16/681, 054.
[26] Lin W, Bitar E. Decentralized stochastic control of distributed energy resources. IEEE Trans Power Syst 2017;33(1):888–900.
[27] Sansawatt T, O'Donnell J, Ochoa LF, Harrison GP. Decentralised voltage control for active distribution networks. In: 2009 44th international universities power engineering conference. IEEE; 2009, p. 1–5.
[28] Martínez J, Kjær PC, Rodriguez P, Teodorescu R. Comparison of two voltage control strategies for a wind power plant. In: 2011 IEEE/PES power systems conference and exposition. IEEE; 2011, p. 1–9.
[29] Bahramipanah M, Torregrossa D, Cherkaoui R, Paolone M. A decentralized adaptive model-based real-time control for active distribution networks using battery energy storage systems. IEEE Trans Smart Grid 2016;9(4):3406–18.
[30] Muthukaruppan V, Baran ME. Implementing a decentralized volt/VAR scheme on a smart distribution system. In: 2020 IEEE power & energy society innovative smart grid technologies conference. IEEE; 2020, p. 1–5.
[31] Zeraati M, Golshan MEH, Guerrero JM. Distributed control of battery energy storage systems for voltage regulation in distribution networks with high PV penetration. IEEE Trans Smart Grid 2016;9(4):3582–93.
[32] Li B, Chen M, Cheng T, Li Y, Hassan MAS, Ruilin X, et al. Distributed control of energy-storage systems for voltage regulation in distribution network with high PV penetration. In: 2018 UKACC 12th international conference on control. IEEE; 2018, p. 169–73.
[33] Golsorkhi MS, Shafiee Q, Lu DDC, Guerrero JM. Distributed control of low-voltage resistive AC microgrids. IEEE Trans Energy Convers 2018;34(2):573–84.
[34] Mahmud N, Zahedi A, Rahman MS. An event-triggered distributed coordinated voltage control strategy for large grid-tied PV system with battery energy storage. In: 2017 australasian universities power engineering conference. IEEE; 2017, p. 1–6.
[35] Huang S, Wu Q, Guo Y, Chen X, Zhou B, Li C. Distributed voltage control based ADMM for large-scale wind farm cluster connected to VSC-HVDC. IEEE Trans Sustain Energy 2019.
[36] Qu G, Li N. Optimal distributed feedback voltage control under limited reactive power. IEEE Trans Power Syst 2020;35(1):315–31.
[37] Robbins BA, Hadjicostis CN, Domínguez-García AD. A two-stage distributed architecture for voltage control in power distribution systems. IEEE Trans Power Syst 2012;28(2):1470–82.
[38] Watanabe K, Kudoh T. Voltage control apparatus, method, and program. 2014, US Patent 8, 716, 888.
[39] Kawano S, Murakami K, Yoshizawa S, Hayashi Y. Basic study on application of real-time satellite-observed solar radiation data for centralized voltage control in distribution networks with PVs. In: 2017 IEEE power & energy society innovative smart grid technologies conference. IEEE; 2017, p. 1–5.
[40] Zafar R, Ravishankar J, Pota HR. Centralized control of step voltage regulators and energy storage system under high photovoltaic penetration. In: 2016 IEEE innovative smart grid technologies-asia. IEEE; 2016, p. 511–6.
[41] Juamperez M, Guangya Y, Kjær SB. Voltage regulation in LV grids by coordinated volt-var control strategies. J Mod Power Syst Clean Energy 2014;2(4):319–28.
