Cyber Security in Control of Grid-Tied Power Electronic Converters - Challenges and Vulnerabilities

Sahoo, Subham; Dragicevic, Tomislav; Blaabjerg, Frede

Published in:
I E E E Journal of Emerging and Selected Topics in Power Electronics

DOI (link to publication from Publisher):
10.1109/JESTPE.2019.2953480

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Citation for published version (APA):
Sahoo, S., Dragicevic, T., & Blaabjerg, F. (2021). Cyber Security in Control of Grid-Tied Power Electronic Converters - Challenges and Vulnerabilities. *I E E E Journal of Emerging and Selected Topics in Power Electronics*, *9*(5), 5326 - 5340. Article 8901166. https://doi.org/10.1109/JESTPE.2019.2953480

Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities

Subham Sahoo, *Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—Grid tied power electronic converters are key enabling technologies for interfacing renewable energy sources, energy storage, electrical vehicles, microgrids and high voltage dc transmission lines with the electrical power grid. As number of power converters in modern grids continually increase, their monitoring and coordinated control in a way to support the grid have become topics of increased practical and research interest. In connection with this, latest standards have also defined mandatory set of control parameters for grid-tied converters, which should be adjustable by a remote entity that sends commands through a communication network. While such remote control capability allows many new control functions in grid tied converters, it also renders them vulnerable to cyber attacks. The aim of this paper is first to shed light on portions of the power converter control systems that are vulnerable to cyber attacks. Next, typical cyber-attacks are overviewed by considering different applications of grid-tied converters. Further, the impact of different types of cyber attacks on grid support functions is studied. Finally, the paper is concluded with summary and recommendation for further research.**

***Index Terms*—Voltage source converters (VSCs), Cyber-physical systems, Distributed generation, Cyber attacks.**

I. Introduction

ONE of the most important global technological goals in this century is to realize carbon-neutral electrical power systems. This will not only reduce the pollution and global warming effects, but will also decrease the overall societal dependency on insecure supply of fossil fuels. Large-scale adoption of renewable energy sources (RES) like wind and photo-voltaic (PV), energy storage systems (ESSs), electrical vehicles (EVs) and high-voltage dc (HVDC) transmission systems are seen as crucial initiatives to reach this goal [1].

Grid-tied voltage source converters (VSCs) play a key role in this scenario, since they serve as the most common energy conversion interfaces between these technologies and the electrical power grid [2]. It is also worth mentioning that VSCs enable the formation of intelligent microgrids (MGs), which are seen as intermediate aggregation entities that can operate either in stand-alone mode or facilitate large-scale integration of distributed energy resources in grid-tied mode [3], [4]. However, as the number of VSCs in renewable-based power grids increase, their influence on performance of such grids also becomes more pronounced. With the grid modernization being carried out swiftly, multiple VSCs are being integrated into the existing utility network to yield grid-supportive services.

This work was supported by THE VELUX FOUNDATIONS under the VILLUM Investigator Grant – REPEPS (Award Ref. No.: 00016591).

S Sahoo, T Dragičević and F Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark. (e-mail: sssa@et.aau.dk, tdr@et.aau.dk and fbl@et.aau.dk)

Further, with the ever-increasing convenience of remote control capabilities using information communication technologies (ICT), the flexibility of operation and robustness of control of VSCs has greatly improved. The integration of these facilities have actually led to a plight, which creates a direct trade-off between efficiency, reliability and security for larger interconnected network of VSCs. In fact, such large scale monitoring using supervisory control and data acquisition (SCADA) makes it highly susceptible to malicious intrusions. Moreover, the reliability factor involved with deep integration of the communication layers to achieve coordination also play a vital role in new security concerns. Such threats ranging from thefts, cyber attacks may result in system shutdown, cascaded failure, damage to the consumer loads, endangered energy market operation, etc. [5]. Many cyber accidents of power blackouts in Brazil have been reported in [6], such as the SQL Slammer worm attack, the Stuxnet attack and various industrial calamities. Furthermore, it has been claimed in the McAfee Report [7] that 80% of the utility companies have undergone at least one denial of service (DoS) attacks in their communication network with 85% of units' data infiltrated by an adversary. As the most prominent mode of communication in smart grids is wireless, IT security clients are managing various data protection plans to handle the unreliability of data transmission systems. However, intelligently modeled cyber attacks with plentiful system information creates disparity in securing the electric grid as they easily bypass the model verification tests [8]. It emanates additional vulnerabilities in the smart grid from a control systems perspective, albeit the newly IT secure verification methods.

Intelligent attacks often target the physical layer to maneuver the system stability as concealed disorder and uncertainties. Accounting considerable timescale separation of control stages of VSC under a value of no more than 0.1 seconds, this mandates detection of cyber attacks in a timely manner to avoid unnecessary system casualties. Apart from the said casualties, it also breaches confidentiality and optimality of system operation almost immediately on one hand. On the other hand, as the penetration of intelligent attacks go on in a stealth manner, which goes undetected by control-theoretic solutions, the attacker may initiate the attack during slightly alarming conditions to arrange an extreme case of system shutdown. Such cases are brought into perspective considering planning alternatives and power back-up options. Hence, appropriate design of reliable, resilient and intelligent control methodologies for VSC needs to be the current focus to tackle such critical security issues.

For the purpose of better understanding of security problems in power electronics based cyber-physical systems, this paper discuss the following:

1) control and operational challenges faced by the VSCs used in different applications due to cyber attacks.
2) a brief overview of the vulnerabilities in the control and cyber layer of VSCs (in grid-connected and standalone mode) is provided. Further, more aspects on how it disorients their operation from the state of normalcy is detailed.
3) directions and viewpoints, especially in the design of resilient control formulation for VSCs.

The rest of the paper is organized as follows. Typical structure of a power electronic based system with a detailed overview on their various roles is presented in Section II. The impact and vulnerability analysis of the control, communication and physical layer used to handle VSCs are revealed in Section III. Further, the challenges faced due to cyber attacks for different VSC applications are demonstrated using few case studies in Section IV. Finally, the conclusions and recommendations for future research are given in Section V.

II. Cyber-Physical Architecture of Power Electronic Converters

A typical architecture of individual ac grid-connected voltage-source-converter system is shown in Fig. 1. The overall power conversion chain consists of several stages, i.e. the input stage, input-side power converter stage, dc voltage stage, the grid-tied VSC stage, the ac grid stage and the cyber stage. This type of power electronic architecture is most commonly used for interfacing RES like wind and PV [9], ESSs [10] and EV charging infrastructure with the electric power grid [11]. With aims to improve the resiliency and robustness of smart grids, it is expected that in the near future individual VSC systems will be interconnected together through communication links into a singular all-inclusive cyber-physical smart grid. Aforementioned control stages are briefly described below:

A. Physical Stage

The exemplary input power sources/sinks are located on the far left side of Fig. 1. Some units in the input stage such as grid or ESS can either inject or absorb the electric power.

The power exchange between the input side and the intermediate dc stage is regulated by the input-side converters. These converters process the power exchange between the input stage and the dc voltage stage. Further, DC stage serves as a power buffer between the input and the ac stage. It can also operate independently from the ac stage, e.g. as a dc microgrid [12]. To integrate the sources from input stage into the grid, grid-tied VSC serves as an interface between the dc-link stage and the ac electric power grid.

Their output is connected through the interface filter either to an ac electrical power grid, ac microgrid, or to standalone

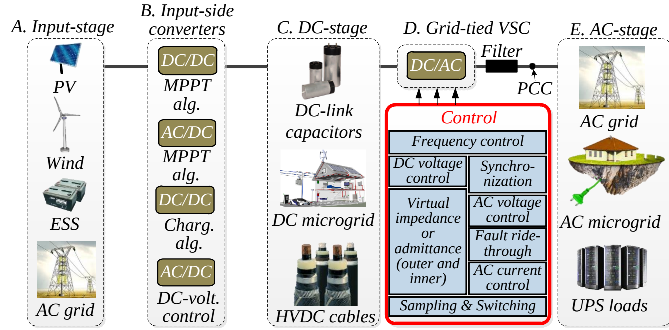


Fig. 1. Control and physical stages in an individual grid-tied voltage-source-converter (VSC) system.

ac loads, as shown in Fig. 1. Based on its interconnection with different AC stages, various standards are applicable. For electric grid, the primary concern lies with the regulation of grid current with high power qualitative signatures during transients (voltage sags, swells and unbalances) [13]. Recently, increasing number grid-ancillary services related to grid voltage and frequency support are also required [13]. On the other hand, their performance in an inertia-less autonomous system (e.g. microgrids) is essentially governed using sharing capabilities for active and reactive power, harmonics during steady-state as well as transients, etc. These objectives are met owing to the primary control associated with the abovementioned quantities, which will be discussed later in this paper.

B. Cyber Stage

We assume that smart grid as a whole comprises of numerous VSCs described in the previous section. They, together with conventional synchronous generators, jointly regulate the grid and each of these units is termed as an agent for an exemplary portion of a smart grid with interconnected VSCs.

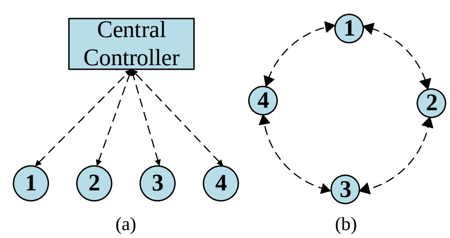


Fig. 2. Communication topologies: (a) Centralized control, (b) Distributed control.

A communication network connects the sensors and controllers co-existing in the smart grid. Each agent communicate in two ways: (a) to a central controller and, (b) among each other in a distributed manner. A pictorial description of both the cyber structures is provided in Fig. 2, where the dotted lines represent the flow of information. Since the control objectives is highly vulnerable to single point-of-failure in centralized network as shown in Fig. 2(a), the distributed control philosophy [14] in Fig. 2(b) is prominently used for

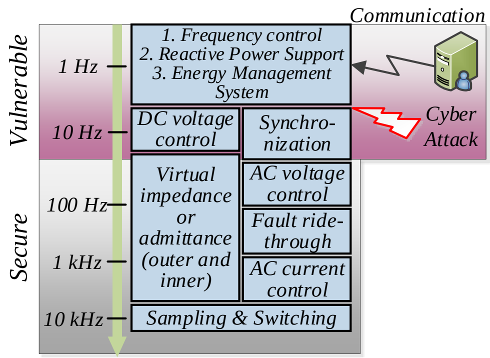


Fig. 3. Conventional control structure for two-level VSC – Secure and vulnerable control layers against cyber attacks.

power electronics based cyber-physical systems to enhance reliability and scalability.

