UC Irvine

UC Irvine Previously Published Works

Title

Secure Power Distribution Against Reactive Power Control Malfunction in DER Units

Permalink

<https://escholarship.org/uc/item/70j0p3bb>

Author

Joseph, Anto

Publication Date

2020-07-23

Peer reviewed

Secure Power Distribution Against Reactive Power Control Malfunction in DER Units

Anto Joseph, Keyue Smedley, *Fellow, IEEE*, and Shahab Mehraeen, *Senior Member, IEEE*

Abstract--Penetration of distributed energy resources (DERs) such as wind, solar and battery units are rapidly increasing in distribution power system (DPS). In view of power grid reliability and efficiency, cyber and physical secure of these units are highly important since it can directly impact power system operations. This paper investigates the dynamic behavior of power distribution during cyber, physical and natural strikes on reactive power control in DER units. Various fault scenarios including modifications in voltage-reactive power (Volt-Var) curve pattern such as slope of the curve, dead band; and changes in capacitive or/and inductive reactive power delivery to the power grid are presented. Further, fault scenarios are investigated with the presence of dynamic VAR (volt-ampere reactive) compensation (DVC) units in the system. A southern California 140-bus commercial distribution power system is selected as a test system and faults are analyzed in both Matlab/Simulink and ETAP simulation platforms. The results evidence that the modifications in reactive power control values at DER units significantly affects the voltage quality/security of the system and affect the number of switching actions of voltage regulators (VRs). In contrast, DPS connected with DVCs improves voltage quality and reduces the number of switching actions of VRs, also voltage quality/security is maintained during the faults.

Index Terms-- Cybersecurity, distributed energy resources, reactive power control, voltage stability, dynamic var compensation units.

I. INTRODUCTION

THE deployment of DER unit is significantly increased in the power utilities, primarily due to: (i) incentives that supporting renewable power generation, (ii) customer participations, and (iii) reduced energy cost of DER units; and the trend is continuing through advanced energy and control technologies [1], [2]. Currently, distribution power system is shifting towards modernization for the better grid operation, subsequently, DER units and voltage regulators are remotely controlled through RF (radio-frequency) communication, 4th generation (4G) mobile network, WAN/LAN (wide/local area network), etc. [3]. It is noted that IEC 61850 standard is commonly applied in the DPS communication [4]. This

intelligent communication provides many benefits to the DPS including efficient transmission, quick restoration of power, lower electricity rates, and customer participation, etc. [5], [6]. However, it is a big challenge for power grid operators considering issues in cybersecurity [7], [8].

In Dec 2015, unprecedented cyber-attacks on the distribution substations in Ukraine affected the 1.4 million peoples without electricity for 6 h. Cyber-attack on transmission substation in the same country was also reported on Dec 2016 [9]. In addition, United States Homeland Security Department reported that hackers breached twelve US power plants including Kansas Wolf Creek nuclear facility, reported in July 2017 [10]. The incidents are evidences that cyber-attack in the power grid control could cause a huge blackout. Therefore, countries are taking effective preventive actions in the DER rich power systems and continually regulating the standards in DER units in view of integration, power quality, fault ride through, protection, control and cybersecurity, etc. [11].

In most of the countries including United States, IEEE 1547 standard is applied for regulating the DER units interconnected with DPS, and this standard are continually updated in consideration of several factors such as reactive power assistance to the power grid, voltage and frequency regulations. As per IEEE 1547-2003, DER units shall not allow to regulate the grid voltage; then it is modified to that DER units may help to regulate the grid voltage through reactive power support or active power modulation via IEEE 1547a-2014. DER units must support grid voltage through reactive power control and may modulate the active power by IEEE 1547-2018. This reactive power control value can be either controlled by digital communication from consumers, distribution system operators (DSO), aggregators (third parties), or by the autonomous control capabilities of smart inverter system [12] - [14]. Therefore, the possibility of cyber and physical attacks against the active and/or reactive power controls are expected in DER units due to the new IEEE regulation. In addition, current sensor faults (i.e. omission, gain, saturation and bias) in smart inverters lead to vary the reactive power delivery of the DER units. It is reported that about 65% of faults in smart inverter units are due to the sensors and controllers in the electrical system [15].