[42] Ranaweera I, Midtgard OM. Centralized control of energy storages for voltage support in low-voltage distribution grids. In: 2016 IEEE 16th international conference on environment and electrical engineering. IEEE; 2016, p. 1–6.
[43] Itaya N. Voltage monitoring control device and voltage monitoring control method. 2017, US Patent 9, 667, 100.
[44] Powell PW, Parker SK, Bollbach MA, Pruett ML. Voltage conservation using advanced metering infrastructure and substation centralized voltage control. 2013, US Patent 8, 577, 510.
[45] Sedighy M, Kamh MZ, El-Deib A, Iravani R, Hagar AA. System, method and controller for managing and controlling a micro-grid. 2018, US Patent 9, 870, 593.
[46] Wood AJ, Wollenberg BF, Sheblé GB. Power generation, operation, and control. John Wiley & Sons; 2013.
[47] Reddy SS, Sandeep V, Jung CM. Review of stochastic optimization methods for smart grid. Front Energy 2017;11(2):197–209.
[48] Ghafouri A, Milimonfared J, Gharehpetian GB. Coordinated control of distributed energy resources and conventional power plants for frequency control of power systems. IEEE Trans Smart Grid 2014;6(1):104–14.
[49] Miller N, Lew D, Piwko R. Technology capabilities for fast frequency response. Tech. rep, 3, GE Energy Consulting; 2017, p. 10–60.
[50] Majumder S, Agalgaonkar AP, Khaparde SA, Perera S, Kulkarni S, Ciufo PP. Allowable delay heuristic in provision of primary frequency reserve in future power systems. IEEE Trans Power Syst 2019;35(2):1231–41.
[51] Kundur P, Balu NJ, Lauby MG. Power system stability and control. vol. 7, McGraw-Hill New York; 1994.
[52] Attya AB, Hartkopf T. Wind turbine contribution in frequency drop mitigation–modified operation and estimating released supportive energy. IET Gener Transm Distrib 2014;8(5):862–72.
[53] Žertek A, Verbič G, Pantoš M. Optimised control approach for frequency-control contribution of variable speed wind turbines. IET Renew Power Gener 2012;6(1):17–23.
[54] Rey JM, Rosero CX, Velasco M, Martí P, Miret J, Castilla M. Local frequency restoration for droop-controlled parallel inverters in islanded microgrids. IEEE Trans Energy Convers 2018;34(3):1232–41.
[55] Shuai Z, Huang W, Chunming T, Luo A, Shen Z, Liu X. Frequency adjustment method for islanded virtual synchronous micro-grid. 2020, US Patent App. 16/714, 764.
[56] Gavriluta C, Candela I, Luna A, Gomez-Exposito A, Rodriguez P. Hierarchical control of HV-MTDC systems with droop-based primary and OPF-based secondary. IEEE Trans Smart Grid 2014;6(3):1502–10.
[57] Guerrero JM, Vasquez JC, Matas J, De Vicuña LG, Castilla M. Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. IEEE Trans Ind Electron 2010;58(1):158–72.
[58] Shafiee Q, Guerrero JM, Vasquez JC. Distributed secondary control for islanded microgrids—A novel approach. IEEE Trans Power Electron 2013;29(2):1018–31.
[59] Bernard MZ, Mohamed TH, Qudaih YS, Mitani Y. Decentralized load frequency control in an interconnected power system using Coefficient Diagram Method. Int J Electr Power Energy Syst 2014;63:165–72.
[60] Dong L, Zhang Y, Gao Z. A robust decentralized load frequency controller for interconnected power systems. ISA Trans 2012;51(3):410–9.
