IET Cyber-Physical Systems: Theory & Applications

Review Article

IET Journals
The Institution of Engineering and Technology

Cybersecurity for distributed energy resources and smart inverters

ISSN 2398-3396
Received on 20th October 2016
Revised on 3rd November 2016
Accepted on 6th November 2016
doi: 10.1049/iet-cps.2016.0018
www.ietdl.org

Junjian Qi[1] ✉, Adam Hahn[2], Xiaonan Lu[1], Jianhui Wang[1], Chen-Ching Liu[2]

[1]*Energy Systems Division, Argonne National Laboratory, 9700 South Cass Avenue, Lemont, IL, USA*
[2]*School of Electrical Engineering and Computer Science, Washington State University, EME, Pullman, WA, USA*
✉ *E-mail: jqi@anl.gov*

Abstract: The increased penetration of distributed energy resources (DER) will significantly increase the number of devices that are owned and controlled by consumers and third-parties. These devices have a significant dependency on digital communication and control, which presents a growing risk from cyber-attacks. This study proposes a holistic attack-resilient framework to protect the integrated DER and the critical power grid infrastructure from malicious cyber-attacks, helping ensure the secure integration of DER without harming the grid reliability and stability. Specifically, the authors discuss the architecture of the cyber-physical power system with a high penetration of DER and analyse the unique cybersecurity challenges introduced by DER integration. Next, they summarise important attack scenarios against DER, propose a systematic DER resilience analysis methodology, and develop effective and quantifiable resilience metrics and design principles. Finally, they introduce attack prevention, detection, and response measures specifically designed for DER integration across cyber, physical device, and utility layers of the future smart grid.

1 Introduction

The threat of cyber-based attacks targeting the Nation's energy sector, and in particular the electric power grid, is growing in number and sophistication [1, 2]. A major cyber incident in the power system could have serious consequences on grid operation in terms of socioeconomic impacts, market impacts, equipment damage, and large-scale blackouts [3–5]. Several effort such as the U.S. Department of Energy (DOE) Cyber Security Roadmap for Energy Delivery Systems [6], North American Electric Reliability Corporation, Critical Infrastructure Protection Standards [7], National Institute of Standards and Technology Interagency Report 7628 [8], and National Electric Sector Cybersecurity Organization Resource (NESCOR) report [9] – have explored the power grid's security and resilience against cyber threats.

Meanwhile, the traditional power grid is undergoing a massive change through renewable integration, microgrids, demand response, advanced metering infrastructure (AMI), and distributed energy resources (DER). Accordingly, the power grid architecture is fast evolving from a utility-centric structure to a distributed smart grid that heavily integrates DER [10]. Currently, Hawaii depends on renewables for over 23% of its energy, while California utilises over 26% renewables [11, 12]. California has a goal of integrating 15 GW of DER including 12 GW of renewable energy into distribution systems by 2020 and achieving 50% renewable energy by 2030.

DER will likely decrease the control that utilities have over the energy resources in power grids. To enable high levels of renewable penetration, utilities must implement wide-area communication to remotely control these devices. While smart meters and AMI already significantly expand the utility's attack surface, DER deployments present additional risks due to the tremendous number of devices and access points that operate outside the typical utility's administrative domain.

To promote DER deployment, the New York State Public Service Commission made an effort to address DER cyber vulnerabilities in its recent Reforming the Energy Vision initiative [13]. California's Rule 21 smart inverter working group has also provided recommendations for technical requirements for smart inverters including cybersecurity requirements [14]. NESCOR has discussed the DER system architectures and cybersecurity requirements of DER systems [15] and has identified many cybersecurity failure scenarios that DER could introduce to the grid [16].

In this paper, we propose a holistic attack-resilient framework and a layered cyber-physical solution portfolio to protect the integrated DER and the critical power grid infrastructure from malicious cyber-attacks, helping ensure the large-scale and secure integration of DER without degrading the grid reliability and stability.

2 Cyber-physical power system with large-scale DER deployments

With the large-scale integration of DER, the power grid is fast evolving from a utility-centric structure to a distributed smart grid. Here, we identify the likely future DER power grid architecture and introduce the unique cybersecurity challenges that DER integration presents.

2.1 Generic architecture of power systems with DER

In [16], a DER system architecture was proposed, which has five levels: (i) autonomous DER generation and storage, (ii) facilities DER energy management, (iii) utility and retail energy provider operational communications, (iv) distribution utility operational analysis, and (v) transmission and market operations. In International Electrotechnical Commission (IEC) 62351-12, a similar DER system architecture was mapped to the European M/490 Smart Grid Architecture Model and the interfaces enabling multiple levels of information exchanges between different levels of the system were also discussed [17].

In this paper, we also summarise the DER system architecture. To assist in the summary, we divide the architecture into four domains as shown in Fig. 1.

- *Domain 1:* DER devices and controllers

○ *Actors:* In this domain, the DER is likely owned and controlled by consumers who gain profit by generating power for personal use and

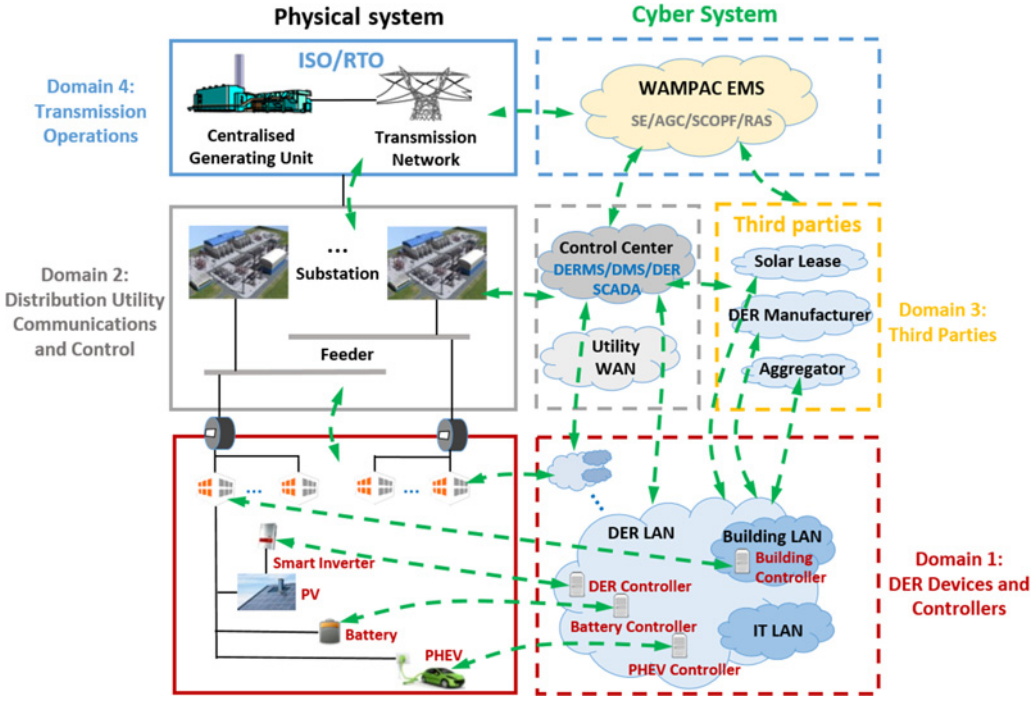

Fig. 1 *Proposed DER architecture*

may sell excess power to the utility. Facilities DER energy management systems (FDEMSs) are the entities that act on the DER and their controllers for operations (using the smart inverters). The owners have complete authority over the devices and controllers, and the FDEMS may have access limited to management of the devices, modifying certain DER operations, and reading real-time data allowed by the DER owner. The AMI system is the third actor; it can collect data from the devices and send it to the utilities.

○ *Interaction:* The DER owners get the information about the DER by communicating with smart inverters with wireless technology such as ZigBee. They can also access the smart inverters through the human–machine interface. FDEMS communicates with DER by the wide area network (WAN)/local area network (LAN) at the facility.

○ *Vulnerability points:* The vulnerabilities include (i) unauthorised access to DER controllers and smart inverters, (iii) penetration through the facility network, (iv) unauthorised access to smart meters, (v) an unauthorised change in the settings in the FDEMS, and (vi) novice owners who fail to adequately secure their devices.

- *Domain 2:* Distribution utility communications and control

○ *Actors:* The utility works as an actor in this domain and can send control commands to the smart inverters such as connecting/disconnecting the DER, regulating the voltage, and managing the amount of penetration allowed. Utilities may also use a FDEMS to handle DER systems located at utility sites such as substations or physical plant sites. The distribution management system ensures the stability of the grid after the addition of the DER. It is also responsible for shutting down the DER in case of an emergency.

○ *Interaction:* The utility interacts with the smart inverters and controllers using communication protocols such as smart energy profile (SEP) 2.0. The distribution system uses the WAN/LAN of the utility.

○ *Vulnerability points:* The protocols in use need to be checked for vulnerabilities. An attacker could penetrate through the utility network. Malicious commands sent to the DER controllers and/or smart meters can cause issues.

- *Domain 3:* Third-parties

○ *Actors:* Key actors within this domain include: (i) aggregators, (ii) companies providing power purchasing agreements (PPAs) or energy leases, and (iii) DER manufacturers. Aggregators must interact with DER in order to participate in an energy market on behalf of the DER owners. Companies supporting PPAs and energy leases invest in the initial capital expenses of DER and then charge the consumer a monthly rate based on the energy produced by the DER. Manufacturers may also have systems that interconnect with the DER and may perform remote maintenance on the systems.