Every agent has a distributed controller that processes data from local and neighboring agents, as well as from other remote sites. These data are normally obtained by phasor measurement units (PMUs), which comprises of dynamic voltage phasors. Communication between the PMUs and local controllers can be achieved in centralized fashion, where measurements from all the agents are collected centrally for processing and decision making. The most prominent method of coordination between agents, SCADA system is usually employed [15] to alleviate monitoring in smart grid networks. If the number of agents is high, this approach not only requires significant communication resources, but it is also prone to potential cyber-attacks. Other option, commonly referred to as decentralized control, refers to a scheme where only local measurements are used. While the communication infrastructure is completely avoided here, control capability is limited. As already explained above, a distributed control paradigm introduces flexibility since the computational resources are uniformly dispersed across the system to achieve coordination. Hence, low bandwidth communication channels can be employed to achieve the same function. Though it provides an obvious criteria of assessment of intrusion attempts, vulnerability to cyber attacks can not be necessarily guaranteed for coordinated attacks [16], [17]. This can be explained owing to insufficient information present in each node, which does not serve as adequate global information for detection of cyber attacks.

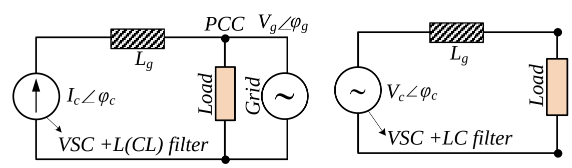
Considering the control layer, a brief overview of the control functions of ac-grid-tied VSCs in accordance with their time-scales are presented in Fig. 3. It can also be noticed that some control loops in Fig. 3 are depicted next to each other, which indicates that they are operated simultaneously (e.g. active damping and ac current control [18], dc-link voltage control and synchronization [19], or a fault-ride through and virtual impedance/admittance control [20]). More discussion on the secure and vulnerable control layers of VSC will be carried out in the next section after providing a brief theory on cyber security.

C. VSC Roles

VSCs roles in renewable-based power systems and microgrids can be divided into three main categories, i.e. grid-feeding, grid-forming and grid-supporting [21]. These roles are discussed in more detail below:

1) Grid-feeding Unit: The function of a grid feeding VSC is to inject specified amount of current into the grid. Therefore, they can be represented as current sources, as shown in Fig. 4(a). From the implementation point of view, they typically comprise an outer dc voltage control loop, a dedicated synchronization unit and an inner current control loop with embedded active or passive damping [22]. For generating the current reference, outer power controllers can also be used to supplement the dc voltage controller.

2) Grid-forming Unit: The function of grid-forming VSCs is to regulate the local voltage. Therefore, it can be represented as an ideal voltage source, as shown in Fig. 4(b). Due to its stiff voltage regulation, this type of units can be considered as a master in the system that defines the local ac grid. Therefore, grid-forming VSC does not need to have any power sharing capabilities and dedicated synchronization. From the implementation standpoint, grid-forming VSCs are typically realized via outer voltage loop and an inner current loop [23]. This functionality is typically employed as a basic philosophy in stand-alone applications, such as microgrids [24].



(a) Grid-feeding unit. (b) Grid-forming unit.

Fig. 4. Simplified representations of basic VSC types : (a) Grid feeding and (b) Grid forming VSC.

Usually for paralleled VSCs in stand-alone microgrids, a primary control law is employed for both active and reactive power to align the frequency ω^* and voltage references V^* respectively for synchronization using:

$$\omega^* = \omega_{ref} - m_p(P - P^*) \quad (1)$$

$$V^* = V_{ref} - n_q(Q - Q^*) \quad (2)$$

where ω_{ref}, V_{ref}, P^* and Q^* are the global frequency, voltage, active and reactive power references respectively. Moreover, m_p, n_q, P and Q denote the active power droop, reactive power droop, measured active and reactive power respectively.

3) Grid-supporting Unit: As opposed to the first two categories, grid-supporting VSCs involve broader spectrum of control functionalities, from grid voltage/frequency support, active/reactive power sharing to virtual inertia and impedance/admittance emulation.

III. Impact and Vulnerability Analysis of Cyber Attacks on Control of VSCs

A. Cyber-Security

With the proliferation of communication technologies, cyber disturbances are becoming a reality. As already witnessed in numerous real-world examples, such disturbances can significantly affect the performance of smart grids. With fast increase in penetration of VSC technologies, their impact on the system is reaching a point where the impact of cyber attacks cannot be ignored. In particular, researchers are focused on designing secure control methodologies apart from the traditional encryption based techniques. Generally, spoofing attacks can be caused on sensors and communication links, where the signals are either interrupted, quantized or coerced. To name a few, false data injection attacks (FDIAs) is caused by injection of auxiliary signals or changing the content in the measurements reported by the sensors [25]. When a similar activity is recognized in the communication links, it is commonly referred to as the man-in-the-middle (MITM) attack [26]. Moreover, jamming of signals can also be caused to interrupt the transmission of signals, which is commonly known as denial of service (DoS) attack [27]. These are some of the prominent attacks that has precipitated in the real-time applications. More details on other critical intrusion approaches, which are the subsets of the abovementioned attacks, can be found in [28].

To familiarize with the said intrusion approaches, cyber attacks can be conducted on sensors, smart meters and load aggregator in an active distribution network to dismantle system objectives such as, frequency regulation based ancillary services, voltage stability, power flow management, etc. Further, any adversarial outbreak into the cyber channels using various techniques, such as jamming the flow of information, altering the communicated measurements, deactivating cyber link(s) can instill system shutdown. The cautious nature of such attacks depends on various factors such as the degree of system information acquired by the attacker and the ability of the attacker to penetrate into the system particulars.

Accounting the implementation of these control layers in real-time processors, intrusion into the control layer only allows access to the reference set-points (dc-link voltage, frequency) during run-time instead of the inner control layers. As the inner loops are compiled into the read-only memory (ROM) section of the processor, intrusion into the sensor values can not dissemble the system operation. However, the system dynamics will vary when the references are changed to trigger instability or activation of the protection layer. Mathematically, this can be explained using the state-space representation of i^{th} VSC for:

$$\begin{aligned} \dot{x}_i(t) &= Ax_i(t) + Bu_i(t) \\ y_i(t) &= Cx_i(t) + Du_i(t) \end{aligned} \tag{3}$$

$\forall i \in N$, where $x_i = [v_g \;\; i_g \;\; P \;\; Q \;\; v_{dc}]^T$ and $u = [\omega^* \;\; v_{dcref} \;\; P^* \;\; Q^* \;\; E^*]^T$ with the state parameters denoted by grid voltage, grid current, active power, reactive power, dc voltage respectively; and the input consisting of the reference parameters of frequency, dc voltage, active power, reactive power and inverter voltage for i^{th} VSC respectively. Further, $x \in \mathbb{R}^N$, $u \in \mathbb{R}^M$, $y \in \mathbb{R}^S$, $A \in \mathbb{R}^{N\text{x}N}$, $B \in \mathbb{R}^{N\text{x}M}$, $C \in \mathbb{R}^{P\text{x}N}$ and $D \in \mathbb{R}^{P\text{x}M}$. Without loss of generality, we assume that each state and output variable can be independently compromised by an attacker. An attack signal $\xi_i(t) \in \mathbb{R}^{P+N}$ depends specifically upon the attack strategy. If $\Sigma = \{\xi_1, \xi_2, ..., \xi_{N+P}\}$ is a null vector, then the system response is unbiased. To detect the presence of cyber attack elements, a residual signal $r : \mathbb{R}_{\geq 0} \to \mathbb{R}^P$ test can be followed. It is worth notifying that ξ_i is not a design parameter; as it completely depends on the intent of the attacker.

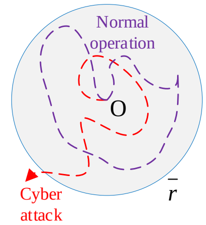


Fig. 5. Attack detection filter law - Trajectories outside $\bar{r}$ denote the presence of cyber attack.

Remark I: The nature and magnitude of attack signal can be bounded/unbounded; and is completely dependent on the motive of the attacker. However, the design of corrective control measures to ensure a resilient system is always done regardless of the nature of attack.

To detect attacks using a centralized attack detection filter based on a modified Luenberger observer, the estimated dynamics of i^{th} VSC with known initial states $x(0)$ can be given by:

$$\begin{aligned} \dot{\hat{x}}_i(t) &= (A + GC)\hat{x}_i(t) - Gy_i(t) \\ r_i(t) &= C\hat{x}_i(t) - y_i(t) \end{aligned} \tag{4}$$

where $\hat{x}_i(t)$ denote the estimated states. Further, $\hat{x}_i(0) = x_i(0)$ and the output injection matrix $G \in \mathbb{R}^{N\text{x}P}$ is such that $(A + GC)$ is Hurwitz.

Remark II: $r_i(t) \leq \bar{r}$ if and only if $\xi_i(t) = 0$ for $t \in \mathbb{R}_{\geq 0}$; where $\bar{r}$ is an infinitesimal value. It is intuitive from Fig. 5 that the normal residual test is passed for the violet trajectory since the residual value remains within the threshold $\bar{r}$. Detailed proof can be referred from [8].

Otherwise, it can be concluded that an attack element is present in the i^{th} VSC. As such attacks cause a change in the system response due to altered model, the residual element overshoots out of the shaded circle in Fig. 5 with radius $\bar{r}$. Hence, any physical disturbances such as load change, faults, line outage will always obey Remark II since the model dynamics will always be unaltered using the *unbiased* measurements during these disturbances.

On the other hand, the inner control loops are resilient to cyber attacks as it operates with a tracking objective for each state. It is worth notifying that the inner control loop is resilient to cyber attacks only when the outer control loop is unattacked, as shown in Fig. 3. Since the secondary control layer exploits communication to alter the references for outer control loop, any bad data injection into the upper control layer (highlighted with red in Fig. 3) will disorient stability or cause system shutdown. The shutdown is usually caused due to the unintentional activation of over-voltage and over-current protection layers.