[61] Tan W, Zhang H, Yu M. Decentralized load frequency control in deregulated environments. Int J Electr Power Energy Syst 2012;41(1):16–26.
[62] Khayat Y, Naderi M, Shafiee Q, Batmani Y, Fathi M, Guerrero JM, et al. Decentralized optimal frequency control in autonomous microgrids. IEEE Trans Power Syst 2018;34(3):2345–53.
[63] Machowski J, Lubosny Z, Bialek JW, Bumby JR. Power system dynamics: stability and control. John Wiley & Sons; 2020.
[64] Andreasson M, Sandberg H, Dimarogonas DV, Johansson KH. Distributed integral action: Stability analysis and frequency control of power systems. In: 2012 IEEE 51st IEEE conference on decision and control. IEEE; 2012, p. 2077–83.
[65] Andreasson M, Dimarogonas DV, Johansson KH, Sandberg H. Distributed vs. centralized power systems frequency control. In: 2013 european control conference. IEEE; 2013, p. 3524–9.
[66] Venkat AN, Hiskens IA, Rawlings JB, Wright SJ. Distributed MPC strategies with application to power system automatic generation control. IEEE Trans Control Syst Technol 2008;16(6):1192–206.
[67] Bevrani H. Robust power system frequency control. vol. 85, Springer; 2009.
[68] Liu F, Song Y, Ma J, Mei S, Lu Q. Optimal load-frequency control in restructured power systems. IEE Proc, Gener Transm Distrib 2003;150(1):87–95.
[69] Bevrani H, Habibi F, Babahajyani P, Watanabe M, Mitani Y. Intelligent frequency control in an AC microgrid: Online PSO-based fuzzy tuning approach. IEEE Trans Smart Grid 2012;3(4):1935–44.
[70] Cheng M, Wu J, Ekanayake J, Coleman T, Hung W, Jenkins N. Primary frequency response in the Great Britain power system from dynamically controlled refrigerators. IET; 2013.
[71] Lu N. An evaluation of the HVAC load potential for providing load balancing service. IEEE Trans Smart Grid 2012;3(3):1263–70.
[72] Muhssin MT, Cipcigan LM, Jenkins N, Cheng M, Obaid ZA. Modelling of a population of heat pumps as a source of load in the great britain power system. In: 2016 international conference on smart systems and technologies. IEEE; 2016, p. 109–13.
[73] Short JA, Infield DG, Freris LL. Stabilization of grid frequency through dynamic demand control. IEEE Trans Power Syst 2007;22(3):1284–93.
[74] Eid BM, Rahim NA, Selvaraj J, El Khateb AH. Control methods and objectives for electronically coupled distributed energy resources in microgrids: A review. IEEE Syst J 2014;10(2):446–58.
[75] Kunte RS, Gao W. Comparison and review of islanding detection techniques for distributed energy resources. In: 2008 40th north american power symposium. IEEE; 2008, p. 1–8.
[76] Nassif AB, Torquato R. Field verification of autonomous anti-islanding schemes and grid support functions of an inverter-based microturbine distributed generator. IEEE Trans Ind Appl 2019;55(6):5652–8.
[77] El-Khattam W, Sidhu TS, Seethapathy R. Evaluation of two anti-islanding schemes for a radial distribution system equipped with self-excited induction generator wind turbines. IEEE Trans Energy Convers 2009;25(1):107–17.
[78] Wang X, Freitas W, Dinavahi V, Xu W. Investigation of positive feedback anti-islanding control for multiple inverter-based distributed generators. IEEE Trans Power Syst 2008;24(2):785–95.