○ *Interaction:* Most of the third-party entities have the ability to monitor the status of DER, and some may also have the ability to directly control their operation. Furthermore, these entities may have connectivity to a very large number of DER. Aggregators must connect to the DER in order to determine their available energy. Many DER manufacturers provide additional online services that come with their device such as automatic cloud storage of device data. Many devices are configured to immediately connect back to a manufacturer-controlled cloud environment in order to provide consumers with easy access to data and to support maintenance operations. Companies that provide PPAs and energy leases also often remotely monitor the energy produced by the DER and maybe responsible for performing maintenance on the devices remotely.

○ *Vulnerability points:* These interconnections introduce centralised points that could potentially be leveraged by attackers to manipulate DER instances. The systems that are used for third-party access may directly interconnect with many more DER instances than the other, more well-defined, DER interconnections. Attacks against these systems have the ability to influence a large number of DER across multiple distribution grids. Although it is unclear how much control these entities have over the DER, the security of these connections is often outside the control of the utility and the DER owner.

- *Domain 4:* Transmission operations

○ *Actors:* These actors include the independent system operators (ISOs) and regional transmission organisations (RTO) that maintain a stable frequency by balancing system based on the operating reliability regulations. In their EMS there are many advanced applications such as state estimation (SE) and automatic generation control (AGC).

○ *Interaction:* The ISOs/RTOs will probably not directly communicate with smart inverters or DER devices. However, ISOs or RTOs and market operations can affect what the DER systems are requested or required to do, based on tariffs and other agreements [16]. DER operations need to be integrated with the

large power grid operations. Distribution utilities may interact with their ISO/RTO as a wholesale market participant. The DER aggregators may also bid into the electricity market for both energy and ancillary services. The operation of the large grid at ISO/RTO level can also impact the operation of DER. Communication protocols on this end commonly include Distributed Network Protocol (DNP3) and IEC 61850.

- *Vulnerability points:* Many advanced applications in energy management system (EMS) are based on the measurements from sensors such as remote terminal units or phasor measurement units (PMUs). The compromised measurements can negatively influence the functionalities of advanced applications and further influence the power grid operation, which can lead to serious voltage or frequency violations.

2.2 Challenges of maintaining DER cybersecurity

The emerging DER architecture introduces a variety of potential vulnerabilities to various cyber threats. First, the high penetration of DER introduces a huge number of energy devices (e.g. smart inverters and battery controllers) owned and operated at many consumer and utility locations. The number of consumer-owned DER devices incorporated into the grid could vastly outnumber the utility owned and controlled resources. Second, DER spans multiple security administrative domains, meaning that the utility may only be able to monitor the security posture of devices up to the smart meter, as the DER owners will likely manage their own devices. Third, the various networks used to control the DER maybe interconnected with building automation networks and other IT networks, thereby increasing their attack surface. These three key features introduce many new threats to both DER and the broader grid.

As identified in Fig. 1, a wide variety of devices and networks are required to support DER; however, current research has only addressed a subset of this underlying infrastructure and its interactions. Numerous key research effort have demonstrated smart metre advances including (i) security attack analysis for smart meters [18], (ii) intrusion detection approaches for smart meters [19], and (iii) the design of new security mechanisms for smart meters. While secure smart meters play a critical role in DER integration, most DER innovation is occurring 'behind the meter' through the integration of new energy sources and cyber-control mechanisms. In addition, the required control techniques must operate across administrative domains (i.e. between utilities and consumers). This creates many new cybersecurity challenges beyond those faced with smart meter deployments. Table 1 identifies key cybersecurity challenges introduced by DER and compares these emerging DER challenges against the current smart meter/AMI systems to demonstrate why current research does not meet these needs.

Table 1 Emerging key DER security challenges

Security challenges	Smart meter/AMI	DER
divided administration	the utility owns the entire AMI infrastructure or utilises a managed service. This ensures that security mechanisms and patches are installed and correctly configured. Utilities also prioritise cybersecurity during system acquisitions	smart inverters will likely be owned by the DER operator or other third parties, instead of the utility [20]. The DER operator and the third parties may not have the technical expertise or incentives to prioritise or maintain the security of their infrastructure
increased cyber-physical interdependencies	smart metre attacks have limited cyber-physical interdependencies. Generally, only an attack that disconnects a metre can be detected by monitoring the physics of the grid	preventing, detecting, and mitigating malicious DER operations will heavily depend on analysing both the cyber and physical properties of the grid
greater impact to grid	while the disconnection of metres will leave consumers without power, it is unlikely to significantly impact the reliability and stability of the distribution grid	if there is a high penetration of DER in the grid, the malicious operation of smart inverters may seriously impact the distribution grid by injecting excessive power or intentionally manipulating voltage, which could present a greater risk to the bulk power system stability
cryptography and key exchange	the utility either owns the entire AMI network or utilises a managed service that simplifies the implementation of the cryptographic protocols and key exchanges necessary to protect communications	the networks must cross multiple administrative boundaries, so that commands from the utility can control the consumer-owned DER. Therefore, key exchange and revocation must occur between multiple parties
privacy	utilities commonly obtain meter readings on 15 or 60 min intervals, which only provide information on changes with major loads [21]	utilities maybe able to measure the status of DER resources in seconds or minutes. This information could be used to infer increasingly accurate profiles of consumer behaviour
more control functions	smart metres have limited control functions, which typically include demand response and load disconnects	smart inverters have advanced control functions that can greatly influence the utility's and customer's ability to control smart inverters

2.3 Overview of DER cybersecurity research framework

Fig. 2 presents an overarching architecture for attack-resilient DER integration that takes into account both the cyber and physical characteristics of the power grid by combining effort to prevent, detect, and respond to cyber-attacks at the cyber, physical device, and utility layers. This overall framework will cover the following key topics within the area of DER cybersecurity by addressing the identified key challenges of DER security:

- *Resilience metrics and design principles for DER:* Common cyber vulnerabilities within DER and smart inverters, along with the risk they present to the grid through complex interactions with other devices and applications must be identified. Resilience metrics and cyber-physical security principles should also be developed to provide increased confidence in DER implementations. Attack-resilient security metrics, vulnerability indices, and design principles should be developed to help guide utilities and consumers as they increasingly adopt DER. The metrics will identify how cyber-attacks against DER could impact the grid, especially with increasing amounts of DER integration, to inform utilities about DER-related decisions. These metrics and design principles will inform utilities about: (i) the percentage of allowable DER penetration to maintain grid reliability while some DER instances are malicious, (ii) how observable the malicious DER actions are within various distribution feeder models, and (iii) what DER functions or commands have the greatest ability to influence grid reliability. In addition, it will provide a foundation for understanding the security mechanisms necessary to protect the grid as the DER integration increases. These security design principles will identify critical DER security properties (e.g. confidentiality, integrity, and availability) for various messages and functions. It will then

leverage the cyber-attack threat models and DER system architectures to provide a ranking of threat impacts and identify tradeoffs between the amount of integrated DER, granularity of control capabilities, and cybersecurity of the infrastructure.

- *Attack prevention for DER:* Current gaps between the existing technologies to prevent attacks against DER need to be explored and previous work on the design of security architectures for smart meters should be extended while incorporating many of the unique properties in DER. Security mechanisms for DER will be investigated at cyber, physical device, and utility layers of the power system, which will inform DER owners and utilities about what security protections are important to maintain a secure system. To enhance the cybersecurity of the power system with a huge number of DER, necessary cybersecurity architectures and mechanisms need to be identified and designed for DER integration. Specifically, cryptographic operations (including key exchanges and management), trusted computing operations, and access control models for DER should be carefully studied. Both cyber and physical techniques to protect DER from attack need to be identified.
- *Attack detection for DER:* It is imperative that malicious activities within DER be quickly detected. Effective methods should be developed to detect DER anomalies and misuse patterns across both the cyber and physical components. Techniques need to be devised to monitor these patterns to provide higher-confidence attack detection. These techniques will then correlate both physical and cyber events to produce high-confidence indicators of attack, and will provide actionable data to enable real-time utility response. The tool will operate within the control centre to collect data across the various utility infrastructures and DER domains. The attack detection techniques must reveal sufficient information regarding the attack to provide utilities with the ability to appropriately respond. Therefore, information that should be provided along with detection alerts includes: (i) the set of affected DER resources, (ii) estimated malicious action (e.g. voltage–frequency violations), and (iii) estimated severity.
- *Attack response for DER:* Proper and prompt response actions should be provided to disconnect offending systems or counteract them through the control of the other DER. The goal of cyber-attack response is to prevent cyber-attacks from further impacting the system while ensuring the continuous operation of the systems to the largest extent possible. Once the intrusion detection system (IDS) identifies the likely cause of the anomaly, it will provide fail-safe responses that protect the grid by minimising the impact of the DER. The response to the attack can be based on the malicious actions performed by the DER, the scale of the attack, and the detection confidence. If the attack is identified at a high-confidence level, those DER should be immediately disconnected from the grid. If lower confidence events are detected, then alternative methods such as controlling neighbouring DER, should be explored to compensate for the malicious DER activities. Various response activities should be studied to determine the optimal approach for different attack scenarios.

3 Potential cyber-attacks on cyber-physical power system with DER

This section provides a brief overview of different types of potential cyber-attacks with respect to the cyber-physical power system with large-scale DER deployments.