Extending this theory for interconnected VSCs, the artificial dynamics created by the attack element can be nullified in (3), only when:

$$\sum_{i=1}^{N} \xi_i = 0 \tag{5}$$

holds true. Further, these attacks in the attack set Σ can be categorized as *undetectable* from the monitors, if and only if $x \in \mathbb{R}^N$ such that $||sI - A||_0 + ||Cx||_0 = \phi$, where $|\Sigma| = \phi$. Such attacks are commonly termed as *coordinated* attacks, since they easily bypass the attack filters in (4). Using (5), it can be extended that the control inputs can either be manipulated in the controller or on communication link(s) by an external entity. As the cyber and control layer are closely coupled, the susceptibility to cyber attacks aggravates for an interconnected system of VSCs. With increase in attack-vulnerable points, the ancillary support provided by interconnected VSCs can be easily misled, leading to system collapse. Such consequences eventually cause techno-economic catastrophes by maligning the electric network with the injection of false data attack vectors into cyber-physical layer. Hence, a detailed vulnerability analysis on the control of VSCs due to cyber attacks has been studied in detail in the following subsection.

B. Vulnerability Analysis of Cyber Attacks on Control of VSCs

1) Grid-forming control for VSCs: A conventional control structure for the grid-forming VSCs is shown in Fig. 4. As already explained, grid-forming VSCs regulate voltage and frequency locally. To synchronize with other AC sources, the general philosophy is to align primary droop control locally using the available measurements. From a cyber-space perspective, this decentralized arrangement is considerably safe as it is difficult for the attackers to access the physical layer. Moreover, suitable physical layer security alternatives such as beamforming is commonly used these days [29]. However, decentralized control philosophies suffer from an operational point of view in matching the commercial regulatory standards [30]. This drawback has been conceived usually by secondary controller using the information from other VSCs. Referring to the cyber structure from Section II-B, distributed or centralized secondary control architectures can be imposed on the primary control law to compensate for the offsets. However, this leaves a large vulnerable space for the attackers to locate the attacked data either into the sensors, communication link or the controller. Below are some of the common methods of intrusion approaches to manipulate each component:

- **Sensors**: The sensors' data are usually manipulated by penetration of the adversary inside the control platform. This penetration can be easily achieved by *Trojan Horse* [31] to use remote systems as host. The sensor output from the acquisition panel is usually within signed 15 V. To calibrate it against the actual measurement, acquisition gains using a linear plotting theory is used. The attacker usually attempts on changing the acquisition gains, which creates a bias in the reported measurements.
- **Communication Links**: The communicated data can be manipulated either inside the controller or in the communication stage involving a router/encoder/decoder. There are several ways in which the transmitted data can be manipulated, such as authorization violation, interruption of transmission of signals, illegitimate opening of information logs, replaying the transmitted information from the past, etc.
- **Controller**: As mentioned already, the controller can be illegitimately accessed using *Trojan Horse* to change the reference input(s) used either in the outer control loop or secondary controller for control of VSCs.

2) Grid-feeding and supporting control for VSCs: Grid-feeding control for VSCs are basically employed to inject active and reactive power into the grid-forming units. This philosophy is mostly used in grid-connected applications for integrating renewable energy sources [3]. To ameliorate grid-supportive services, the desired control inputs are added to the overlaying grid-forming controller, as shown in Fig. 7. As detailed in the previous section, the reference input v_{dcref} or sensor v_{dc} is usually vulnerable to cyber attacks, which allows the attacker to either limit or increase the power flow from VSCs thereby creating a stability/coordination issue in the network. Moreover, the outputs of grid-supportive services P_{gss} and Q_{gss} can also be compounded with false data to misinform the controlled units. The vulnerable points of attack in the control of grid-forming and grid-feeding VSCs are summarized in Table I. It is worth notifying that the measurements/references, denoted as x_j, are transmitted by other units to the upper level control either responsible for grid-supportive services or for secondary control objectives.

Using the vulnerable hotspots in control systems for VSC, the challenges faced due to cyber attacks in different fields have been studied in detail to project system outage, non-optimal operation, economic feasibility, instability, consumer discomfort, etc.

IV. Grid-Supportive Services by Multiple VSCs: Challenges from Cyber Attacks

In the previous section, the vulnerable points of cyber attack in control of VSCs have been briefly discussed. Building upon the said theory for conventionally modeled cyber attacks, this section will introduce the challenges faced by single/multiple VSCs in different fields due to cyber attacks to meet the grid-supportive services. It is worth notifying that the reference frequency f^* for all the considered cases in this paper is equal to 50 Hz. As a consequence, ω^* = 314.16 rad/s. Moreover, since the focus of this paper is based only on evaluating different control principles for VSCs in the presence of cyber attacks, each attack scenario is carried out considering the system and control parameters from the paper(s), which are consistently highlighted in the caption of results of the respective case study.

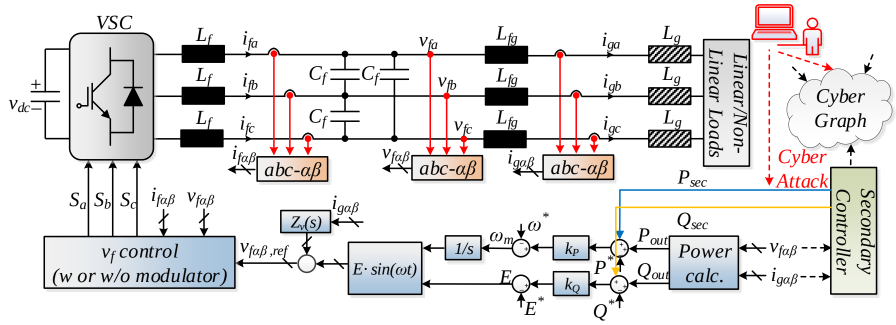


Fig. 6. Basic $V-f$ control of Grid-forming VSCs: black and red dotted lines represent the communication layer and attack elements injected into sensors/communication link respectively.

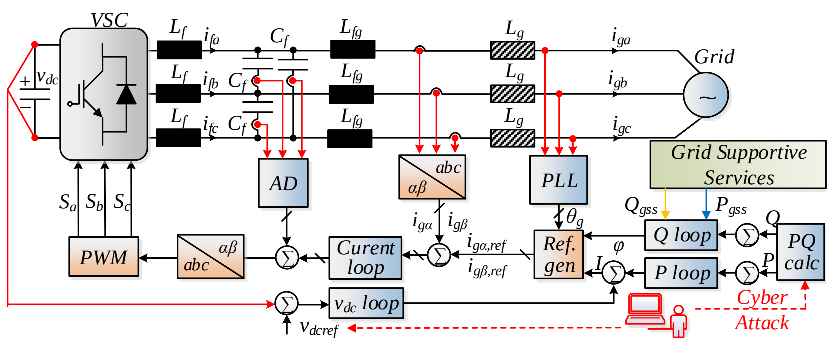


Fig. 7. Basic $P-Q$ control of grid-supportive VSCs: black and red dotted lines represent the communication layer and attack elements injected into sensors/communication link respectively.

TABLE I
VULNERABLE POINTS IN CONTROL STAGES OF DIFFERENT VSC TYPES

	Current control (Inner)	Outer control	Secondary controller	Grid-supportive services
Grid-feeding	×	v_{dc}, v_{dcref}	×	×
Grid-forming	×	P^*, Q^*	DoS [1]/MITM [2] attack on v_j, ω_j [3] FDIA [4] on v_i, ω_i, P_{sec}, Q_{sec}	×
Grid-supporting	×	×	×	P_{gss}, Q_{gss}, ω^*, E^*

[1] Denial of service, [2] Man-in-the-middle, [3] $\circ_j$ denote communicated measurements, [4] False data injection attack

A. Frequency Response and Wide Area Damping Control

As introduced before, grid frequency control can be supported by the VSC local control system. In fact, modern grid codes require converters to stay connected and to continue exchanging the power with the grid under moderate frequency deviations and rate of change of frequency (ROCOF) [13]. Moreover, VSCs must be equipped by static frequency-power droops to continually adapt to frequency variations. The implementation of such static frequency-power droop functions can be done as an outer controller with respect to virtual impedance loop [32], [33] using:

$$\omega_m = -\frac{P_{out} - P^*}{k_p} + \omega^*. \tag{6}$$

where k_p is the frequency-power droop. Moreover, ω_m, P_{out}, P^* and ω^* denote the primary frequency control output, measured active power, active power reference and reference for grid frequency, respectively. Although it provides reduced frequency nadir, static frequency-power droop characteristic does not increase the inertia of the system. In this context, virtual inertia emulation controllers have been increasingly proposed as viable substitutes for static droop controllers [34], [35], [36]. It has been shown in [?] that both controllers have identical steady-state performance, but virtual inertia has additional swing-equation type dynamics that allows reduced ROCOF, as follows:

$$P^* - k_p(\omega_m - \omega^*) - P_{out} = J\omega_m \frac{d\omega_m}{dt} + D(\omega_m - \omega_g), \tag{7}$$

where J, D and ω_g are inertia, damping constants and measured phase locked loop (PLL) grid frequency, respectively. If these constants are set to zero, (7) becomes equivalent to (6). An exemplary implementation of virtual inertia emulator in the outer control loop coupled with the filter voltage controlled VSC in the inner loop is shown in Fig. 8.

Moreover in (7), only local measurements are used to emulate the synthetic inertia. However, it has been shown that improved damping of frequency oscillations can be achieved by supplementing the local control law with measured vari-

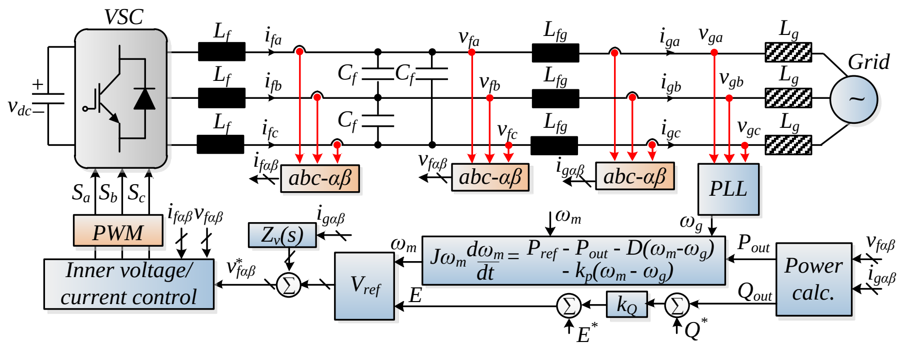


Fig. 8. Application of virtual inertia emulator combined with reactive power support in the outer loop. Since these outer loops generate the filter voltage reference $v^*_{f\alpha\beta}$, this VSC can be categorized as a unit with filter voltage control.