[79] Bower W, Ropp M. Evaluation of islanding detection methods for photovoltaic utility-interactive power systems. Technical report report IEA PVPS T5-09, International Energy Agency (IEA); 2002.
[80] Stevens JW, Bonn RH, Ginn JW, Gonzalez S, Kern G. Development and testing of an approach to anti-islanding in utility-interconnected photovoltaic systems. Technical report, Albuquerque, NM (US): Sandia National Labs; 2000.
[81] Sadan N, Strandberg N, Renz B. Method and system for distributed generation trip protection using power line carrier signaling. 2017, US Patent 9, 733, 632.
[82] Xu W, Zhang G, Li C, Wang W, Wang G, Kliber J. A power line signaling based technique for anti-islanding protection of distributed generators—Part I: Scheme and analysis. IEEE Trans Power Deliv 2007;22(3):1758–66.
[83] Walling R. Application of direct transfer trip for prevention of DG islanding. In: 2011 IEEE power and energy society general meeting. IEEE; 2011, p. 1–3.
[84] Ellis A, Gonzalez S. Implementation of voltage and frequency ride-through requirements in distributed energy resources interconnection standards. Technical report, Sandia National Laboratories; 2014.
[85] Code G. High and extra high voltage. 2006, April.
[86] Mahela OP, Gupta N, Khosravy M, Patel N. Comprehensive overview of low voltage ride through methods of grid integrated wind generator. IEEE Access 2019;7:99299–326.
[87] Johnson DO, Hassan KA. Issues of power quality in electrical systems. Int J Energy Power Eng 2016;5(4):148.
[88] Heising C, et al. IEEE recommended practice for the design of reliable industrial and commercial power systems. New York: IEEE Inc.; 2007.
[89] Baggini A. Handbook of power quality. John Wiley & Sons; 2008.
[90] Chouhan PK, McClean S, Shackleton M. Situation assessment to secure IoT applications. In: 2018 fifth international conference on internet of things: systems, management and security. IEEE; 2018, p. 70–7.
[91] Payne EK, Lu S, Wang Q, Wu L. Concept of designing thermal condition monitoring system with ZigBee/GSM communication link for distributed energy resources network in rural and remote applications. Processes 2019;7(6):383.
[92] Payne EK, Shulin L, Wang Q, Wu L. Design concept of thermal behavior condition monitoring of distributed energy resources network system with ZigBee and GSM technology in remote and rural areas. In: 2018 IEEE international conference on smart energy grid engineering. IEEE; 2018, p. 298–302.
[93] Goldin JR, Baldassari M, Berdner JS. Fire detection, automated shutoff and alerts using distributed energy resources and monitoring system. 2017, US Patent App. 15/345, 012.
[94] Cerotti D, Codetta-Raiteri D, Dondossola G, Egidi L, Franceschinis G, Portinale L, et al. Evidence-based analysis of cyber attacks to security monitored distributed energy resources. Appl Sci 2020;10(14):4725.
[95] Siqueira de Carvalho R, Saleem D. Recommended functionalities for improving cybersecurity of distributed energy resources. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2020.
[96] Hussain A, Bui VH, Kim HM. Optimal operation of hybrid microgrids for enhancing resiliency considering feasible islanding and survivability. IET Renew Power Gener 2017;11(6):846–57.
[97] Adhikari S, Li F. Coordinated Vf and PQ control of solar photovoltaic generators with MPPT and battery storage in microgrids. IEEE Trans Smart Grid 2014;5(3):1270–81.
[98] Ganjian-Aboukheili M, Shahabi M, Shafiee Q, Guerrero JM. Seamless transition of microgrids operation from grid-connected to islanded mode. IEEE Trans Smart Grid 2019.
[99] Lopes JP, Moreira C, Madureira A. Defining control strategies for microgrids islanded operation. IEEE Trans Power Syst 2006;21(2):916–24.
[100] Ustun TS, Ozansoy C, Zayegh A. Recent developments in microgrids and example cases around the world—A review. Renew Sustain Energy Rev 2011;15(8):4030–41.
[101] Sao CK, Lehn PW. Control and power management of converter fed microgrids. IEEE Trans Power Syst 2008;23(3):1088–98.
[102] Guerrero JM, Hang L, Uceda J. Control of distributed uninterruptible power supply systems. IEEE Trans Ind Electron 2008;55(8):2845–59.
[103] IEEE. IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces. 2018, p. 1–138, IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003).
[104] Lai C, Jacobs N, Hossain-McKenzie S, Carter C, Cordeiro P, Onunkwo I, et al. Cyber security primer for DER vendors, aggregators, and grid operators. Tech. Rep., Sandia National Laboratories; 2017.
[105] Mahmud K, Khan B, Ravishankar J, Ahmadi A, Siano P. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. Renew Sustain Energy Rev 2020;127:109840.
[106] Cleveland F, Lee A. Cyber security for DER systems. National Electric Sector Cybersecurity Organization Resource. Electric Power Research Institute (EPRI); 2013.
[107] Elyengui S, Bouhouchi R, Ezzedine T. The enhancement of communication technologies and networks for smart grid applications. 2014, arXiv preprint arXiv:1403.0530.
[108] Ghavidel S, Li L, Aghaei J, Yu T, Zhu J. A review on the virtual power plant: Components and operation systems. In: 2016 IEEE international conference on power system technology. IEEE; 2016, p. 1–6.