3.1 Cyber-physical threat modelling

Research is required to explore the threat models and the associated risks that DER and smart inverters introduce to the reliability of the distribution or even bulk transmission grids. The key issues that should be modelled and simulated are identified below:

- *Cyber-threat model:* NESCOR has identified many cybersecurity threats to DER [15]. Key targets of cyber threats include DER controllers, smart inverters, and the interactions between wide-area monitoring, protection, and control (WAMPAC) of the power system and DER.
- *DER control and communication:* The control architectures and communication networks of the DER implementation directly determine the risk exposure from cyber-attacks. Multiple devices are involved in controlling DER, especially smart inverters, DER controllers, and battery controllers. Models can be developed using cyber-architectural languages such as data flow diagrams or the architectural analysis and design language. Specific properties of DER control and communication that need to be modelled include: (i) communication protocols [e.g. IEEE 1815 (DNP3), IEC 61850-7-420, SEP 2.0, and Modbus] tailored for the control of DER devices; (ii) unicast, multicast, and broadcast communication topologies for DER messages; and (iii) smart inverter control functions including volt–var management, frequency–watt management, status reporting, and time synchronisation.
- *Distribution grid and DER:* The physical properties of the distribution grid, feeders, and integrated DER also significantly influence the degree to which attackers impact the stability and reliability of the grid. The components that will be modelled include photovoltaic (PV) systems energy storage, smart inverters, voltage regulators, capacitor banks, transformers, and protections such as relays, reclosers, and fuses. A primary factor that will be evaluated is the percentage of DER that can be integrated into the grid while still remaining reliable during cyber-attacks. The role of local aggregated controllers such as microgrid controllers should also be considered in the evaluation.
- *Coupled transmission and distribution with DER:* Increased integration of DER will not only influence the distribution grid; it can also potentially influence the transmission grid. In addition, the disturbances in the transmission grid can influence a large number of DER in the distribution grid. Therefore, there is a need to perform coupled transmission and distribution modelling and analysis, by extending the power flow analysis for integrated transmission and distribution systems [22, 23] and incorporating DER.

3.2 Threat scenarios targeting DER

An attack against DER could target a number of devices and communication networks owned by either the utility or the DER owner. Furthermore, there may also be a variety of third-party services and entities that are interdependent with the operation of DER. The severity of attacks on the various system components and entities will be determined by the size of the DER and the number of available DER instances they are connected to.

Fig. 3 is a high-level schematic representation of potential cyber-attacks targeting DER. These are described in the following paragraphs, which are numbered to correspond to the red triangles in Fig. 3:

- (1) *Malicious DER commands sent through utility WAN:* Utilities may need to remotely communicate with DER in order to control the operating points and monitor the status of the devices. These communications will be critical to maintain the reliability of the distribution grid, but an attack that can deny, disrupt, or tamper with these messages could prevent the utility from performing necessary control actions. A number of vulnerabilities could enable these attacks including insecure network protocols, misuse of cryptographic operations, or unauthorised intrusions into the utility DER systems. If these attacks occurred, they could provide the attacker with the ability to control a large number of DER systems, which could produce a serious impact on the distribution grid. Similar attack scenarios identified by NESCOR include [15]:

  - Compromised DER sequence of commands causes power outage (DER.6).
  - DER SCADA system issues invalid commands (DER.14).
  - Loss of DER control occurs due to invalid or missing messages (DER.9).

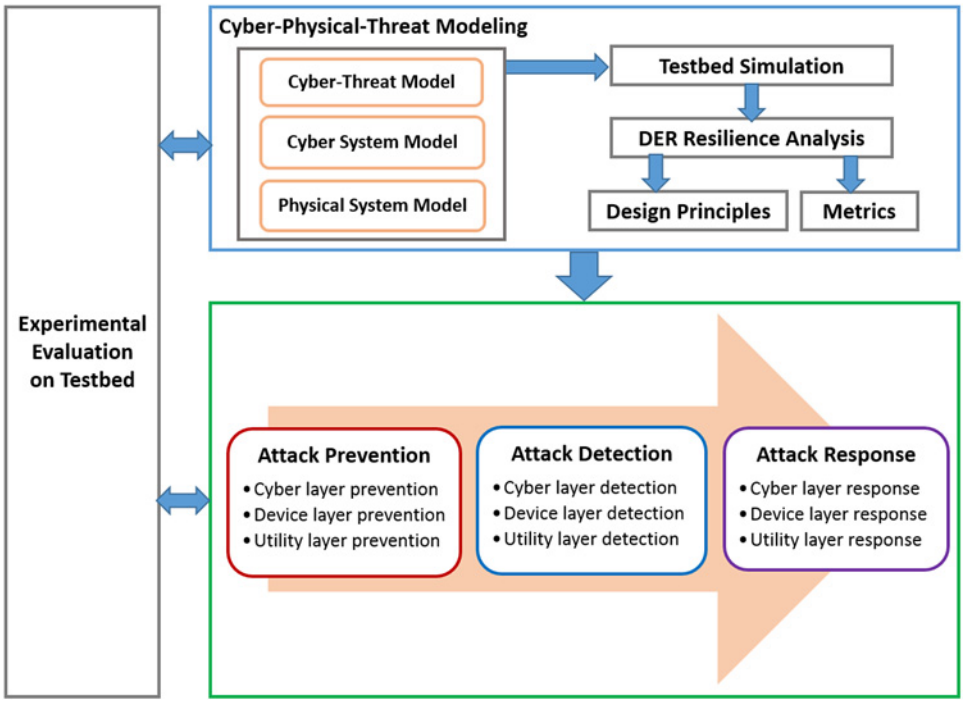

Fig. 2 *Attack-resilient framework for DER cybersecurity*

• (2–3) *Malware or unauthorised control of smart inverters and DER controllers:* DER requires a wide variety of digital devices to control their operation and provide consumers and utilities information about their operation. Most DER will likely include smart inverters and DER controllers; others may also include battery controllers and even electric vehicle (EV) controllers. If attackers can directly access these systems, they will be able to manipulate any of their control functions, or spoof status information to the utilities or owners. Attacks that have direct control over the smart inverters could be particularly dangerous, because the attack could intelligently manipulate the device's operation based on the state of the grid. This could help the attacker amplify undesirable grid states. Similar attack scenarios identified by NESCOR include [15]:

○ Malware introduced in DER system during deployment (DER.3).
○ Threat agent modifies field DER EMS efficiency settings (DER.10).

• (4–6) *Attacks from connected building control systems, IT networks, and vehicle systems:* DER devices will likely be interconnected with a variety of other systems and networks including various Internet of things devices and other third-party

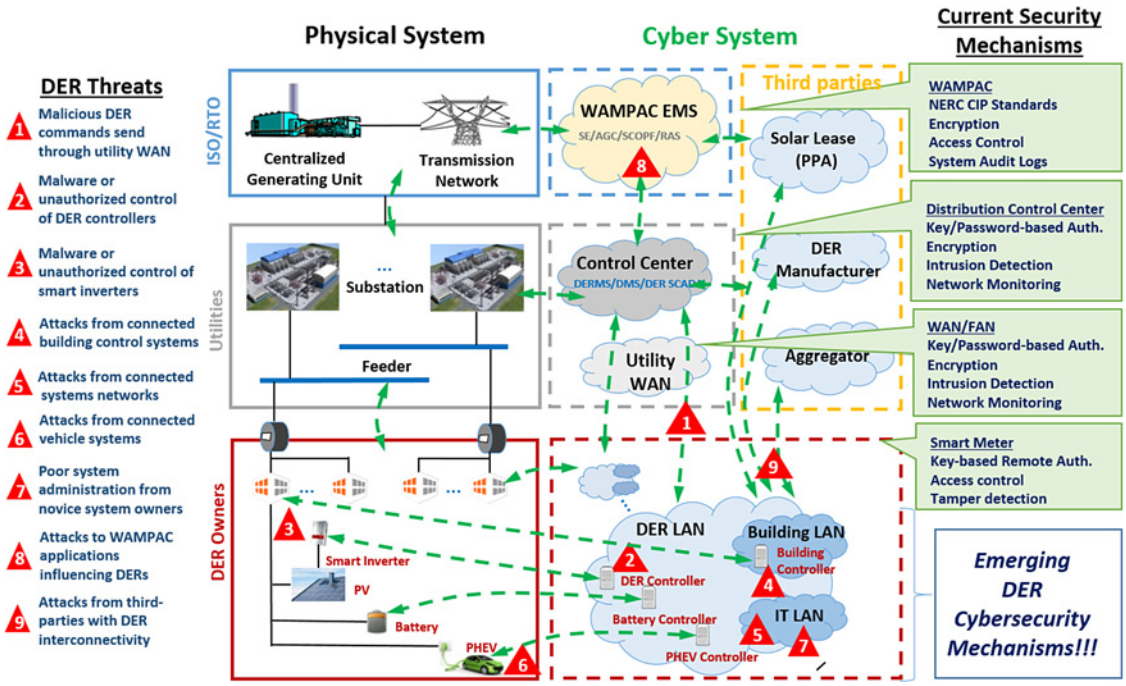

Fig. 3 *High-level schematic representation of cyber-attacks on DER*

Table 2 Impact levels of DER attack

Impact	Attack target	Rational
high	large-scale coordinated attack on DER	DER devices may have remotely accessible functions, which can provide an attacker with large-scale access to many DER. For example, many current manufactures or third-party DER operators could have access to large numbers of DER. If these systems have the capability to control the DER, attacks could then have broader impact across many different distribution grids
	utility DMS[1]/DER SCADA server	the utility's DMS/DER SCADA[2] system could have some control over all residential, commercial, and utility-scale instances. Attacks against these instances could potentially influence multiple DER across the distribution grid
moderate	utility-scale DER	utility-scale DER could be in the 100 kW to 10 MW range, which could cause many grid misoperations if manipulated by an attacker
	group of residential DER	on a power grid with high PV penetration, there could be hundreds of residential DER. A coordinated attack against a large number of residential DER could have a significant impact on grid stability or available load
	commercial DER	larger commercial DER (10–100 kW) could contribute to protection system misoperations and other system stability problems
low	single residential DER	single resident DER (1–10 kW) have little impact on the grid, but could negatively impact a resident or residents on the same transformer [30]