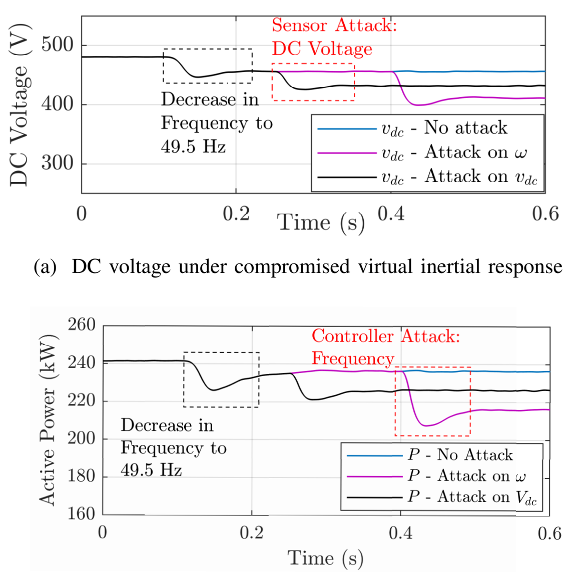
ables from other locations in the system [37]:

$$P^* - k_p(\omega_m - \omega^*) - P_{out} + u_c = J\omega_m \frac{d\omega_m}{dt} + D(\omega_m - \omega_g) \quad (8)$$

where u_c is the supplementary control signal that can be defined as follows:

$$u_c = -\alpha_i(\omega_g - \bar{\omega}). \quad (9)$$

Here α_i is a tunable parameter, while $\bar{\omega}$ is the average frequency in a given cluster of VSCs that can be computed either in centralized or distributed way. In this way, the ancillary features provided by networked VSCs can be an asset to the management and stability of power networks.



(a) DC voltage under compromised virtual inertial response

(b) Active power under compromised virtual inertial response

Fig. 9. Performance of virtual inertial response by VSCs [37] under attacks on frequency (controller attack) and DC voltage (sensor attack).

A brief overview on impact of cyber attacks on ancillary services is provided in Fig. 9. Owing to the frequency response from VSCs such as EV charging parks, the increase/decrease of active power setpoint corresponding to the change in grid frequency (from 50 to 49.5 Hz at t = 0.12 s) can be manipulated by the following FDIAs: (a) controller attack on frequency (ω), and (b) sensor attack on DC voltage sensor. These FDI attacks are basically carried out using the intrusion approach into the controller (as explained in Section III(B)) by adding a DC bias to the sensed measurement v_{dc} via the data acquisition unit or to ω obtained via PLL; thereby manipulating the control theory with illegitimate measurements. It can be seen in Fig. 9 that the virtual inertial response under attacks is subjected to further dip in DC voltages, thereby leading to decrease in active power generation. Assuming a uniform virtual inertial response based control strategy for interconnected VSCs, any false data intrusion into frequency/DC voltage contravenes the system objectives to provide grid supportive services and may even lead to instability.

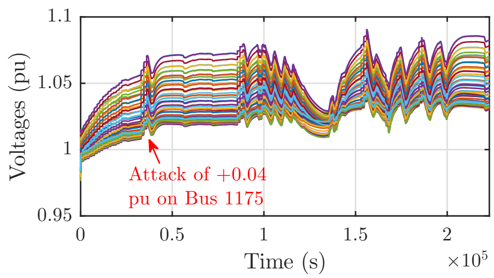
B. Coordinated Voltage and Reactive Power Control

Large scale integration of renewable energy sources owing to their intermittent nature often cause violation of voltage regulatory limits [38]. Such violation may lead to disconnection of VSCs and possibly voltage stability problems [39]. Several local voltage control strategies for VSC are discussed in [40]- [41]. However, an optimal operation is achieved only by tuning the local parameters centrally with a day-ahead prediction of renewable energy sources and load profile. Moreover, the day-ahead forecasting error could go large leading to uncoordinated control in many cases. To address these issues, robust multi-step voltage control mechanisms [42], [43] have been devised to provide reactive power support from VSCs under such scenarios. Basically, these control mechanisms for local reactive power support operate to minimize tap changes of on-load tap changer (OLTC) based on the minimum and maximum voltage setpoints. Another primary goal is to limit the voltage fluctuation inside a narrow band.

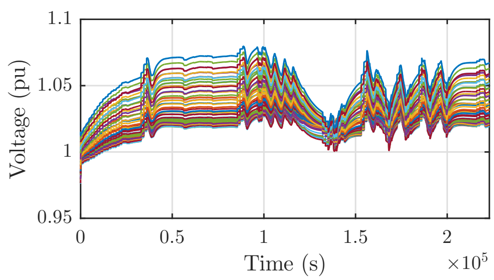
The prediction of node voltage in a distribution network considering the sensitivities of voltage with respect to reactive power Q, active power P and the number of tap changes N_p can be done using:

$$V(k+1) = V(k) + \frac{\partial V}{\partial Q}\Delta Q_{pv}(k) + \frac{\partial V}{\partial P}\Delta P_{pv}(k) + \frac{\partial V}{\partial N_p}\Delta V_p(k) \quad (10)$$

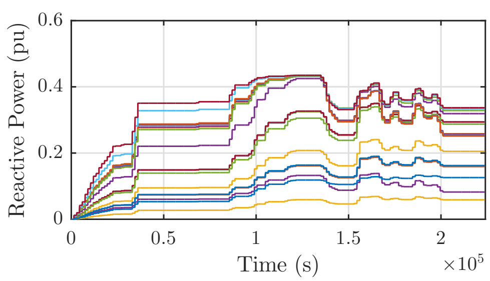
where ΔP_{pv} is a vector of predicted change in PV power at various PV locations whereas ΔQ_{pv} and ΔV_p are the control



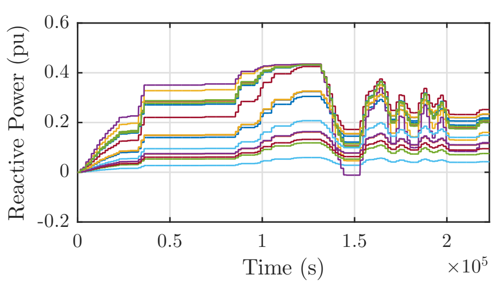
(a) Voltage of each node under attack.



(b) Voltage of each node under normal conditions.



(c) Reactive power from each VSC under attack.



(d) Reactive power from each VSC under normal conditions.

Fig. 10. Impact on United Kingdom General Distribution System (UKGDS) {test system can be found in [44]} due to false data injection on bus voltages in bus 1175 [42], [43].

variable to arrest the node voltage within the targeted limits. Considering a maximum reactive power limit for each VSC of 0.436 pu. for voltage ranging between [1, 1.05] pu., the objective function to maintain the voltages under specified limits using the control variable $\Delta u(k) = [\Delta Q_{inv}(k), \Delta V_p(k)]$ can be given by:

$$\min \sum_{i=0}^{N-1} (\Delta u(k+i) R u^T(k+i)) \tag{11}$$

where, R is a diagonal weight matrix to penalize the desired control variable.

A case study is done in Fig. 10 to analyze the steady state voltage stability when false data is injected into the bus voltage of one of the nodes. A 11 kV United Kingdom General Distribution System (UKGDS) [44] is employed as the test distribution network to analyze the impact of centralized voltage regulatory schemes. Since day-ahead PV forecasting may introduce large error in case of uncertain events, robust voltage control mechanisms have been devised to handle these uncertainties. As per the grid code compliance, PV based VSC systems start providing reactive power as an immediate solution to voltage recovery within the hard bound limits. However, compromised voltage measurements from each node represent a biased depiction of the reactive power requirements.

As shown in Fig. 10(a), when an attack of 0.04 pu is injected into the voltage measurement in bus 1175, the reactive power from each VSC increases which results in increased average voltage profile as compared to the unattacked scenario in Fig. 10(b) & (d). Under worse circumstances of large false data injected into the system, it may diverge outside the maximum voltage threshold, leading to unnecessary operation of OLTCs. Moreover, it leaves out the available reactive power reserve with interconnected VSCs, which are primarily assigned for voltage support as per grid-code compliance. On the other hand, a coordinated set of attack can also be modeled, which passes bad data detection test, such that the network operator is unaware of the presence of any attack elements. These attacks may reduce the optimal efficiency of the distribution system leading to over-utilization of back-up resources.

C. *Optimal Energy Management*

Energy management system (EMS) is an effective mechanism to handle the generation profiles of different sources while attaining their economical benefits [45], [46]. To date, generation dispatching is usually carried out in a centralized manner to minimize the operational cost using hierarchical stages of optimization including, integer programming [47], artificial intelligence based techniques [48], etc. To achieve more flexibility in control under issues such as transmission delay and information failure, distributed controllers with robust performance towards cyber layer imperfections have been preferred in recent times [49]. As opposed to longer time scales with static demand input in the centralized scheme, distributed dispatching allows online actions for every load change in real-time [50]. As a result, it improves the economic profile for optimal utilization of resources.