[109] Nosratabadi SM, Hooshmand RA, Gholipour E. A comprehensive review on microgrid and virtual power plant concepts employed for distributed energy resources scheduling in power systems. Renew Sustain Energy Rev 2017;67:341–63.
[110] Kaplan D. Distributed energy resources manager. 2011, US Patent App. 12/905, 292.
[111] Braun M, Strauss P. A review on aggregation approaches of controllable distributed energy units in electrical power systems. Int J Distrib Energy Resour 2008;4(4):297–319.
[112] US, California EC, et al. Recommendations for utility communications with distributed energy resources (DER) systems with smart inverters. Smart Invert Work Group Phase 2015;2.
[113] Jogunola O, Ikpehai A, Anoh K, Adebisi B, Hammoudeh M, Gacanin H, et al. Comparative analysis of P2P architectures for energy trading and sharing. Energies 2018;11(1):62.
[114] Gerard H, Puente EIR, Six D. Coordination between transmission and distribution system operators in the electricity sector: A conceptual framework. Util Policy 2018;50:40–8.
[115] Zhang J, Hasandka A, Wei J, Alam S, Elgindy T, Florita AR, et al. Hybrid communication architectures for distributed smart grid applications. Energies 2018;11(4):871.
[116] Marzal S, Salas R, González-Medina R, Garcerá G, Figueres E. Current challenges and future trends in the field of communication architectures for microgrids. Renew Sustain Energy Rev 2018;82:3610–22.
[117] Henry J, Ramirez R, Cleveland F, Lee A, Seal B, Tansy T, et al. Cyber security requirements and recommendations for CSI RD&D solicitation # 4 distributed energy resource communications. 2015, Oct.
[118] Leccese F. An overwiev on IEEE Std 2030. In: 2012 11th international conference on environment and electrical engineering. IEEE; 2012, p. 340–5.
[119] Basso T. IEEE 1547 and 2030 standards for distributed energy resources interconnection and interoperability with the electricity grid. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2014.
[120] Ghalib M, Ahmed A, Al-Shiab I, Bouida Z, Ibnkahla M. Implementation of a smart grid communication system compliant with IEEE 2030.5. In: 2018 IEEE international conference on communications workshops. IEEE; 2018, p. 1–6.
[121] Ravikumar G, Hyder B, Govindarasu M. Hardware-in-the-loop CPS security architecture for DER monitoring and control applications. In: 2020 IEEE texas power and energy conference. 2020, p. 1–5.
[122] IEEE. IEEE standard for electric power systems communications-distributed network protocol (DNP3) - redline. 2012, p. 1–821, IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010) - Redline.
[123] Newaz A, Ospina J, Faruque MO. Controller hardware in the loop validation of a graph search based energy management strategy for grid-connected distributed energy resources. IEEE Trans Energy Convers 2019.
[124] Cleveland F. 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, p. 1–4.
[125] Baigent D, Adamiak M, Mackiewicz R, Sisco G. IEC 61850 communication networks and systems in substations: An overview for users. SISCO Systems; 2004.
[126] Ustun TS, Ozansoy C, Zayegh A. Modeling of a centralized microgrid protection system and distributed energy resources according to IEC 61850-7-420. IEEE Trans Power Syst 2012;27(3):1560–7.
[127] Liu X, Aichhorn A, Liu L, Li H. Coordinated control of distributed energy storage system with tap changer transformers for voltage rise mitigation under high photovoltaic penetration. IEEE Trans Smart Grid 2012;3(2):897–906.
[128] Agashe RV. IEEE 1547 compliant communication framework for a distributed energy resource [Master's thesis], North Carolina State University; 2017.
[129] Ferreira J, Martins H, Barata M, Monteiro V, Afonso JL. OpenADR—intelligent electrical energy consumption towards internet-of-things. In: CONTROLO 2016. Springer; 2017, p. 725–36.
[130] Kolenc M, Ihle N, Gutschi C, Nemček P, Breitkreuz T, Goedderz K, et al. Virtual power plant architecture using OpenADR 2.0 b for dynamic charging of automated guided vehicles. Int J Electr Power Energy Syst 2019;104:370–82.
[131] McParland C. OpenADR open source toolkit: Developing open source software for the smart grid. In: 2011 IEEE power and energy society general meeting. IEEE; 2011, p. 1–7.
[132] Stallings W. Data and computer communications. Prentice Hall; 2005.
[133] Stallings W, Brown L, Bauer MD, Bhattacharjee AK. Computer security: principles and practice. NJ, USA: Pearson Education Upper Saddle River; 2012.
[134] Qi J, Hahn A, Lu X, Wang J, Liu CC. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys Syst: Theory Appl 2016;1(1):28–39.
[135] Seal B, Cleveland F, Hefner A. Distributed energy management (DER): Advanced power system management functions and information exchanges for inverter-based DER devices, modelled in IEC 61850-90-7. Tech. Rep., EPRI, Xanthus Consulting International, NIST; 2012.
[136] Ibrahim E. Disruptive ideas for power grid security and resilience with DER. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2017.