While transmission system operators mainly utilize the DER reactive power control for optimal power flow and enhance voltage stability in the power system, the reactive power control is rarely employed to mitigate voltage

This work is supported by the University of California, Office of the President under Grant No. LFR-18-548175.

A. Joseph and K. Smedley are with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA. (ajosephr@uci.edu, smedley@uci.edu)

S. Mehraeen is with the Electrical and Computer Engineering Department, Louisiana State University, Baton Rouge, LA, USA. (e-mail: smehraeen@lsu.edu).

Fig. 1. Power flow and control diagram of DER units

fluctuations due to variations in active power generation neither it interferes with the operation of other mechanisms. By contrast, distribution system operators (DSO) use the DER reactive power control for mitigating voltage fluctuations due to the variations in DER active power generation. Distribution DERs may also provide reactive power support to the transmission system for improved voltage stability. However, reactive power support from these sources cause challenges to the conventional voltage regulating devices (OLTC, SVR, SCBs) operation due to uncertainties in DER generation. Several types of reactive power control functions are possible based on DERs, wherein volt-var control is preferred by the distribution system operators in view of reduced interference with the OLTC, SVR, and SCB operations. Nevertheless, modifications (i.e. cyber-attack) in volt-var curve pattern significantly affects the voltage stability (i.e. dynamic voltage oscillations) and voltage security of the grid.

Recently, more researches have been reported regarding the cybersecurity issues on distribution power system. BJ. Kang et al discussed the possible cyber-attacks against the manufacturing message specification (MMS) of standard IEC 61850 in the smart inverter unit. It has detailed the physical impact on PV inverter during cyber-attack on active power control value [4]. Ref [16] comprehensively reviewed the fault data injection attacks (FDIA) against on supervisory control and data acquisition system. In addition, economical and physical impacts of FDIA were discussed. Impacts on smart grid during cyber-attack on voltage regulating devices including static synchronous compensator (STATCOM) and static VAR compensator (SVC) are detailed in [17]. Cybersecurity challenges, attack scenarios, resilience analysis and attack prevention techniques on DERs are summarized in [18]. The possible data integrity attack on voltage control loop in power grid voltage compensation devices (static) is discussed in [19]. Further, reliability estimation of distribution power network considering various cyber-attacks on intelligent electronic devices and distribution main station is considered in [20]. A study in [21] discussed the cyber-attack on voltage measurement devices in the DPS, also it presented the detection algorithm to minimize the effects. Teymouri et al has listed the various cyber-attacks on reactive power capability of photo-voltaic systems. However, it does not detail the impacts of distribution system considering VRs

switching operations, voltage transients, and grid stability, etc. [22].

In the authors' prior work, static and dynamic control strategies were proposed in [23]. The static control strategy employs time delays and hysteresis capacitive-inductive control characteristics. The dynamic control strategy employs a novel approach to estimate the grid voltage and inject reactive power to mitigate voltage fluctuation and imbalance unlike the IEEE 1547-2018. This control strategy can mitigate the voltage fluctuations due to the variations in DER active power generations (either it can be through solar variation or cyber-attack on the active power control) or sudden load variations (either it can be through natural load disconnection or cyber-attack on the smart meters). The control strategy is also useful when a smaller number of DERs connected in the distribution system are cyber-attacked affecting reactive power control. However, if all the DERs or significant number of the DERs connected in the DPS are cyberattacked, this significantly affects voltage stability and voltage security of the grid that requires an enhanced control mechanism beyond the authors' prior work. Therefore, this paper incorporates the dynamic var compensator (DVC) in the DPS which improve the voltage stability and voltage security of the grid. In addition, it proposes coordinated reactive power control strategy between DER and DVC units which reduce the reactive power support interference between DER and DVC units and improve the voltage stability and security of the grid during normal and unexpected situations.