The active power control in each VSC is augmented with frequency restoration to minimize the generation cost for economic operation. To this end, we consider the general quadratic cost function for each DG to provide the operational cost, given by:

$$C_i(P_i) = a_i P_i^2 + b_i P_i + c_i \tag{12}$$

where a_i, b_i and c_i are the cost coefficients of i^{th} VSC. Following the generation-demand balance equality constraint, the objective of optimal load sharing is to minimize the total cost of all DGs using:

$$\min\ C(P) = \sum_{i=1}^{N} C_i(P_i) \tag{13}$$

$$\text{s.t.} \sum_{i=1}^{N} P_i = P_D,\ \ P_i^{min} < P_i < P_i^{max} \tag{14}$$

where P_D, P_i^{min} and P_i^{min} denotes the total demand in the microgrid, minimum and maximum active power for i^{th} DG respectively. Further, (13) can be solved using its associated Lagrange function as:

$$\mathcal{L}_\lambda = \sum_{i=1}^{N} C_i(P_i) + \lambda_i(P_D - \sum_{i=1}^{N} P_i) \tag{15}$$

where λ_i is the Lagrangian operator. Differentiating (15) with respect to P_i using the first-order optimality condition, we obtain the incremental cost as:

$$\lambda_i = 2a_i P_i + b_i \tag{16}$$

To minimize the total generation cost subject to the equality constraints, it is required that the incremental cost of each VSC to be equal [51], which is carried out using a power correction term ΔP_i, given by:

$$\Delta \dot{P_i} = \sum_{j\ \epsilon\ N_i} a_{ij}(\lambda_j - \lambda_i) \tag{17}$$

In (17), each agent is represented via a node and a communication digraph via edges using an adjacency matrix $A = [a_{ij}]\ \epsilon\ R^{N\times N}$. The communication weights are given by:

$$a_{ij} = \begin{cases} > 0, & \text{if } (x_i, x_j)\ \epsilon\ E \\ 0, & \text{else} \end{cases}$$

where E is an edge connecting two nodes, with x_i and x_j being the local and neighboring node respectively. The final active power reference for each DG can be designed by adding (17) to P^* in Fig. 6 to achieve the desired optimal response.

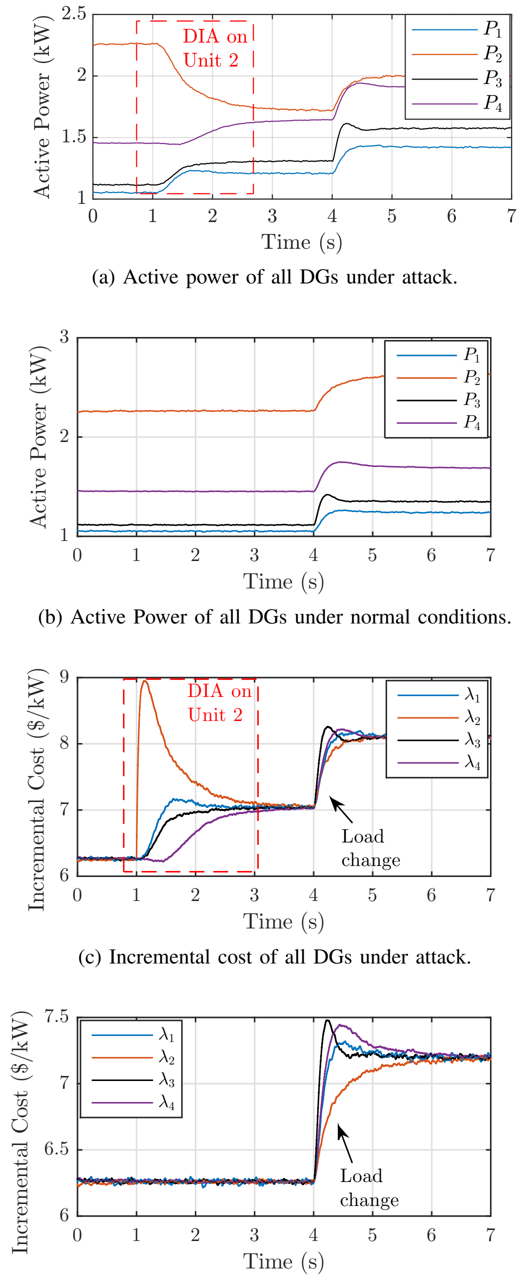
To increase the generation cost, any adversarial false data in the cooperative ED optimization model is categorized as a *data integrity attack* (DIA). Such attack alters the power flows with respect to the optimal solution. Basically using the DIA, the local incremental cost λ_i is updated in every iteration using:

$$\lambda_i(k+1) = \lambda_i(k) + \sum_{j\ \epsilon\ N_i} w_{ij}(\lambda_j(k) - \lambda_i(k)) + u^a_{\lambda_i} \tag{18}$$

where $u^a_{\lambda_i}$ is an exogenous attack input in i^{th} VSC. This can be done by changing the cost parameters in the local VSC using:

$$u^a_{\lambda_i} = \begin{cases} \Delta a_i P_i, & \text{if } u^a_{\lambda_i} = f(P_i) \\ \Delta b_i, & \text{else} \end{cases} \tag{19}$$

where Δa_i and Δb_i denote positive quantities, when added to the cost parameters in (16) increase the generation cost per unit power and fixed cost, respectively.



(a) Active power of all DGs under attack.

(b) Active Power of all DGs under normal conditions.

(c) Incremental cost of all DGs under attack.

(d) Incremental cost of all DGs under normal conditions.

Fig. 11. Comparative evaluation of active power, and incremental cost of DGs under no attack and DIA attack [50] – Change in cost parameters causes a drift in the convergence of incremental cost λ causing a non-optimal operation.

From the perspective of an adversary, the goal is to increase the generation cost by hacking critical parameters and leading to a reduction in the energy efficiency of the system [52]. Such attack vectors will create economic loss for the operator. In the context of a cooperative real-time ED, the final state of convergence ensures *unbiased* operation inside the constrained optimization space.

To provide with the basic understanding of such attacks, a case study on a microgrid with $N = 4$ VSCs in Fig. 6 is done using a DIA with increase in the cost parameters of unit 2. It can be seen that the system states achieve consensus despite the presence of DIA. The realism behind

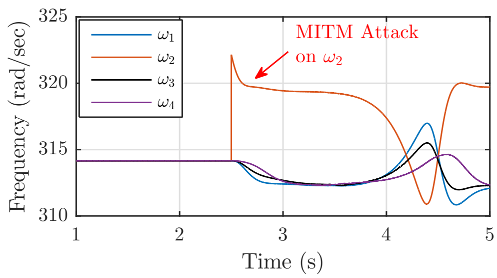


Fig. 12. Cyber attack on the communication channel of Unit II [49] – Synchrony among VSCs is disturbed leading to instability.

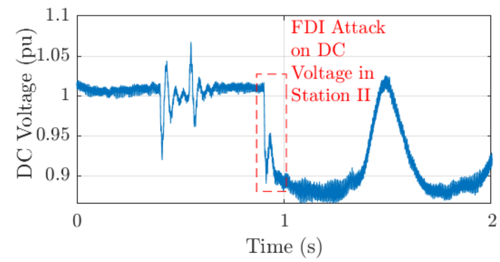
its operation under such attacks is unknown considering a particular agent since adequate information on the total active power demand is not centrally available. Moreover, it can be seen in Fig. 11(c) that the steady state value of the incremental cost initially upon attacks is raised by 0.85 \$/W at t = 1 s as compared to the normal unattacked scenarios shown in Fig. 11(b) & (d). It clearly suggests that minimization of (13) is violated under attacks for the same loading condition. Hence, the abovementioned case study raises serious concerns on detecting and mitigation of such attacks in cooperative microgrid, since the local neighborhood error in (17) converges to zero. As a result from a techno-economic perspective, such attacks cause reduction in energy efficiency.

D. Distributed Active Power Sharing in Autonomous Microgrids

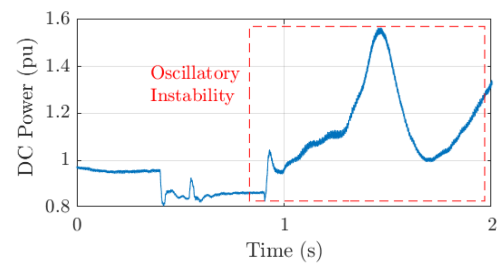
Using a setup of $N = 4$ grid-forming VSCs shown in Fig. 6, a man-in-the middle (MITM) attack is conducted on ω_2 by injecting an attack element of 8 rad/s into the outgoing communication links from unit II. Following the cooperative synchronization law in autonomous microgrids [49], frequency restoration and average voltage regulation are the two objectives, which govern stability. Using the active power primary control law for grid-forming VSCs [3], the active power among the DGs are shared equally for equal active power droop m_p. However, due to injection of false data into ω_2 of 8 rad/s at t = 2.5 s in Fig. 12, the synchrony is disturbed leading to instability. Hence, such attacks can lead to shutdown of small standalone powerhouses such as microgrids, and thereby affecting its operation.

E. Cyber Attack in VSC Based HVDC Stations

With increasing demand, the evolution of microgrids is surfacing to facilitate integration of renewable energy sources. However, power extraction from renewable energy sources depend on a lot of suitable socio-environmental factors, such as temperature, area of installation, wind, etc. Under implausible circumstances, transmission of power has been made possible using high voltage DC(HVDC) by means of two-level VSCs. More details on multi-polar and multi-level topologies of VSCs used for HVDC transmission can be found in [53]. As compared to the line commutated HVDC solution [54], VSC-HVDC provides many features such as independent control of active and reactive power with black start capability. The control philosophy of VSC-HVDC is quite commonly a set of grid-feeding VSCs with one station following $P-Q$ control whereas the other station with DC voltage regulation.



(a) DC Voltage (pu) in VSC-HVDC.



(b) Active Power (pu) via DC link in VSC-HVDC.

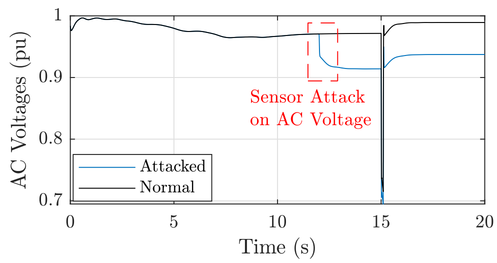
Fig. 13. Cyber attack on station II in VSC-HVDC [53]: (a) DC voltage, (b) Active power – FDIA to cause undervoltage causes oscillatory instability.

To demonstrate the impact of cyber attacks in 200 MVA, ± 100 kV VSC based HVDC, a FDI attack is injected into the DC voltage sensor in station II at t = 0.85 sec in Fig. 13. As soon as the attack is initiated, DC voltage drops to 0.9 pu, which creates oscillatory instability for the same droop value. Hence, such attacks raise critical concerns of stability. Moreover, it could lead to activation of protection devices installed in both HVDC stations.