[137] Xue Y, Starke M, Dong J, Olama M, Kuruganti T, Taft J, et al. On a future for smart inverters with integrated system functions. In: 2018 9th IEEE international symposium on power electronics for distributed generation systems. IEEE; 2018, p. 1–8.

[138] Kaster P, Sen PP. Cybersecurity and rural electric power systems: considering competing requirements for implementing a protection plan. IEEE Ind Appl Mag 2017;23(5):14–20.

[139] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proc IEEE 2011;100(1):210–24.

[140] Jacobs N, Hossain-McKenzie S, Jose D, Saleem D, Lai C, Cordeiro P, et al. Analysis of system and interoperability impact from securing communications for distributed energy resources. In: 2019 IEEE power and energy conference at illinois. IEEE; 2019, p. 1–8.

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

[142] Saleem D, Sundararajan A, Sanghvi A, Rivera J, Sarwat AI, Kroposki B. A multidimensional holistic framework for the security of distributed energy and control systems. IEEE Syst J 2019.

[143] Carter C, Onunkwo I, Cordeiro P, Johnson J. Cyber security assessment of distributed energy resources. In: 2017 IEEE 44th photovoltaic specialist conference. IEEE; 2017, p. 2135–40.

[144] Onunkwo I, Wright B, Cordeiro P, Jacobs N, Lai C, Johnson J, et al. Cybersecurity assessments on emulated DER communication networks. Technical report, Sandia National Laboratories; 2018.

[145] Saleem D, Carter C. Certification procedures for data and communications security of distributed energy resources. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2019.

[146] Veichtlbauer A, Langthaler O, Engel D, Kasberger C, Andrén FP, Strasser T. Towards applied security-by-design for DER units. In: 2016 IEEE 21st international conference on emerging technologies and factory automation. IEEE; 2016, p. 1–4.

[147] Kang B, Maynard P, McLaughlin K, Sezer S, Andrén F, Seitl C, et al. Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In: 2015 IEEE 20th conference on emerging technologies & factory automation. IEEE; 2015, p. 1–8.

[148] Yang Y, McLaughlin K, Littler T, Sezer S, Im EG, Yao ZQ, Pranggono B, et al. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems. In: International conference on sustainable power generation and supply. 2012, p. 1–8.

[149] Tweneboah-Koduah S, Tsetse AK, Azasoo J, Endicott-Popovsky B. Evaluation of cybersecurity threats on smart metering system. In: Information technology-new generations. Springer; 2018, p. 199–207.

[150] Liu CC, McArthur S, Lee SJ. Smart grid handbook, 3 volume set. John Wiley & Sons; 2016.

[151] Saleem D, Johnson J. Distributed energy resource (DER) cybersecurity standards. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2017.

[152] Mohassel RR, Fung A, Mohammadi F, Raahemifar K. A survey on advanced metering infrastructure. Int J Electr Power Energy Syst 2014;63:473–84.

[153] Feuerhahn S, Kohrs R, Wittwer C. Remote control of distributed energy resources using IEC 61850 as application-layer protocol standard. Energy Technol 2014;2(1):77–82.

[154] Gourisetti SNG, Hansen J, Hofer W, Manz D, Kalsi K, Fuller J, et al. A cyber secure communication architecture for multi-site hardware_in_the_Loop co_Simulation of DER control. In: 2018 resilience week. IEEE; 2018, p. 55–62.

[155] Sundararajan A, Chavan A, Saleem D, Sarwat AI. A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. Energies 2018;11(9):2360.

[156] Khan MMS, Palomino A, Brugman J, Giraldo J, Kasera SK, Parvania M. The cyberphysical power system resilience testbed: architecture and applications. Computer 2020;53(5):44–54.

[157] Morris T, Srivastava A, Reaves B, Gao W, Pavurapu K, Reddi R. A control system testbed to validate critical infrastructure protection concepts. Int J Crit Infrastruct Prot 2011;4(2):88–103.

[158] Silos Á, Señís A, De Pozuelo RM, Zaballos A. Using IEC 61850 goose service for adaptive ANSI 67/67N protection in ring main systems with distributed energy resources. Energies 2017;10(11):1685.

[159] Wimmer W. Determining VLAN-IDs for a switched-based communication network of a process control system. 2015, US Patent 9, 021, 067.

[160] Pedersen AB, Hauksson EB, Andersen PB, Poulsen B, Træholt C, Gantenbein D. 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, p. 61–6.

[161] Joo JY, Stewart E, Salazar B, Yee N. Selection of ten (10) cybersecurity scenarios for project cybersecure interconnection of distributed energy resources. Technical report, Livermore, CA (United States): Lawrence Livermore National Lab.(LLNL); 2018.

[162] Carter C, Cordeiro PG, Onunkwo I, Johnson JT. Cyber assessment of distributed energy resources. Technical report, Albuquerque, NM (United States): Sandia National Lab.(SNL-NM); 2018.