[1] distribution management system (DMS)
[2] supervisory control and data acquisition (SCADA)

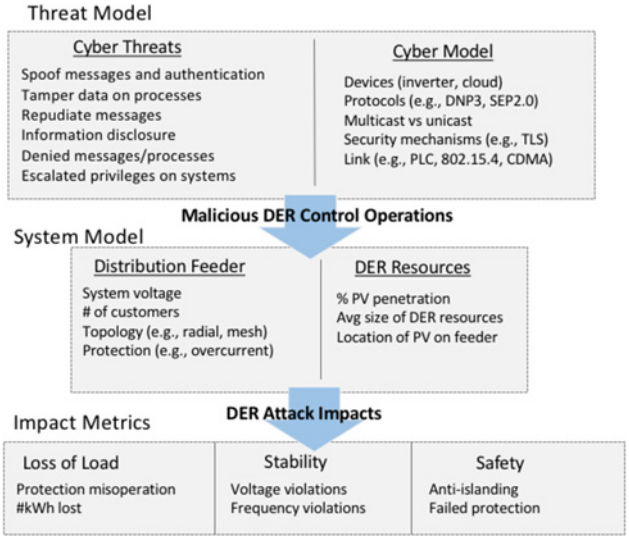

Fig. 4 *DER attack impact evaluation*

cloud systems and services. Many of these devices and networks will not have a strong security posture and may provide avenues for remote access to the DER components. These interconnections could be used by attackers to access the DER and spoof various commands and messages to change operational settings. These vulnerabilities could be caused by weak authentication of mechanisms or software vulnerabilities within the DER components. Similar attack scenarios identified by NESCOR include [15]:

o Threat agent spoofs DER data monitored by DER SCADA systems (DER.15).
o DER's rogue wireless connection exposes the DER system to threat agents via the Internet (DER.2).

• (7) *Poor system administration from novice system owners:* Many DER systems are likely to be operated by individuals who do not have expertise in cybersecurity. In these scenarios, the devices are unlikely to get critical system updates and may miss key security configurations. Furthermore, these systems maybe the object of social engineering attempts directed at the unsuspecting administrators. Similar attack scenarios identified by NESCOR include [15]:
o Custom malware gives threat agent control of field DER EMS (DER.13).
• (8) *Attacks to WAMPAC applications influencing DER:* Malicious attacks on WAMPAC applications such as AGC and remedial action schemes (RASs) can produce severe system-level frequency or voltage problems, further influencing the operation of a huge number of DER which can in turn cause serious problems in distribution and transmission grids. For example, AGC issues an area control error (ACE) that reflects the supply–demand mismatch to dispatch the generators and balance the generation and demands. When the tie-line bias control is considered as the operation mode of interconnected power grids, ACE will be calculated based on the frequency and tie-line power deviations. If these measurements are compromised, it will lead to the miscalculation of ACE, and in extreme cases the system frequency could go beyond the acceptable range [24]. When the system frequency is too low due to cyber-attacks against AGC, smart inverters have to be disconnected, which will lead to a further reduction of generation and may make the system frequency even lower.
• (9) *Attacks from third-parties with DER interconnectivity:* The third-party aggregators, manufacturer, and energy leasing entities all have connectivity to a potentially large number of DER, likely across multiple distribution grids. An attack against any of the systems supporting this connectivity could potentially provide an attacker with access to a large number of DER instances. These impacts maybe minor if the third-party access is limited to only monitoring the state of the DER. However, if the third-party has the ability to change operational setpoints or software configurations, then attacks against these systems could have serious impacts that may cascade beyond any single distribution grid. Furthermore, the access maintained by these third-parties is often not directly controlled by the utility or DER owner, which further complicates the risk management functions.

In addition, coordinated attacks against DER can negatively influence the operation of the bulk power system or impact the system stability:

o With high penetration of DER, the widespread fault propagation under coordinated and targeted attacks on carefully selected DER can negatively influence WAMPAC applications; for example, they could lead to the misoperation of the RAS system and produce severe unexpected consequences for DER and the power grid, or even cause cascading blackouts. These complex interdependencies will dramatically increase the risk of power grid operation [25, 26] and should be carefully analysed.
o Coordinated attacks can target system instability by manipulating the operation of a large number of DER. There has been research on the impact of PV integration on system stability including small-signal stability [27], voltage stability [28], and transient stability [29]. Manipulating the output power of many DER such as PV and battery storage can change the net load from substations and further impact the system stability. It is possible for an attacker to launch an attack on the DER connected to the distribution system

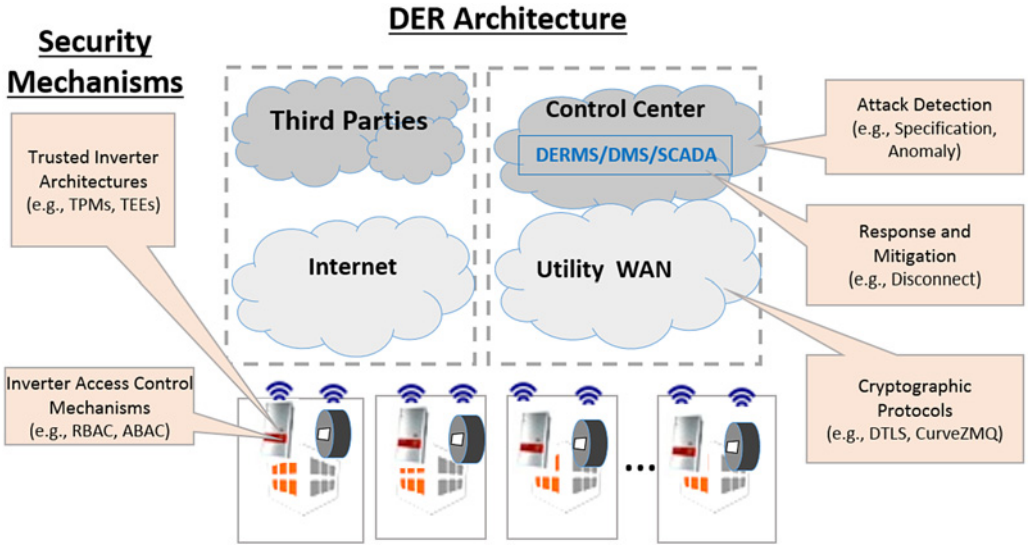

Fig. 5 *Overview of cyber-layer attack resilience*

at those most vulnerable load buses, in which case manipulating the smallest number of DER can cause serious stability problems such as undamped oscillation or voltage collapse. Therefore, it is critical for the system operator to identify those most vulnerable load buses and implement targeted protection of them in order to eliminate the possibility of the above-mentioned low-cost high-impact cyber-attacks to the greatest extent.

3.3 Attack threat ranking

Various attacks can be ranked based on their ability to negatively impact the grid (Table 2). An attack on a single DER instance is considered critical only if it is associated with a large utility-scale facility (e.g. 1 MW). However, as demonstrated in Fig. 3, many systems and networks interconnect with large numbers of smaller DER. Attacks against these assets have the potential to access many system components, and therefore could also introduce serious risks to the grid.

3.4 Attack impact analysis and metrics

This section will introduce a variety of attack impact metrics that provide both qualitative and quantitative mechanisms to evaluate the severity of the cyber-attacks. The attack severity metrics are used to evaluate how significantly the attack can manipulate the DER control functions. Fig. 4 illustrates the proposed methodology for the evaluation of DER attacks.

The proposed attack impact evaluation will utilise various threat models to identify potential attacks against DER. These threats to cybersecurity will then be mapped to a physical system model that includes various properties of the distribution feeder and DER. Furthermore, additional properties of the communication architecture will also be explored to evaluate what impacts various attacks have on the system. By manipulating the DER instances, the attacker can influence a number of system actions as identified below:

- *Disconnect:* The DER can be tripped off from the grid. This can prevent the consumer from selling back energy to the grid, and it may also negatively influence grid operation by creating frequency or voltage violations or influencing the system stability.
- *False trip:* If the PV manipulation can masquerade as a fault, the attacker could potentially trigger an incorrect tripping of a protection relay. This attack could cut off power to a number of consumers on a distribution feeder.
- *Overloads:* Under light load conditions or when the load is disconnected either by the operator or by an attacker, the power from PV or other DER devices can flow back to the substation and may cause overloading of the feeder between the DER system and the substation. If PV generation masks the actual load, the unexpected disconnection of PV may cause overloading of the feeder; more generally, manipulating the active power of many DER devices can change the power flow of the distribution system, which can cause further power flow violations [31].
- *Voltage–frequency violations:* Malicious control of a smart inverter could cause a violation of acceptable grid voltage and frequency ranges, resulting in grid instabilities, and potential outages. High penetration of DER can influence voltage profile and system frequency, depending on the location and capacity of the DER and their loading conditions.
- *Failed protection:* The DER operation can mask a real system fault such that a protection device does not operate correctly, causing a fault to propagate. Reverse power flow caused by DER can lead to exceeding the interruption ratings of circuit protections and sympathetic tripping of adjacent circuits [31]. High PV penetration can change the fault current levels and the protection zone of the protective relays, and may influence the coordination of overcurrent relays, fuses, sectionalisers, and auto-reclosers [32]. The misoperations of protective relays may even lead to a cascading event in the distribution grid.
- *System instability:* Manipulating the active and reactive powers of a large number of DER can influence the small-signal stability and voltage stability of the power system, which may cause undamped oscillations or voltage collapse.