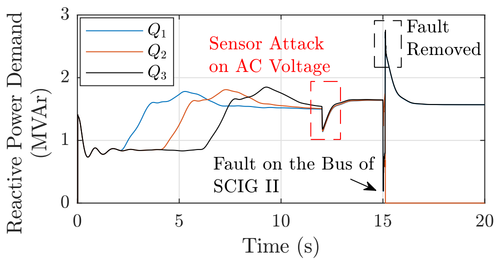
F. Impact of Cyber Attack on Wind Farms

1) Role of STATCOM: As potentially large installations of VSCs in grid-tied applications include wind farm, many robust and reliable control strategies have been designed to extract maximum output [55]. However, traditional wind farms with squirrel-cage induction generators (SCIG), where its stator is directly connected to the grid need large capacitor banks for reactive power to be absorbed by the IGs. If the reactive power requirement increases, it is withdrawn from the grid. Since the wind farms are usually connected to a 25 kV distribution network, excess withdrawal of reactive power deteriorates the voltage profile. To prevent this, static compensators (STATCOMs) are usually connected at the PCC to provide reactive power support to the wind farm [56].

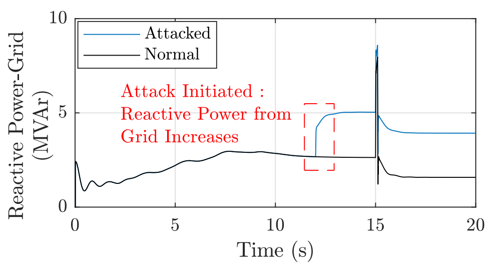
To exploit under-utilization of STATCOM, a false data injection attack is initiated in the AC voltage sensor at t = 12 sec as shown in Fig. 14. As AC voltage measurement reports a false bias as an undervoltage scenario, reactive power injection from the grid increases. As a result, the STATCOM with 3% droop setting starts absorbing the reactive power. Moreover with a L-G fault on the line at t = 15 sec, the peak reactive power demand from STATCOM under normal and attacked



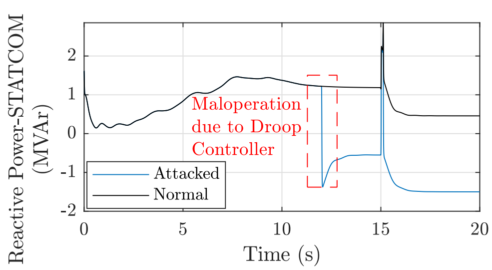
(a) AC Voltage at the PCC.



(b) Reactive Power Demand of each WT.

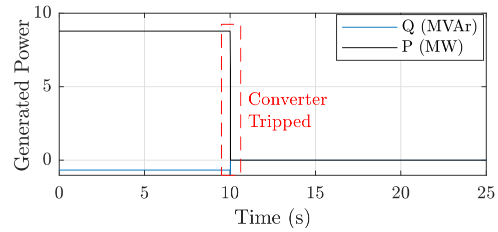


(c) Reactive Power from Grid.

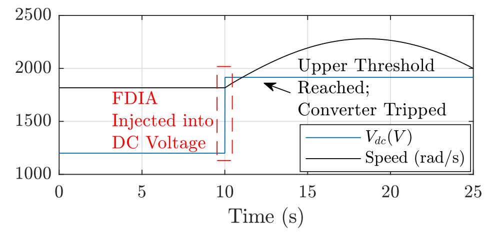


(d) Reactive Power from STATCOM.

Fig. 14. Performance of SCIG based wind farm under normal conditions and attack: Reactive power requirement from the grid increases unnecessarily due to FDIA on AC voltage [56].

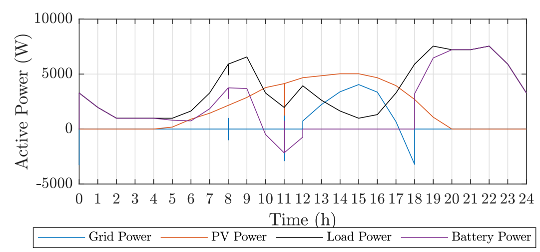


(a) Generated active and reactive power from DFIG.

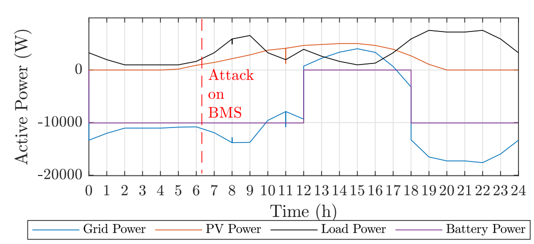


(b) DC voltage and speed.

Fig. 15. Impact of FDIA on DC voltage sensor in GSC of DFIG [58]: Overvoltage protection above 1600 V DC, resulting into tripping.



(a) Active power profile under normal conditions.



(b) Active power profile under MITM attack.

Fig. 16. Impact of MITM attack in centralized home management system [60]: Unnecessary scheduling from grid leading to increased consumer expenses.

conditions vary as a matter of grid code for fault ride through capability of every grid-connected unit [57].

2) Role of Grid Side Converter in Doubly-Fed IG (DFIG): With enhanced control flexibility, the DFIG technology allows extracting maximum energy from the wind for low speeds by optimizing the turbine speed while regulating the mechanical stress on the turbine. Moreover, the active power capacity is also increased by 40% as a virtue of the AC/DC/AC bridge using two back-to-back VSCs [58]. The function of the rotor side converter (RSC) is to extract maximum power from the IG based on the power-tip speed ratio graph [59]. Following this stage, the grid side converter (GSC) regulates the DC voltage to wheel the power from RSC into the grid.

Using the pre-defined set of vulnerable points in Table I, the DC voltage sensor is attacked with a large value of 400 V at t = 10 sec in Fig. 15. As DC voltage reaches 1600 V, it ultimately affects the control dynamics in the GSC, which leads to tripping owing to the overvoltage threshold. Hence, simpler attacks on the outer layer control loop can lead to shutdown or tripping of a large renewable generating unit, thereby challenging the reliability of operation.

G. Cyber Attack in Home Management System

With increased utility tariff rates, a battery empowered residential unit is a mandate requirement for grid-supporting units to enhance reliability under grid outage scenarios. Hence, proper power management using batteries is usually monitored and controlled by a centralized home energy management system (HEMS) [60]. The battery is basically connected as an auxiliary source, which is programmed to charge when there's surplus power from PV or discharge when there's excess load. This greatly reduces power utilization from the grid to deliver monetary benefits to the community. However, intrusion into the active generation profile of any source/load may disorient the control objective. This has been briefly shown in Fig. 16, where the load profile is manipulated using a MITM attack. With initialization of the attack, the battery stops responding to the surplus/deficient power locally. As a result, the grid power profile changes accordingly leading to non-optimal solution.

H. Voltage Regulation by DSTATCOM

To manifest practical scenarios of cyber attacks in power electronics based systems, a real-time simulation is carried out in OPAL-RT simulator OP5600 to demonstrate how cyber attacks on AC voltage measurement disorients the voltage regulation control action by a DSTATCOM (Distribution static compensator), as shown in Fig. 17 [61]. Fig. 18 shows the conceptual diagram of the real-time simulation process, where RT-LAB software is used as the interface between MATLAB and real-time OPAL-RT simulator. The MATLAB/SimPowerSystems model is loaded on to OPAL-RT through the RT-LAB and the real-time data is obtained conversely. To reduce the computational burden for each core, the model is split into three subsystems, i.e. a subsystem comprising of the physical layer (power unit), another subsystem comprising of control layer for the real-time simulation. Further a subsystem is employed, which includes console units to display real-time measurements. As shown in Fig. 18, the cyber attack is conducted on the control unit, which affects the system operation. In this way, an adversary can potentially penetrate into the host control unit to alter the actual controller by injecting false data and disregard the normal operation.

As shown in Fig. 17, a DSTATCOM is used to regulate voltage on a 11 kV distribution feeder connected to unbalanced and reactive power loads by either absorbing or generating reactive power. The DSTATCOM is programmed to provide reactive power support to regulate voltage when it increases/decreases by $\pm$ 6%. When simulated under real-time environment in Fig. 18, it can be seen that the DSTATCOM responds normally in Fig. 19(a) by absorbing and generating reactive power into the network with decrease and increase in voltage at t = 0.1 and 0.2 s, respectively. However, when an attack element of 0.1 p.u. is introduced into the control system at t = 0.2 s, it can be seen in Fig. 19(b) that the reactive power generated for both cases is considerably different. In fact, when the voltage is restored back to normal at t = 0.3 s, DSTATCOM continues to inject reactive power into the network, which will lead to overvoltage conditions. Further, this attack impedes over-utilization of resources, as shown in Fig. 19(c). To counter such attempts, the conventional state-estimation technique is exploited using (3)-(4) to extract the residual element; thereby indicating a significant change in the model parameters to confirm the presence of an attack. This has been clearly shown in Fig. 19(d) where the residual element goes out of bounds $\bar{r}$ to indicate the presence of an attack element in either of the vulnerable points (highlighted in Table I).

Usually in practical cases, such security mechanisms will be implemented on top of the existing controller to study the observability. As soon as the presence of attack is confirmed, the pre-attack measurement(s) will be held to operate using the last *unbiased* set-point [62]. This is the most simple countermeasure that can be applied to power-electronics systems; which can assure system recovery in milliseconds. It should be noted that the abovementioned mitigation criteria is limited to the magnitude of attack with varying performance. However to completely remove the attack element from control system, resilient control strategies need to be developed for power electronic systems such that it guarantees resilient and robust operation to tackle all security concerns in power electronics based systems [63], [64].

Finally, to accommodate the basics of impact due to all the discussed cyber attacks, the attack methodologies on different grid supportive services by VSC based systems are overviewed in Table II. As evident from the system impact and behavior in Table II, a generalized attack detection and mitigation strategy needs to be developed to provide a resilient networked control norm. Moreover, system observability needs to be accommodated to design a cyber attack resilient control mechanism to alleviate security in the modern electric grid.