[163] Johnson JT. PV cybersecurity final report. Technical report, Albuquerque, NM (United States): Sandia National Lab.(SNL-NM); 2019.

[164] Johnson J, Quiroz J, Concepcion R, Wilches-Bernal F, Reno MJ. Power system effects and mitigation recommendations for DER cyberattacks. IET Cyber-Phys Syst: Theory Appl 2019;4(3):240–9.

[165] Powell C, Hauck K, Sanghvi AD, Reynolds TL. Distributed Energy Resource Cybersecurity Framework Best Practices. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2020.

[166] Schmutzler J, Gröning S, Wietfeld C. Management of distributed energy resources in IEC 61850 using web services on devices. In: 2011 IEEE international conference on smart grid communications. IEEE; 2011, p. 315–20.

[167] Keogh M, Cody C. Resilience in regulated utilities. Washington DC: National Association of Regulatory Utility Commissioners; 2013, November. Accessible at: www.naruc.org/Grants/Documents/Resilience%20in%20Regulated%20Utilities%20ONLINE%2011_12.pdf.

[168] Commission I-IE, et al. IEC TR 62351-12. 2016.

[169] Hersent O, Boswarthick D, Elloumi O. The internet of things: key applications and protocols. John Wiley & Sons; 2011.

[170] Fovino IN, Carcano A, Masera M, Trombetta A. Design and implementation of a secure modbus protocol. In: International conference on critical infrastructure protection. Springer; 2009, p. 83–96.

[171] Javier J. Using snort for intrusion detection in modbustcp/ip communications.

[172] Carcano A, Fovino IN, Masera M, Trombetta A. Scada Malware, a proof of concept. In: International workshop on critical information infrastructures security. Springer; 2008, p. 211–22.

[173] Liao GY, Chen YJ, Lu WC, Cheng TC. Toward authenticating the master in the modbus protocol. IEEE Trans Power Deliv 2008;23(4):2628–9.

[174] Shahzad A, Lee M, Lee YK, Kim S, Xiong N, Choi JY, et al. Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information. Symmetry 2015;7(3):1176–210.

[175] Xuan L, Yongzhong L. Research and implementation of modbus TCP security enhancement protocol. J Phys: Conf Ser 2019;1213(5):052058.

[176] Rao M, Newe T, Omerdic E, Kaknjo A, Elgenaidi W, Mathur A, et al. Bump in the wire (BITW) security solution for a marine ROV remote control application. J Inf Secur Appl 2018;38:111–21.

[177] Ferst MK, de Figueiredo HF, Denardin G, Lopes J. Implementation of secure communication with modbus and transport layer security protocols. In: 2018 13th IEEE international conference on industry applications. IEEE; 2018, p. 155–62.

[178] Hayes G, El-Khatib K. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In: 2013 third international conference on communications and information technology. IEEE; 2013, p. 179–84.

[179] Benisha R, Raja Ratna S. Design of intrusion detection and prevention in SCADA system for the detection of bias injection attacks. Secur Commun Netw 2019;2019.

[180] Goldenberg N, Wool A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. Int J Crit Infrastruct Prot 2013;6(2):63–75.

[181] Morris T, Vaughn R, Dandass Y. A retrofit network intrusion detection system for MODBUS RTU and ascii industrial control systems. In: 2012 45th hawaii international conference on system sciences. IEEE; 2012, p. 2338–45.

[182] Morris TH, Jones BA, Vaughn RB, Dandass YS. Deterministic intrusion detection rules for MODBUS protocols. In: 2013 46th hawaii international conference on system sciences. IEEE; 2013, p. 1773–81.

[183] McGrew D, Bailey D. Aes-ccm cipher suites for transport layer security (tls). Technical report, 2012, RFC 6655, july.

[184] IEEE. IEEE approved draft standard for smart energy profile application protocol. 2018, p. 1–358, IEEE P2030.5/D2, March 2018.

[185] Alliance Z, Alliance H. Smart energy profile 2 application protocol standard. 2013, document 13–0200-00.

[186] Jin D, Nicol DM, Yan G. An event buffer flooding attack in DNP3 controlled SCADA systems. In: Proceedings of the 2011 winter simulation conference. IEEE; 2011, p. 2614–26.