Once the threat and system model have been defined, system simulations can be performed with various simulators to evaluate their impacts on the grid. A variety of quantitative attack impact metrics can be explored based on (i) the amount of load lost, (ii) the number of feeders tripped, (iii) fraction of components not surviving a given attack, (iv) voltage or frequency violations, (v) decreased system stability margins, (vi) time to recover a given fraction of network functionality, (vii) average propagation of cascading failures, and (viii) safety violations.

3.5 Cyber-physical DER security design principles

Designing a secure cyber-physical DER requires a strong understanding of the impacts of various attacks. While foundational computer security design principles have been identified in [33], these principles must be explored within the context of a modern DER environment to identify what security mechanisms must be integrated to ensure that the systems achieve

these principles. Key design principles that must be further explored within the context of DER include:

- Should we implement rules requiring diversity in DER devices (e.g. smart inverter manufacturers) to minimise the severity of vulnerabilities discovered in a certain manufacturer?
- Does the grid depend too heavily on security mechanisms that the utility does not control?
- Do any third-parties have control of, or access to, an excessive number of DER?
- Can DER network provide sufficient availability to forward time-sensitive messages?
- Are there DER settings/setpoints that must be verified by the utility to ensure devices are operating as expected?
- How accurate do these checks need to be, and when do we need to add high-assurance device architectures to ensure adequate security?
- Should smart inverters and other DER devices have default states that they should fail over to in the face of a security event?

4 Cybersecurity for renewables, DER, and smart inverters framework

This section presents an overview of the proposed research framework that includes cyber, physical device, and utility layer security measures at multiple levels for different attack classes. The proposed framework enables resiliency by providing techniques to prevent, detect, and respond to an attack throughout the cyber, physical device, and utility layers to ensure that the grid can remain operational during an attack.

4.1 Cyber-layer attack resilience

An overview of the cyber-layer attack resilience is presented in Fig. 5. More details are discussed in these sections that follow.

4.1.1 Cyber-layer attack prevention: A broad array of cybersecurity mechanisms is needed to prevent attackers from gaining control over DER. We need to explore gaps and challenges in the currently available security mechanisms and introduce novel techniques tailored to this domain.

Trusted computing bases: The utility's increased dependency on DER for grid control operations presents a strong need for trustworthy DER devices. However, because the utility has little administrative control over the various DER devices, it is difficult to establish the appropriate level of trust in critical DER operations. To protect the critical cryptographic operations and DER control functions, DER devices should implement a trusted computing base. Research is needed to explore how DER devices implement trusted platform modules and trusted execution environments (TEEs) to support the protection of critical DER operations. These techniques provide additional assurance that software-based vulnerabilities will not provide attackers with access to critical system data. This effort will explore methods and architectures to protect critical DER devices and functions using modern hardware-based security mechanisms (e.g. ARM TrustZone [34], and GlobalPlatform [35]).

While hardware-based techniques can provide improved security, it is important to prioritise the criticality of various system devices so they can be appropriately protected. In addition, many DER instances have long lifespans due to their large initial capital costs, and may have to operate for over 20 years. Therefore, the software must be updatable to address new software requirements and evolving security technologies. This constraint may make it difficult to depend on hardware security modules and secure co-processors, which have limited flexibility. Instead, techniques that separate processes based on their criticality and placing them within TEEs can provide improved security while still providing support to add new functionality. Examples of functions that may need to be isolated include: (i) cryptographic functions and key storage, (ii) event auditing/reporting, and (iii) setpoint management.

Access control mechanisms: As identified in Section 2, DER devices will likely be accessible by a number of different entities (e.g. manufacturer, utility, aggregator, consumer, and PPA). Therefore, granular access control mechanisms are required to prevent these actors from gaining unauthorised access. Currently, there is limited research exploring access control models for DER. The following list explores potential actors and functions that could be used to build such a model:

- *Manufacturer:* The manufacturer may request read-only access to operational data from the smart inverters' performance in order to determine inefficiencies or defects in the devices. Furthermore, the manufacturer may need to provide firmware updates to the devices to solve some of these issues.
- *Consumer:* The consumer will likely need read-only access to system parameters, status information, and load data. They may also want to specify operational parameters for the smart inverter because they are responsible for the DER's initial configuration. Furthermore, the consumer may want to limit the access to usage data from other owners.
- *Utility:* The utility may need to dynamically change the smart inverter parameters and setpoints in order to control smart inverter responses to many grid events. Utilities will also need access to view device parameters to verify that the various DER are operating as expected and to support various grid analysis functions.
- *PPA:* The third-party provider may own the PV array and may also be responsible for maintaining it; therefore, they will likely

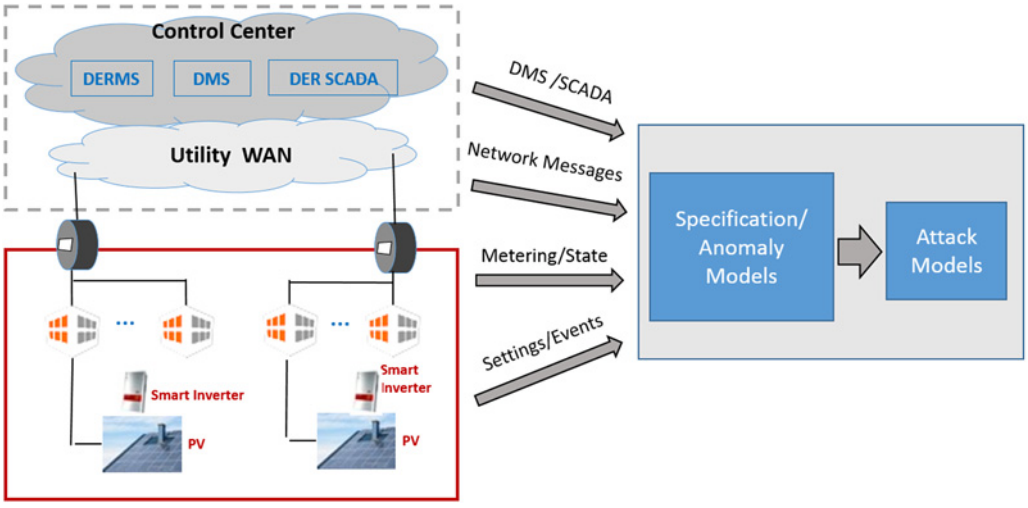

Fig. 6 *Cyber-layer attack detection*

possess access to the system. This party will likely need access to PV production data, which they may use to (i) charge the consumer, (ii) monitor the efficiency of the PV array, (iii) debug current settings and parameters, and (iv) collect analytics for determining cost/energy savings and techniques.

Role-based access control (BAC) will be an important technique to help simplify the access control decisions in this space. However, there may also be a need to change access decisions over time depending on the state of the grid and DER. Therefore, attribute BAC mechanisms and models maybe necessary to provide more granular access control changes at different times to account for scheduling and forecasting capabilities. These models will be developed to include the roles, objects, and temporal properties that should dictate access control decisions for DER.

Secure communications: Secure communications based on strong cryptographic operations and protocols are important to protect DER messages. While the primary communication protocol being proposed for DER, SEP 2.0, utilises transport layer security (TLS) to provide message encryption and authentication, it does not address many of the challenges faced with a large-scale DER deployment. Additional research is needed to address these key challenges enumerated below:

- *Device discovery and key management:* The large number of DER devices requires that utilities implement auto-discovery techniques to ensure they can easily connect with a large number of devices. However, this requires the pre-establishing trust between device manufacturers, utilities, and consumers. Techniques are needed to securely distribute cryptographic keys and manage them through the system's life cycle.
- *Long protocol lifespans:* While DER devices will have long lifespans, often cryptographic protocols require periodic updates to address new attacks. For example, TLS has a long history of critical vulnerabilities due to the complexity of its protocols. The current version 1.2 has numerous concerns with weak ciphers and modes of operations. Fortunately, version 1.3 addresses these issues, by encryption and authentication in sequence, rather than combined authenticated encryption with associated data support.
- *Network availability:* Current AMI networks have strong integrity and confidentiality requirements, but do not have strong availability, because smart metre operations typically do not have timely operations. However, utility-controlled smart inverter functions have greater availability needs because they will probably be used to maintain grid stability. Therefore, techniques to ensure high network availability maybe required to support key DER functions.

4.1.2 Cyber-layer attack detection: Techniques to detect DER cyber-attacks should expand on previously researched attack detection methods demonstrated for the smart grid, while tailoring them to the salient DER communication and control properties. Techniques should be developed to monitor both the network communications and the various control devices within the utility and deployed at the DER locations; however, the utility will likely have limited control over many of these devices. Fig. 6 demonstrates how data from various sources can be collected and sent to the control centre and then be analysed for potential attacks. Key data sources that could be used to detect potential attacks include WAN network, smart inverters, smart meters, and SCADA measurements.