A. Problem Description and Importance of Work

The integration of increased penetration of DERs into the DPS challenges the distribution system operators in view of power quality, and cybersecurity issues. Currently, the later one attracts a great attention since the fourth industrial revolution shifting conventional DPS into the intelligent DPS with the inclusion of remote monitoring, digital communication and control. Hence, active and reactive power of DER units could be remotely controlled by the consumers, DSOs and third parties. Also, these remote communications can be hacked or controlled by the unknown operators (i.e. cyber-attacks), then bring the potential threat to the DPS in view of power loss, grid stability and reliability.

In addition, it is noted that DER units typically do not support security features including encryption in all the controls due to the limited processing capabilities and high cost equipment [2]. Furthermore, to allow excessive amounts of renewable penetration in the DPS (based on future projections), utilities must employ the remotely controlled functions in DER units in consideration of uncertainties in renewable generation and load variation. It allows large number of access points where these DER sources can be operated outside the utility supervision domain. Therefore, power and cyber experts are working together and selectively encrypt the certain controllers in order to minimize the processing overhead and application latency.

The variations in DER reactive power support to the power grid is significantly affecting the voltage stability than active

Table 1. Time delays corresponding to DER and VR units [23]

DER Unit Time delays			SCB Time delays			SVR/OLTC Time delays		DER – VRs Coordination Time delays	
*Synchronous generator dynamics (τ_s)	**Transient current decay (τ_i)	***Remote communication time delay (τ_c)	Intentional time delay (τ_i)	Operational time delay	Mandatory discharging time	Intentional time delay (τ_i)	Operational time delay	****Grid measurements time constant(τ_m)	Immediate VRs switching
~1 s	~1 s – 5 s	~2-5 s	1 s – 60 s	0 s – 10 s	60 s – 360 s	1 s – 360 s	4 s – 10 s	~2 s – 5 s	$\tau_s + \tau_i + \tau_c + \tau_m$
* depends on conventional synchronous machine excitor time constant				** depends on resistance to reactance ratio of a power distribution system.					
*** depends on remote data processing from communication				**** depends on impedance value between DER and VR units					

power variations. It can be either capacitive or inductive reactive power. In addition, rapid changes in reactive power in DER unit could results in active power curtailment in accordance with the power rating of DERs. It motivates the present research with the intention to investigate the DPS in view of: (i) how the modifications in DER-reactive power support does affecting the distribution system, (ii) how to maintain the stability of the DPS during the changes in reactive power support from DER units.

IEEE standards allow for variations of the dead band and slope of volt-var characteristics; however, the modifications can be conducted in various directions and an appropriate setting is not trivial. Several research groups are currently working on these settings to find optimal settings; however, no standard has been established yet. This work is an effort to investigate appropriate modifications in the conventional characteristics. The contributions of this paper include: (i) it analyses the commercial distribution power system subjected to modification in volt-var curve (slope & dead band), supplying inductive reactive power to the grid than capacitive reactive power and swapping the capacitive and inductive reactive power supply to the grid. The findings are verified through the switching operations of SVR, & OLTC units, voltage oscillations and voltage security of the grid under the influence of intermittent active power (ii) this paper proposed the coordinated reactive power control strategy between DER and DVC units which reduce the reactive power support interference between DER and DVC units and improve the voltage stability and security of the grid during normal and unexpected situations and (iii) compare the fault scenarios with the inclusion of DVC units in the DPS and conventional system (i.e. without incorporation of DVC units. The fault analysis and results from this article shall be beneficial for the policy makers and grid operators for the reliable and safe operation of DPS.

B. Organization of Paper

The organization of this paper is following: Section II discusses the various conventional voltage regulating devices and their competence in the distribution power system. In addition, cooperation control between DER and DVC unit is proposed based on practical constrains. The cyber-physical attacks and malfunction on reactive power control on DERs are summarized in section III. To understand the study, a Southern California commercial 140-bus distribution system is simulated (single day with varying solar power generation and load profile) in time domain simulations and results are discussed in section IV. The performance of the DVCs under the cyber-physical fault scenarios are investigated and

outcomes are presented in section V and finally concluding statements are briefed in section VI.