V. Conclusions and Future Scope of Work

In this paper, the challenges and vulnerabilities associated with the control of modern grid-tied power converters due to cyber attacks have been analyzed from the system standpoint. At first, basic local control principles used for VSCs in different fields and applications have been revised. Then, an overview of potential attacks and their impact on interconnected converters has been provided. A detailed tutorial on the vulnerable points in the control and communication layer used for control of VSC is provided. Using these attack models as a proof of concept, many test cases considering VSCs in various fields such as DFIG, HVDC, STATCOM, DSTATCOM, microgrids, etc. are performed to demonstrate the consequences of cyber attacks. It has been demonstrated that cyber attacks with minimum sophistication can result into system shutdown, cause instability and potential damage to the consumer appliances. To address these concerns, attack resilient control strategies need to be devised to mitigate impact of cyber attacks on the electrical grid as a future scope of work. The design of resilient strategies requires appropriate understanding of the control and protection layer. From an ideal point of view, eliminating communication channel to promote localized control strategies would facilitate security of the power electronic converters. However, this idea propels as an overstatement from the performance perspective. Hence, it is important to restrict the cyber-physical interactions to a minimum synergy by targeting a manageable trade-off with system performance. Robust and resilient control strategies using watermarking [65] and model-verification techniques

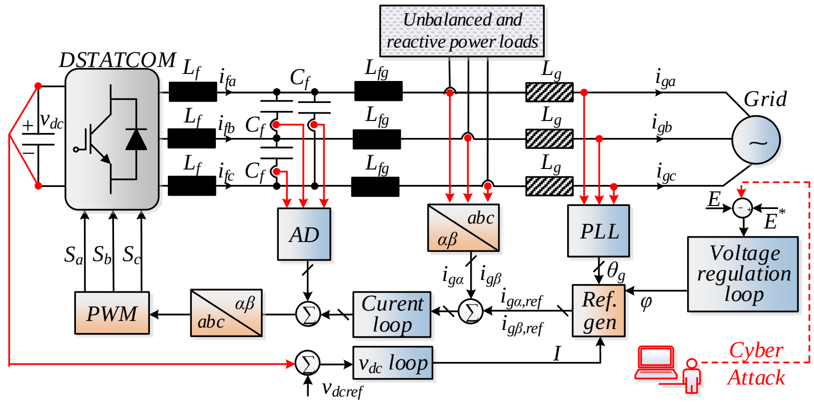


Fig. 17. Basic voltage regulatory control mechanism for DSTATCOM in the presence of unbalanced and reactive loads. Red dotted lines represent the attack element into the voltage control layer.

TABLE II
OVERVIEW OF CYBER ATTACKS ON GRID SUPPORTIVE SERVICES BY VSC BASED SYSTEMS

Grid-Supportive Services	**Attack Methodologies**	**System Impact**
Virtual inertial response by EV Charging Parks	Attack on frequency (FDIA, DoS, MITM) and DC voltage (FDIA)	Unnecessary tripping caused by RoCoF relays, causing unintentional islanding
Reactive power support by STATCOMs, PV based VSCs	Attack (FDIA, MITM) on voltage(s), Coordinated attack can cause *severe* impact	Manipulated voltages provide unneccesitated reactive power, thereby affecting the voltage profile which puts penalty on power distributors
Scheduling and dispatch	Attack on active power dispatch (FDIA) and data integrity attack (DIA) on cost parameters	Sub-optimal operation; may diverge to the active power generation bounds
Demand side management	Attack on load consumption pattern (FDIA, MITM, DoS)	Conditions where overloaded conditions are manipulated as normal loading level, leads to lifetime deterioration of transformers and lines; poor performance

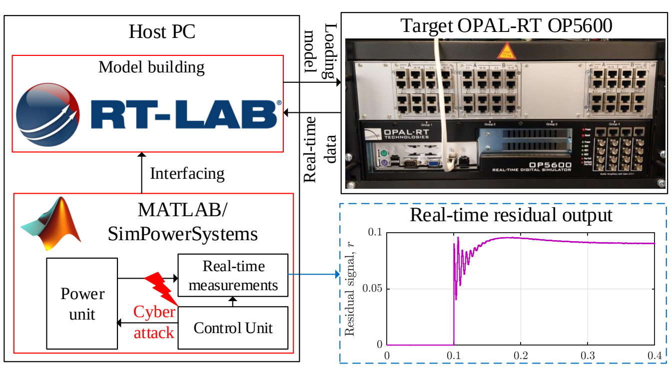


Fig. 18. Real-time setup to demonstrate practical feasibility and impact of cyber attacks to disregard voltage regulation by DSTATCOM.

[66] could be an asset to infiltrate such cyber attacks in real-time. Accommodating these view-points, the development of resilient technologies and preparing a line of defence against the cyber attacks is a new goal to enhance security and reliability of the dominant power electronic converters in the electric grid.

REFERENCES

[1] B. V. Mathiesen, H. Lund, and K. Karlsson, "100% renewable energy systems, climate mitigation and economic growth," *Applied Energy*, vol. 88, no. 2, pp. 488–501, 2011.

[2] F. Blaabjerg, R. Teodorescu, M. Liserre, and A. V. Timbus, "Overview of control and grid synchronization for distributed power generation systems," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1398–1409, 2006.

[3] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of Power Converters in AC Microgrids," *IEEE Trans. on Power Electron.*, vol. 27, no. 11, pp. 4734–4749, 2012.

[4] T. Dragicevic, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC Microgrids-Part II: A Review of Power Architectures, Applications, and Standardization Issues," *IEEE Trans. on Power Electron.*, vol. 31, no. 5, pp. 3528–3549, 2016.

[5] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, 2015.

[7] S. A. Baker, N. Filipiak, and K. Timlin, *In the dark: Crucial industries confront cyber attacks*. McAfee, Incorporated, 2011.

[8] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

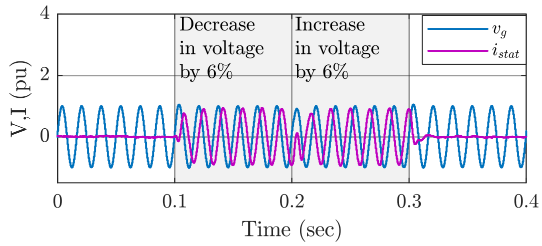
[9] J. M. Carrasco, L. G. Franquelo, J. T. Bialasiewicz, E. Galvan, R. C. PortilloGuisado, M. A. M. Prats, J. I. Leon, and N. Moreno-Alfonso, "Power-electronic systems for the grid integration of renewable energy sources: A survey," *IEEE Trans. on Ind. Electron.*, vol. 53, no. 4, pp. 1002–1016, 2006.

[10] C. A. Hill, M. C. Such, D. Chen, J. Gonzalez, and W. M. Grady, "Battery energy storage for enabling integration of distributed solar power generation," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 850–857, 2012.

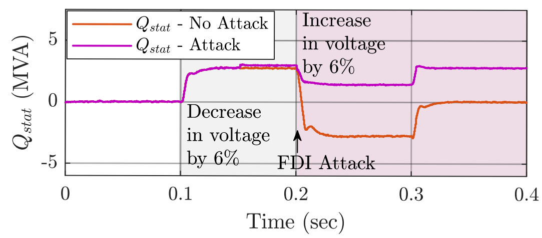
[11] M. Yilmaz and P. T. Krein, "Review of battery charger topologies, charging power levels, and infrastructure for plug-in electric and hybrid vehicles," *IEEE Trans. on Power Electron.*, vol. 28, pp. 2151–2169, May 2013.

[12] T. Dragicevic, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC Microgrids-Part I: A Review of Control Strategies and Stabilization Techniques," *IEEE Trans. on Power Electron.*, vol. 31, pp. 4876–4891, July 2016.

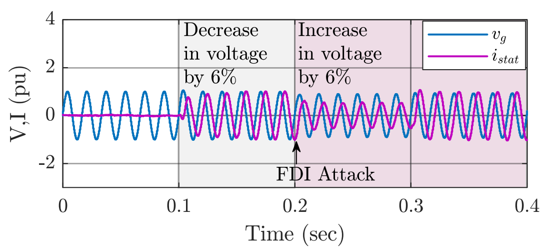
[13] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces,"



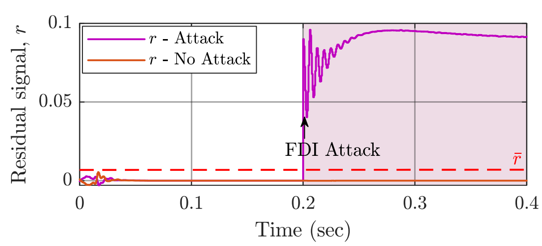
(a) PCC voltage and current by DSTATCOM in the absence of attack.



(b) Reactive power from DSTATCOM in the presence and absence of attack.



(c) PCC voltage and current by DSTATCOM in the presence of attack.



(d) Residual signal to indicate possibility of cyber attack and normal disturbances (calculated using (4)).

Fig. 19. Performance of DSTATCOM under normal conditions and attack: Reactive power provided by the DSTATCOM increases unnecessarily due to FDIA on AC voltage leading to over-utilization of resources [61].

IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003), pp. 1–138, April 2018.

[14] S. Sahoo and S. Mishra, “A distributed finite-time secondary average voltage regulation and current sharing controller for dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 282–292, 2019.

[15] S. A. Boyer, *SCADA: Supervisory control and data acquisition*. International Society of Automation, 2009.

[16] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragicevic, “A stealth cyber attack detection strategy for dc microgrids,” *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, 2018.

[17] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, “On detection of false data in cooperative dc microgrids–a discordant element approach,” *IEEE Trans. Ind. Electron.*, 2019.

[18] W. Wu, Y. Liu, Y. He, H. S. H. Chung, M. Liserre, and F. Blaabjerg, “Damping methods for resonances caused by lcl-filter-based current-controlled grid-tied power inverters: An overview,” *IEEE Trans. Ind. Electron.*, vol. 64, pp. 7402–7413, Sept 2017.

[19] L. Harnefors, X. Wang, A. G. Yepes, and F. Blaabjerg, “Passivity-based stability assessment of grid-connected vscs: An overview,” *IEEE J. of Em. and Sel. Topics in Power Electron.*, vol. 4, pp. 116–125, March 2016.

[20] D. M. Vilathgamuwa, P. C. Loh, and Y. Li, “Protection of microgrids during utility voltage sags,” Oct 2006.

[21] K. D. Brabandere, B. Bolsens, J. V. den Keybus, A. Woyte, J. Driesen, and R. Belmans, “A Voltage and Frequency Droop Control Method for Parallel Inverters,” *IEEE Trans. on Power Electron.*, vol. 22, pp. 1107–1115, July 2007.

[22] R. Teodorescu, M. Liserre, and P. Rodriguez, *Grid Converters for Photovoltaic and Wind Power Syst.* Wiley, 2011.