Specification-based techniques can be used to model expected system behaviour (e.g. Petri net and hybrid automata) and compare observed events against these models. Specification-based techniques have already demonstrated their effectiveness against smart meters and AMI [19]; however, new models and analysis techniques are necessary to support DER. In particular, specification-based models will be proposed for various DER communication protocols (e.g. SEP 2.0, IEC 61850-70-9, and DNP3), communication patterns (e.g. unicast and multicast), and coupling points (e.g. electric coupling point (ECP) and point of common coupling (PCC)). Anomaly-based techniques will also be explored to detect DER attacks that may not be easily inferred from specification-based approaches. We will explore statistical models and machine learning techniques to identify anomalies and malicious events within the various collected data sources. Anomaly-based techniques will be tailored to address the false positives and false negatives that commonly underlie many modern IDS techniques [36].

4.1.3 Cyber-layer attack response: Cyber response strategies can be deployed to send different control messages to various devices or modify the network based on the type, scope, and confidence level of an attack. Many techniques can be used to modify the network topology in response to potentially malicious nodes. Since the utility WANs often use wireless mesh networks that depend on distributed routing algorithms, disconnecting malicious devices presents challenges. Therefore, algorithms are necessary to rebuild mesh routes around malicious devices. Besides, other responses such as shutting down the network, turning off computers, isolating the network, smart manual activities to replace automated activities, and ensuring that systems providing essential services remain operational so long as they are directly affected by the failure or attack can also be applied under a cyber-attack [17].

4.2 Physical device layer attack resilience

4.2.1 Physical device layer attack prevention: Smart inverters are usually designed to fulfil multiple control objectives. For example, PV inverters can achieve anti-islanding detection and low-/high-voltage ride through. One major problem is that these multiple functionalities may conflict with each other under certain grid conditions. An example is that the volt–var function, frequency–watt function, or low-voltage ride through may make anti-islanding detection less effective [37]. Unintentional islanding of distributed generation, which is not permitted by the existing IEEE standards such as IEEE 1547, can result in personnel safety hazards, equipment damage, and interference with grid protection devices. Thus, this can be an important vulnerability that an attacker can use to produce a high impact.

To solve this problem, the degree of freedom needs to be increased and functions need to be realised more independently. As shown in Fig. 7*a*, an additional power electronic interface inverter called an energy buffer can be developed to provide functionalities including: (i) low-/high-frequency ride through, (ii) low-/high-voltage ride through, (iii) harmonic distortion, (iv) unbalance distortion, and (v) anti-islanding. The energy buffer will be powered by energy storage and can be flexibly connected at

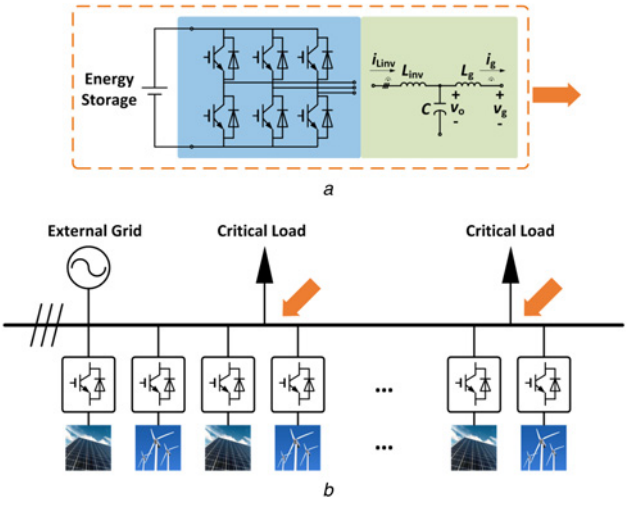

Fig. 7 *Energy buffer*
a Configuration of electric buffer
b Connection of electric buffers at the critical loads

different locations in distribution grids such as the connecting points of sensitive devices, the critical PCC, and the coupling point of the distribution system, as shown in Fig. 7*b*. By moving some functionalities of smart inverters to an energy buffer and separating the functionalities in different devices, we expect that the functionality conflicts can be eliminated.

4.2.2 Physical device layer attack detection: Various DER control devices such as smart inverters must be monitored for malicious activity (e.g. malware) that could manipulate the operation of DER without the knowledge of the system owner or utility. To detect the attack at the physical device layer, smart inverter design must be enhanced to monitor the local system status such that the cyber threats can be detected at an early stage. In particular, smart inverters can measure the local voltage and current to detect system anomalies. In this anomaly-based approach, the indices of power quality, voltage–current unbalance, and other events will be designed to identify the cyber-attacks. Furthermore, the energy buffers, as shown in Fig. 7 will also be used to enhance the detection of cyber-attacks at critical buses or the point of common coupling.

4.2.3 Physical device layer attack response: Apart from eliminating the conflicts between different functionalities of the smart inverters, the energy buffer can also be used to improve the fault ride-through capability and further strengthen the system's ability to survive cyber-attacks. The fault can be voltage–frequency sag–swell, harmonic distortion, unbalance distortion, or unintentional islanding. A detailed implementation is shown in Fig. 8. On the basis of device-level detection, different faults will be identified, and corresponding device-level control algorithms will be designed to enable fault response. An index matrix can be developed to summarise the criteria of the physical device layer and should be customised for cybersecurity study by featuring a wider scope compared with the criteria required by the existing IEEE standards.

Meanwhile, coordination between fault response using energy buffers and conventional protective devices should also be considered. The protective functions of the energy buffer will be focused on localised fault response, while the conventional protective devices are used to prevent further fault propagation in a larger area of the system.

4.3 Utility layer attack resilience

4.3.1 Utility layer attack prevention: With a large number of DER devices integrated into the distribution grid, there will be tighter interdependence between cyber and physical systems and thus a deep understanding of the physics of the grid is indispensable in preventing high-impact attacks on DER. If an attacker has information about which DER systems are more vulnerable, he/she will be able to launch an attack on one or several of the most vulnerable DER systems to cause widespread outage propagation. Fortunately, the system operators should better understand their system and can perform a thorough analysis to identify the most vulnerable DER systems.

- *Identify the DER systems that play important roles in fault propagation:* Since the distribution grid with DER integration is operated under physical laws, the outage propagation triggered by cyber-attacks on DER systems should have patterns and traces. These useful patterns can be extracted by applying and extending previous work on the transmission system interaction network and interaction model [38, 39], based on the developed cyber-physical models. Using the samples describing the fault propagation, the interaction network can be obtained by advanced statistical algorithms. The DER systems can be ranked and the key DER systems can be identified. By enhancing the cybersecurity of the identified most vulnerable DER systems, the overall system security will be greatly enhanced.
- *Identify the load buses that can influence the system stability most:* On the basis of the linearised transmission system dynamic model, the sensitivity between the largest real part of the eigenvalues and the load change at various buses can be analytically calculated, which can be further used to identify the load buses that can negatively impact the small-signal stability most. Similarly, based on the transmission system steady-state model, the load buses that have the lowest voltage stability margins can also be identified. On the basis of these identified load buses, targeted protection should be implemented for the DER devices that are connected to them in order to prevent the attacker from launching attacks against those load buses under which significant impact is produced at the lowest cost.

4.3.2 Utility layer attack detection: Anomalies within the physical distribution grid can also be used to help identify cyber-attacks. If attacks are beginning to manipulate the operation of DER, a variety of traditional power meters on the distribution grid, along with a large number of smart metres and micro-PMUs, can be used to infer which DER devices and consumers are misoperating and what malicious functions they are performing. Historical data describing the operation of DER can also help detect anomalies and potential attacks. Owing to inaccurate or even unavailable distribution