[187] Lee D, Kim H, Kim K, Yoo PD. Simulated attack on DNP3 protocol in scada system. In: Proceedings of the 31th symposium on cryptography and information security, kagoshima, japan. 2014, p. 21–4.

[188] Rodofile N, Radke K, Foo E. Real-time and interactive attacks on DNP3 critical infrastructure using scapy. In: Proceedings of the 13th australasian information security conference. 2015, p. 67–70.

[189] Darwish I, Igbe O, Celebi O, Saadawi T, Soryal J. Smart grid DNP3 vulnerability analysis and experimentation. In: 2015 IEEE 2nd international conference on cyber security and cloud computing. IEEE; 2015, p. 141–7.

[190] East S, Butts J, Papa M, Shenoi S. A taxonomy of attacks on the DNP3 protocol. In: International conference on critical infrastructure protection. Springer; 2009, p. 67–81.

[191] Rosborough C, Gordon C, Waldron B. All about eve: comparing DNP3 secure authentication with standard security technologies for SCADA communications. 2019.

[192] Majdalawieh M, Parisi-Presicce F, Wijesekera D. DNPSec: Distributed network protocol version 3 (DNP3) security framework. In: Advances in computer, information, and systems sciences, and engineering. Springer; 2007, p. 227–34.

[193] Hoyos J, Dehus M, Brown TX. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. In: 2012 IEEE globecom workshops. IEEE; 2012, p. 1508–13.
[194] Moussa B, Debbabi M, Assi C. A detection and mitigation model for PTP delay attack in an IEC 61850 substation. IEEE Trans Smart Grid 2016;9(5):3954–65.
[195] Yang HS, Kim SS, Jang HS. Optimized security algorithm for IEC 61850 based power utility system. J Electr Eng Technol 2012;7(3):443–50.
[196] Youssef TA, El Hariri M, Bugay N, Mohammed O. IEC 61850: Technology standards and cyber-threats. In: 2016 IEEE 16th international conference on environment and electrical engineering. IEEE; 2016, p. 1–6.
[197] Allience O. OpenADR 2.0 profile specification B profile. 2013, Document.
[198] Herberg U, Mashima D, Jetcheva JG, Mirzazad-Barijough S. OpenADR 2.0 deployment architectures: Options and implications. In: 2014 IEEE international conference on smart grid communications. IEEE; 2014, p. 782–7.
[199] Park M, Kang M, Choi JY. The research on vulnerability analysis in OpenADR for smart grid. In: International workshop on data analytics for renewable energy integration. Springer; 2014, p. 54–60.
[200] Paverd A, Martin A, Brown I. Security and privacy in smart grid demand response systems. In: International workshop on smart grid security. Springer; 2014, p. 1–15.
[201] Pillitteri VY, Brewer TL. Guidelines for smart grid cybersecurity. Technical report, 2014.
[202] Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security. NIST Spec Publ 2011;800(82):16.
[203] NERC C. Standards as approved by the NERC board of trustees may 2006. Atlanta, GA, USA: North American Electric Reliability Corporation; 2006.
[204] Horowitz KA, Peterson Z, Coddington MH, Ding F, Sigrin BO, Saleem D, et al. An overview of distributed energy resource (DER) interconnection: current practices and emerging solutions. Technical report, Golden, CO (United States): National Renewable Energy Lab.(NREL); 2019.
[205] WG15 IT. IEC 62351 security standards for the power system information infrastructure. 2016.
[206] Fries S. Security in power system automation status and application of IEC 62351 - an introduction. 2017, http://dx.doi.org/10.13140/RG.2.2.10747.21284.
[207] IEEE. IEEE standard cybersecurity requirements for substation automation, protection, and control systems. 2015, p. 1–38, IEEE Std C37.240-2014.
[208] IEEE. IEEE standard for intelligent electronic devices cyber security capabilities. 2014, p. 1–29, IEEE Std 1686-2013 (Revision of IEEE Std 1686-2007).
[209] Amaio T, Van T. IEEE 1711–2010 security for legacy SCADA protocols. SEQUI Inc; 2011.
[210] Meyer D, Baker F. Internet protocols for the smart grid. IETF; 2011.
[211] Stevens J. Electricity subsector cybersecurity capability maturity model (es-c2m2)(case study). Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst; 2014.
[212] DOE N. NERC, electricity subsector cybersecurity risk management process. Technical report, 2012, May.