[23] F. Bosio, L. A. de Souza Ribeiro, F. D. Freijedo, M. Pastorelli, and J. M. Guerrero, “Effect of State Feedback Coupling and System Delays on the Transient Performance of Stand-Alone VSI With LC Output Filter,” *IEEE Trans. on Ind. Electron.*, vol. 63, pp. 4909–4918, Aug 2016.

[24] Q. Shafiee, C. Stefanovic, T. Dragicevic, P. Popovski, J. C. Vasquez, and J. M. Guerrero, “Robust networked control scheme for distributed secondary control of islanded microgrids,” *IEEE Trans. on Ind. Electron.*, vol. 61, pp. 5363–5374, Oct 2014.

[25] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[26] F. Callegati, W. Cerroni, and M. Ramilli, “Man-in-the-middle attack to the https protocol,” *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78–81, 2009.

[27] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[28] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[29] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: A tutorial,” *IEEE Wireless Comm.*, vol. 18, no. 2, pp. 66–74, 2011.

[30] A. Ovalle, G. Ramos, S. Bacha, A. Hably, and A. Rumeau, “Decentralized control of voltage source converters in microgrids based on the application of instantaneous power theory,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1152–1162, 2014.

[31] A. Stefanov and C.-C. Liu, “Cyber-power system security in a smart grid environment,” in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–3, IEEE, 2012.

[32] I. Serban and C. Marinescu, “Control strategy of three-phase battery energy storage systems for frequency support in microgrids and with uninterrupted supply of local loads,” *IEEE Trans. Power Electron.*, vol. 29, pp. 5010–5020, Sept 2014.

[33] T. Dragicevic, “Model predictive control of power converters for robust and fast operation of ac microgrids,” *IEEE Trans. Power Electron.*, vol. 33, pp. 6304–6317, July 2018.

[34] Q. C. Zhong and G. Weiss, “Synchronverters: Inverters that mimic synchronous generators,” *IEEE Trans. on Ind. Electron.*, vol. 58, pp. 1259–1267, April 2011.

[35] S. D’Arco, J. A. Suul, and O. B. Fosso, “A virtual synchronous machine implementation for distributed control of power converters in smartgrids,” *Electric Power Systems Research*, vol. 122, pp. 180 – 197, 2015.

[36] P. Rodríguez, C. Citro, J. I. Candela, J. Rocabert, and A. Luna, “Flexible grid connection and islanding of spc-based pv power converters,” *IEEE Trans. on Ind. Appl.*, vol. 54, pp. 2690–2702, May 2018.

[37] J. Liu, Y. Miura, and T. Ise, “Comparison of dynamic characteristics between virtual synchronous generator and droop control in inverter-based distributed generators,” *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3600–3611, 2015.

[38] B. Palmintier, R. Broderick, B. Mather, M. Coddington, K. Baker, F. Ding, M. Reno, M. Lave, and A. Bharatkumar, “On the path to sunshot. emerging issues and challenges in integrating solar with the distribution system,” tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States), 2016.

[39] M. Ahmed, R. Bhattarai, S. J. Hossain, S. Abdelrazek, and S. Kamalasadan, “Coordinated voltage control strategy for voltage regulators and voltage source converters integrated distribution system,” *IEEE Trans. on Ind. Appl.*, pp. 1–1, 2019.

[40] R. Yan and T. K. Saha, “Investigation of voltage stability for residential customers due to high photovoltaic penetrations,” *IEEE transactions on power systems*, vol. 27, no. 2, pp. 651–662, 2012.

[41] J. Yaghoobi, N. Mithulananthan, and T. K. Saha, “Dynamic voltage stability of distribution system with a high penetration of rooftop pv

units," in *2015 IEEE Power & Energy Society General Meeting*, pp. 1–5, IEEE, 2015.

[42] S. Maharjan, A. M. Khambadkone, and J.-X. Xu, "Probing the impact of reduced dc capacitor size in variable speed drive loads on voltage stability of the distribution network at high pv penetration," in *2018 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*, pp. 220–225, IEEE, 2018.

[43] S. Maharjan, A. M. Khambadkone, and J. C.-H. Peng, "Integration of centralized and local voltage control scheme in distribution network to reduce the operation of mechanically switched devices," *arXiv Preprint*, 2019.

[44] "Sustainable electrical energy centre. united kingdom generic distribution system (ukgds)," *Previously Available: http://www.sedg.ac.uk*, 2010.

[45] V. V. G. Krishnan, S. Gopal, R. Liu, A. Askerman, A. Srivastava, D. Bakken, and P. Panciatici, "Resilient cyber infrastructure for the minimum wind curtailment remedial control scheme," *IEEE Trans. Ind. Appl.*, vol. 55, pp. 943–953, Jan 2019.

[46] P. Srikantha and D. Kundur, "Hierarchical signal processing for tractable power flow management in electric grid networks," *IEEE Trans. Signal and Inf. Proc. over Net.*, vol. 5, pp. 86–99, March 2019.

[47] R. Palma-Behnke, C. Benavides, F. Lanas, B. Severino, L. Reyes, J. Llanos, and D. Sáez, "A microgrid energy management system based on the rolling horizon strategy," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 996–1006, 2013.

[48] P. Siano, C. Cecati, H. Yu, and J. Kolbusz, "Real time operation of smart grids via fcn networks and optimal power flow," *IEEE Trans. Ind. Inform.*, vol. 8, no. 4, pp. 944–952, 2012.

[49] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids—a novel approach," *IEEE Transactions on power electronics*, vol. 29, no. 2, pp. 1018–1031, 2014.

[50] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, 2017.

[51] N. Rahbari-Asr, U. Ojha, Z. Zhang, and M.-Y. Chow, "Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2836–2845, 2014.

[52] S. Lusk, D. Lawrence, and P. Suvana, *Cyber-intrusion Auto-response and Policy Management System (CAPMS)*. ViaSat Inc., Boston, MA (United States), 2015.

[53] O. Gomis-Bellmunt, J. Liang, J. Ekanayake, R. King, and N. Jenkins, "Topologies of multiterminal hvdc-vsc transmission for large offshore wind farms," *Electric Power Systems Research*, vol. 81, no. 2, pp. 271–281, 2011.

[54] C. Thio, J. Davies, and K. Kent, "Commutation failures in hvdc transmission systems," *IEEE Transactions on Power Delivery*, vol. 11, no. 2, pp. 946–957, 1996.

[55] Z. Saad-Saoud, M. Lisboa, J. Ekanayake, N. Jenkins, and G. Strbac, "Application of statcoms to wind farms," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 145, no. 5, pp. 511–516, 1998.

[56] S. Ahsan and A. Siddiqui, "Dynamic compensation of real and reactive power in wind farms using statcom," *Perspectives in Science*, vol. 8, pp. 519–521, 2016.

[57] M. Molinas, J. A. Suul, and T. Undeland, "Low voltage ride through of wind farms with cage generators: Statcom versus svc," *IEEE Trans. Power Electron.*, vol. 23, no. 3, pp. 1104–1117, 2008.

[58] L. Xu and P. Cartwright, "Direct active and reactive power control of dfig for wind energy generation," *IEEE Trans. Energy Conv.*, vol. 21, no. 3, pp. 750–758, 2006.

[59] F. Blaabjerg and Z. Chen, "Power electronics for modern wind turbines," *Synthesis Lectures on Power Electronics*, vol. 1, no. 1, pp. 1–68, 2005.

[60] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "An algorithm for intelligent home energy management and demand response analysis," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 2166–2173, 2012.

[61] B. Singh and J. Solanki, "A comparison of control algorithms for dstatcom," *IEEE Trans. Ind. Electron.*, vol. 56, no. 7, pp. 2738–2745, 2009.

[62] S. Sahoo and S. Mishra, "An adaptive event-triggered communication-based distributed secondary control for dc microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, 2017.

[63] A. M. Farid, "Multi-agent system design principles for resilient coordination & control of future power systems," *Intelligent Industrial Systems*, vol. 1, no. 3, pp. 255–269, 2015.

[64] C. G. Rieger, K. L. Moore, and T. L. Baldwin, "Resilient control systems: A multi-agent dynamic systems perspective," in *IEEE Intl. Conf. Electro-Information Technology, EIT 2013*, pp. 1–16, IEEE, 2013.

[65] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking," in *53rd IEEE Conference on Decision and Control*, pp. 3757–3764, IEEE, 2014.

[66] B. Bérard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, and P. Schnoebelen, *Systems and software verification: model-checking techniques and tools*. Springer Science & Business Media, 2013.

Subham Sahoo (S'16-M'18) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSS University of Technology, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018 respectively. He has worked as a visiting student with the Department of Electrical and Electronics Engineering in Cardiff University, UK in 2017 and as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore in 2018-2019. He is currently working as a research fellow in the Department of Energy Technology, Aalborg University, Denmark.

He is a recipient of the Innovative Students Projects Award for Doctoral level by Indian National Academy of Engineering (INAE) for the year 2019. His current research interests include control and stability of microgrids, cyber security in power electronics based cyber-physical systems.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral research associate at Aalborg University, Denmark. From March 2016, he is an Associate Professor at Aalborg University, Denmark where he leads an Advanced Control Lab.

He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His principal field of interest is design and control of microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and co-authored more than 170 technical papers (more than 70 of them are published in international journals, mostly IEEE Transactions) in his domain of interest, 8 book chapters and a book in the field.

He serves as Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Dr. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, and a Robert Mayer Energy Conservation award.

Frede Blaabjerg (S'86–M'88–SM'97–F'03) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got the PhD degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania and Tallinn Technical University (TTU) in Estonia.

His current research interests include power electronics and its applications such as in wind turbines, PV systems, reliability, harmonics and adjustable speed drives. He has published more than 600 journal papers in the fields of power electronics and its applications. He is the co-author of four monographs and editor of ten books in power electronics and its applications.

He has received 32 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award 2014 and the Global Energy Prize in 2019. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been Distinguished Lecturer for the IEEE Power Electronics Society from 2005 to 2007 and for the IEEE Industry Applications Society from 2010 to 2011 as well as 2017 to 2018. In 2019-2020 he serves a President of IEEE Power Electronics Society. He is Vice-President of the Danish Academy of Technical Sciences too. He is nominated in 2014-2018 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.