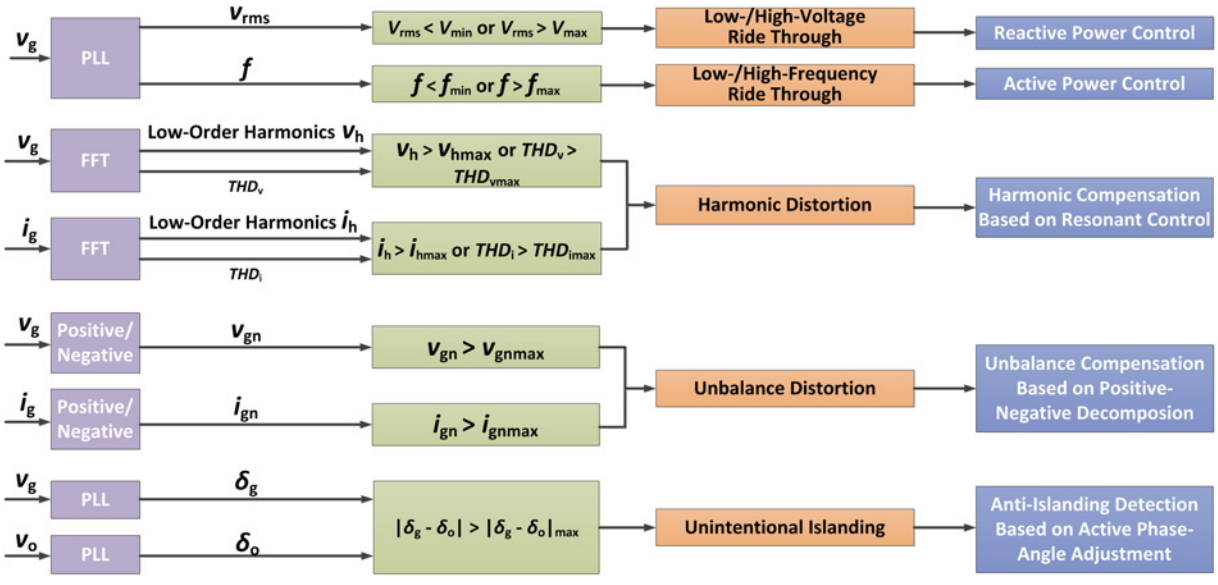

Fig. 8 *Energy buffer for attack response*

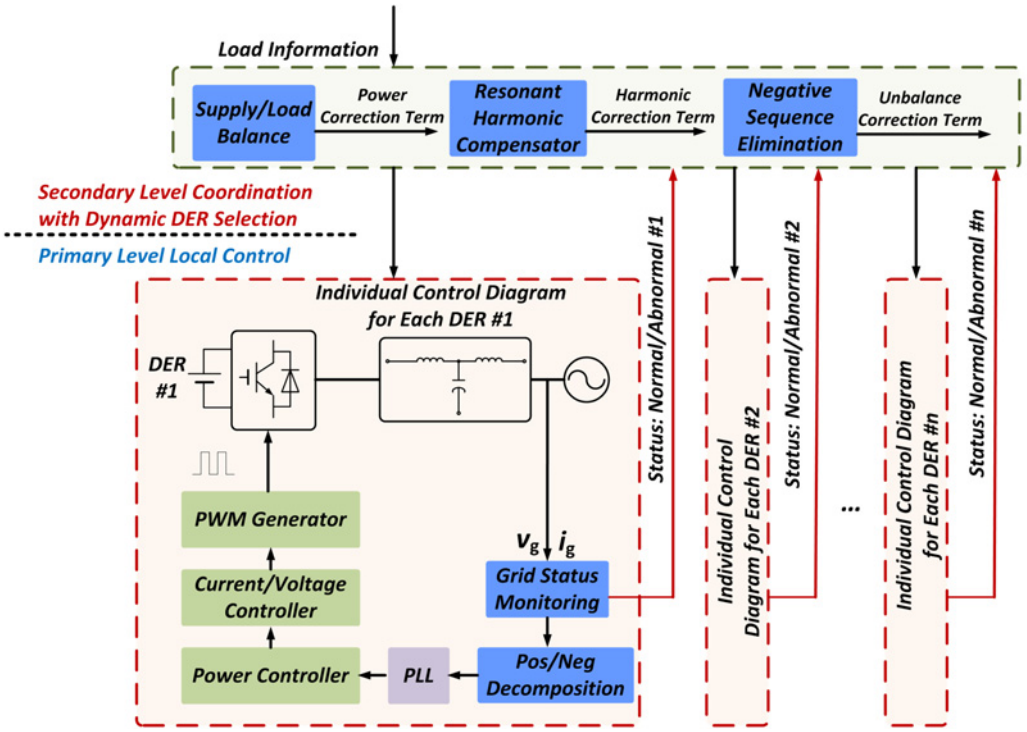

Fig. 9 *Coordinated hierarchical control for DER*

grid and DER system models, an insufficient number of sensors, and DER operation that closely depends on weather conditions, it is difficult to accurately estimate and predict dynamic states of the distribution grid using dynamic SE [40–43] for early detection of anomalies. Therefore, it is better to predict the DER system states and anomalies by data-driven approaches and advanced data analytics to detect potential cyber-attacks on DER:

- *Real-time intrusion detection based on forecasting model:* Accurate PV power generation forecasting can help detect anomalies in PV operation at the aggregated level, which can be performed by statistical [44–46], artificial intelligence [47, 48], physical [49, 50], and hybrid approaches [51–54].
- *Real-time intrusion detection by machine learning algorithms:* Supervised learning, unsupervised learning, or statistics-based learning approaches can be developed by using the collected smart meter and micro-PMU data. Well-known machine learning techniques such as support vector machine (SVM), self-organising maps, decision trees, naïve Bayes networks, and ensemble classifiers need to be evaluated to guide the selection of techniques that are most suitable for DER intrusion detection. Techniques should be developed to increase the reliability and detection accuracy of the IDS and to reduce the false-alarm rate.

4.3.3 Utility layer attack response: When there are major outages caused by targeted DER cyber-attacks or attacks on WAMPAC applications, relying only on cyber- or device-level response will be insufficient; a coordinated control at the microgrid level or utility level will be necessary, depending on how great and widespread the impact of a cyber-attack is:

- *Coordinated hierarchical emergency control for DER:* Although hierarchical control has been widely employed in AC and DC microgrids [55], it mainly focuses on steady-state operation such as active and reactive power sharing or voltage deviation elimination, but may not be resilient against cyber-attacks. To address this problem, an enhanced hierarchical control architecture such as the one shown in Fig. 9 can be developed to achieve flexible operation of DER when a cyber-attack has produced a large impact or is continuing to cause outages.
- In this control hierarchy, an enhanced secondary control diagram can be developed to improve the transient performance of the system, especially when the DER affected by a cyber-attack is disconnected. By monitoring the status of each DER unit, three compensating terms (i.e. a power mismatch correction term, a harmonic correction term, and an unbalance correction term), which are mainly designed and generated to mitigate the transient issue, will be added to the reference values in the primary control level. In addition, the secondary control will run in real time to deal with the sequential disconnection of several DER if continuous cyber-attacks exist in the system.
- *Corrective control to improve system stability:* After the anomalies of DER operation have been detected and the system stability has been impacted to some extent, corrective control can be performed for the centralised generators in the transmission system or for those trusted DER to counteract the malicious attacks. The optimal dispatch strategies can be obtained by solving an optimal power flow with stability constraints [56]. Efficient algorithms can be developed to solve the corresponding optimisation problem, which are non-linear and non-smooth. Alternatively, sensitivities between the stability margin and the control strategies obtained offline can also be used to implement quick and effective re-dispatch strategies, so as to prevent outage propagation or other severe consequences as much as possible.

5 Conclusion

Before large-scale integration of DER, we should first address its cybersecurity issues and make sure that the system is still reliable and secure with a high DER penetration. In this paper, we propose an architecture of the cyber-physical power system with a huge number of DER, discuss the unique cybersecurity challenges introduced by DER integration, and summarise the important attack scenarios against the DER and the power grid. On the basis of these, we propose a DER cybersecurity research framework that is composed of cyber-threat modelling, resilience analysis, and attack prevention, detection, and response specifically designed for DER integration at the cyber, physical device, and utility layers of the power system.

6 Acknowledgments

This work is supported by U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability.

7 References

1 North American Electric Reliability Corporation (NERC): 'Cyber attack task force – final report'. Technical Report, 2012. Available at http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf

2 Baker, S., Waterman, S., Ivanov, G.: 'In the crossfire: critical infrastructure in the age of cyber war'. Technical Report, 2009, McAfee. Available at: https://www.resources2.secureforms.mcafee.com/LP=2733

3 Carreras, B.A., Lynch, V.E., Dobson, I., *et al.*: 'Critical points and transitions in an electric power transmission model for cascading failure blackouts', *Chaos: Interdiscip. J. Nonlinear Sci.*, 2002, **12**, (4), pp. 985–994

4 Qi, J., Mei, S., Liu, F.: 'Blackout model considering slow process', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 3274–3282

5 Qi, J., Dobson, I., Mei, S.: 'Towards estimating the statistics of simulated cascades of outages with branching processes', *IEEE Trans. Power Syst.*, 2013, **28**, (3), pp. 3410–3419

6 U.S. Department of Energy (DOE) – Energy Sector Control Systems Working Group: 'Roadmap to Achieve Energy Delivery Systems Cybersecurity'. Technical Report, 2011. Available at http://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

7 North American Electric Reliability Corporation (NERC): 'Critical Infrastructure Protection (CIP) Standards', 2015. Available at http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

8 National Institute of Standards and Technology (NIST): 'NISTIR 7628 Revision 1: Guidelines for Smart Grid Cyber Security', 2014. Available at https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

9 National Electric Sector Cybersecurity Organization Resource (NESCOR): 'Wide area monitoring, protection, and control systems (WAMPAC) – standards for cyber security requirements', 2012. Available at http://www.smartgrid.epri.com/doc/ESRFSD.pdf

10 Taft, J.D., Becker-Dippmann, A.: 'Grid architecture, release 3.0'. Pacific Northwest National Laboratory (PNNL) Report 24044, 2015. Available at http://www.gridarchitecture.pnnl.gov/media/white-papers/Grid%20Architecture%20%20-%20DOE%20QER.pdf

11 Hawaii State Energy Office: 'Hawaii energy facts & figures', 2015. Available at http://www.energy.hawaii.gov/wp-content/uploads/2011/10/FF_May2016_FINAL_5.13.16.pdf

12 California Energy Commission: 'Renewable energy – overview', 2016. Available at http://www.energy.ca.gov/renewables/tracking_progress/documents/renewable.pdf

13 New York State (NYS) Department of Public Service: 'Reforming the energy vision'. Report, 14-M-0101, 2014. Available at http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688/FILE/ATTK0J3L.pdf/Reforming%20The%20Energy%20Vision%20(REV)%20REPORT%204.25.%2014.pdf

14 California Public Utilities Commission (CPUC): 'Recommendations for updating the technical requirements for inverters in distributed energy resources: smart inverter working group recommendations', 2013. Available at http://www.energy.ca.gov/electricity_analysis/rule21/documents/recommendations_and_test_plan_documents/Recommendations_for_updating_Technical_Requirements_for_Inverters_in_DER_2014-02-07-CPUC.pdf

15 National Electric Sector Cybersecurity Organization Resource (NESCOR): 'Electric sector failure scenarios and impact analyses', Version 1.0, Electric Power Research Institute (EPRI), 2013. Available at http://www.smartgrid.epri.com/doc/NESCOR%20failure%20scenarios09-13%20finalc.pdf

16 Cleveland, F., Lee, A., National Electric Sector Cybersecurity Organization Resource (NESCOR): 'Cyber security for DER systems', Version 1.0, Electric Power Research Institute (EPRI), 2013. Available at http://www.smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf

17 International Electrotechnical Commission (IEC), IEC TR 62351-12:2016: resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems, Edition 1, 2016

18 Grochocki, D., Huh, J.H., Berthier, R., *et al.*: 'AMI threats, intrusion detection requirements and deployment recommendations'. Third Int. Conf. Smart Grid Communications, Tainan city, Taiwan, November 2012, pp. 395–400

19 Berthier, R., Sanders, W.H., Khurana, H.: 'Intrusion detection for advanced metering infrastructures: requirements and architectural directions'. First Int. Conf. Smart Grid Communications, October 2010, pp. 350–355

20 Seal, B., Cleveland, F., Hefer, A.: 'Distributed energy management (DER): advanced power system management functions and information exchanges for inverter-based DER devices, modelled in IEC 61850-90-7', 2014. Available at http://www.xanthus-consulting.com/Publications/documents/Advanced_Functions_for_DER_Inverters_Modeled_in_IEC_61850-90-7.pdf

21 Eibl, G., Engel, D.: 'Influence of data granularity on smart meter privacy', *IEEE Trans. Smart Grid*, 2015, **6**, (2), pp. 930–939

22 Sun, H., Guo, Q., Zhang, B., *et al.*: 'Master-slave-splitting based distributed global power flow method for integrated transmission and distribution analysis', *IEEE Trans. Smart Grid*, 2015, **6**, (3), pp. 1484–1492

23 Li, Z., Wang, J., Sun, H., *et al.*: 'Transmission contingency analysis based on integrated transmission and distribution power flow in smart grid', *IEEE Trans. Power Syst.*, 2015, **30**, (6), pp. 3356–3367

24 Sridhar, S., Govindarasu, M.: 'Model-based attack detection and mitigation for automatic generation control', *IEEE Trans. Smart Grid*, 2014, **5**, (2), pp. 580–591

25 Buldyrev, S.V., Parshani, R., Paul, G., *et al.*: 'Catastrophic cascade of failures in interdependent networks', *Nature*, 2010, **464**, (7291), pp. 1025–1028

26 Qi, J., Ju, W., Sun, K.: 'Estimating the propagation of interdependent cascading outages with multi-type branching processes', *IEEE Trans. Power Syst.*, doi: 10.1109/TPWRS.2016.2577633

27 Eftekharnejad, S., Vittal, V., Heydt, G.T., *et al.*: 'Small signal stability assessment of power systems with increased penetration of photovoltaic generation: a case study', *IEEE Trans. Sustain. Energy*, 2013, **4**, (4), pp. 960–967

28 Kawabe, K., Tanaka, K.: 'Impact of dynamic behavior of photovoltaic power generation systems on short-term voltage stability', *IEEE Trans. Power Syst.*, 2015, **30**, (6), pp. 3416–3424

29 Tamimi, B., Canizares, C., Bhattacharya, K.: 'System stability impact of large-scale and distributed solar photovoltaic generation: the case of Ontario, Canada', *IEEE Trans. Sustain. Energy*, 2013, **4**, (3), pp. 680–688

30 Barker, P.P., Mello, R.W.D: 'Determining the impact of distributed generation on power systems. I. Radial distribution systems'. IEEE Power Engineering Society Summer Meeting, 2000, pp. 1645–1656

31 Seguin, R., Woyak, J., Costyk, D., *et al.*: 'High-penetration PV integration handbook for distribution engineers'. NREL/TP-5D00-63114, National Renewable Energy Laboratory (NREL), 2016. Available at http://www.nrel.gov/docs/fy16osti/63114.pdf

32 Hajahmed, M.A., Illindala, M.S.: 'The influence of inverter-based DGs and their controllers on distribution network protection'. IEEE Industry Applications Society Annual Meeting, October 2013

33 Saltzer, J.H., Schroeder, M.D.: 'The protection of information in computer systems', *Proc. IEEE*, 1975, **63**, (9), pp. 1278–1308

34 ARM Limited: 'Building a secure system using TrustZone technology'. Report, PRD29-GENC-009492C, ARM Limited, 2016. Accessed: http://www.infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf

35 GlobalPlatform: 'TEE internal API specification v1.0', 2008. Available at http://www.globalplatform.org/specificationsdevice.asp

36 Axelsson, S.: 'The base-rate fallacy and the difficulty of intrusion detection', *ACM Trans. Inf. Syst. Secur.*, 2000, **3**, (3), pp. 186–205

37 Sandia National Laboratories: 'Accelerating development of advanced inverters: evaluation of anti-islanding schemes with grid support functions and preliminary laboratory demonstration', 2013. Available at http://www.prod.sandia.gov/techlib/access-control.cgi/2013/1310231.pdf

38 Qi, J., Sun, K., Mei, S.: 'An interaction model for simulation and mitigation of cascading failures', *IEEE Trans. Power Syst.*, 2015, **30**, (2), pp. 804–819

39 Ju, W., Qi, J., Sun, K.: 'Simulation and analysis of cascading failures on an NPCC power system test bed'. IEEE PES General Meeting, Denver, CO, 2015

40 Ghahremani, E., Kamwa, I.: 'Local and wide-area PMU-based decentralized dynamic state estimation in multi-machine power systems', *IEEE Trans. Power Syst.*, 2016, **31**, (1), pp. 547–562

41 Sun, K., Qi, J., Kang, W.: 'Power system observability and dynamic state estimation for stability monitoring using synchrophasor measurements', *Control Eng. Pract.*, 2016, **53**, pp. 160–172

42 Qi, J., Sun, K., Wang, J., *et al.*: 'Dynamic state estimation for multi-machine power system by unscented Kalman filter with enhanced numerical stability', *IEEE Trans. Smart Grid*, doi: 10.1109/TSG.2016.2580584

43 Taha, A.F., Qi, J., Wang, J., *et al.*: 'Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs', *IEEE Trans. Smart Grid*, doi: 10.1109/TSG.2016.2570546

44 Campbell, S.D., Diebold, F.X.: 'Weather forecasting for weather derivatives', *J. Am. Stat. Assoc.*, 2005, **100**, (469), pp. 6–16

45 Huang, R., Huang, T., Gadh, R., *et al.*: 'Solar generation prediction using the ARMA model in a laboratory-level micro-grid'. Third Int. Conf. Smart Grid Communications, Tainan city, Taiwan, November 2012, pp. 528–533

46 Box, G.E.P., Jenkins, G.M., Reinsel, G.C.: 'Time series analysis: forecasting and control' (John Wiley & Sons, 2015)

47 Hornik, K., Stinchcombe, M., White, H.: 'Multilayer feedforward networks are universal approximators', *Neural Netw.*, 1989, **2**, (5), pp. 359–366

48 Benghanem, M., Mellit, A.: 'Radial basis function network-based prediction of global solar radiation data: application for sizing of a stand-alone photovoltaic system at Al-Madinah, Saudi Arabia', *Energy*, 2010, **35**, (9), pp. 3751–3762

49 Lorenz, E., Hurka, J., Heinemann, D., *et al.*: 'Irradiance forecasting for the power prediction of grid-connected photovoltaic systems', *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, 2009, **2**, (1), pp. 2–10

50 Bin Mohd Shah, A.S., Yokoyama, H., Kakimoto, N.: 'High-precision forecasting model of solar irradiance based on grid point value data analysis for an efficient photovoltaic system', *IEEE Trans. Sustain. Energy*, 2015, **6**, (2), pp. 474–481

51 Benmouiza, K., Cheknane, A.: 'Small-scale solar radiation forecasting using ARMA and nonlinear autoregressive neural network models', *Theor. Appl. Climatol.*, 2016, **124**, (3), pp. 945–958

52 Ji, W., Chee, K.C.: 'Prediction of hourly solar radiation using a novel hybrid model of ARMA and TDNN', *Sol. Energy*, 2011, **85**, (5), pp. 808–817

53 Bouzerdoum, M., Mellit, A., Massi Pavan, A.: 'A hybrid model (SARIMA–SVM) for short-term power forecasting of a small-scale grid connected photovoltaic plant', *Sol. Energy*, 2013, **98**, pp. 226–235

54 Bacher, P., Madsen, H., Nielsen, H.A.: 'Online short-term solar power forecasting', *Sol. Energy*, 2009, **83**, (10), pp. 1772–1783

55 Guerrero, J.M., Vasquez, J.C., Matas, J., *et al.*: 'Hierarchical control of droop-controlled AC and DC microgrids – a general approach toward standardization', *IEEE Trans. Ind. Electron.*, 2011, **58**, (1), pp. 158–172

56 Li, P., Qi, J., Wang, J., *et al.*: 'An SQP method combined with gradient sampling for small-signal stability constrained OPF', *IEEE Trans. Power Syst.*, doi: 10.1109/TPWRS.2016.2598266