II. VOLTAGE REGULATORS IN DISTRIBUTION POWER SYSTEM

Conventionally, OLTC, SCB and SVR units are employed to regulate the voltage in the DPS. The OLTCs and SVRs are used to maintaining power grid voltage in the safety region through adjusting tap changing operations, whereas SCB unit supply capacitive reactive power to the power grid for the voltage regulation. The conventional control and operation of these devices are detailed in [23]. Nowadays, the development of innovative control functions in the smart inverter results to provide reactive power to the power grid from DER units, it is regulated through IEEE 1547:2018. As per IEEE rule, the static reactive power support is based on active power generation of such DER unit and it is given below.

$$\left\{ \begin{array}{l} Q_{g(max)} = 0, P_g = 0 \\ Q_{g(max)} = 44\% \text{ Nameplate kVA} \times \left(\frac{\text{Active power generation}}{20\% \times \text{rated active power}} \right), 20\% \geq P_g > 0 \\ Q_{g(max)} = 44\% \text{ Nameplate kVA}, 100\% \geq P_g > 20\% \end{array} \right\} \quad (1)$$

The static reactive power support can be utilized in the operational voltage region (regulated by IEEE) between 0.88 p.u. and 1.10 p.u. of the grid voltage. Also, the greatest possible reactive power support (i.e. up to 100%) can be applied only during the abnormal voltage range (i.e. $V_{bus} < 0.88$ p.u. (or) $V_{bus} > 1.10$ p.u.). Nevertheless, voltage supplied at the DPS must be within the range from 0.95 p.u. and 1.05 p.u. in view of voltage security, as specified by ANSI C84.1 [24]. Moreover, the static reactive power support to the power grid must be between 1s and 90s, as defined by IEEE in consideration of system stability and switch gear (protection) devices connected in the DPS. The selection of time delay during the static reactive power support is explained in [23]. The various time delays employed in SCB, OLTC and DER units corresponding to the grid voltage support are summarized in Table.1. Presently, voltage support from DER unit is at the forefront of traditional devices like OLTC, and SCB units in the DPS. For example, voltage support from DERs takes place about 3 s from the power quality disturbance whereas voltage support from OLTC and SCB units require minimum 30 s for the operation. Therefore, if anyone of the traditional devices malfunction (i.e. natural fault (or) cyber-attack) then it could lead to operate the DER reactive power support. Moreover, if the grid voltage is more than 1.10 p.u. then it could curtail the active power generation in DER units and lead to more uncertainties in the distribution power system.

A. Dynamic VAr Compensator

Dynamic VAr compensator is a voltage source inverter connected to the grid. It dynamically supports both capacitive and inductive reactive power to the power grid. The One-Cycle Control (OCC) or grid voltage-oriented vector control system can be employed in DVC units for the dynamic grid voltage support. The first reported DVC demonstration in an SDGE commercial power distribution circuit has shown an OCC-DVC regulating grid voltage to a flat line against solar intermittency [25, 26]. Further, control system employed in DVC unit is autonomous and it is not concern with the cybersecurity issues. Usually, DVC delivers reactive power to the power grid based on the grid voltage, i.e. it follows the voltage-reactive power mode. However, the curve (volt-var) does not follows the IEEE regulated curve and it is calculated based on the relationship between the change in reactive power and change in voltage of a certain distribution system. This Q-V relationship can be varied from system one another and it is addressed via non-linear Q-V curve of the distribution system, and it is detailed in [27].

B. Coordinated Control of DVC & DER units.

The traditional voltage regulated devices such as SCB, SVR, and OLTC units are not feasible to provide dynamic grid voltage support due to their practical limitations and only used for static grid voltage/reactive power support. However, DER and DVC units can support both dynamic and static reactive power to the power grid due to its operational qualities.

The coordination between DER and DVC units is important during the static and dynamic reactive power support to the power grid, and it shall be structured based on: (i) maximizing the utilization of static reactive power support from DER units, (ii) reduces the active power curtailment from DER units, (iii) maintaining the voltage quality/security in the grid during faults/disturbances. The transient current decay time constant (τ_t) and synchronous generator excitor time constant (τ_s) are determining the time delay for providing static reactive

power support from DER units. Generally, the former one is selected between 1 s and 5 s in consideration of grid voltage stability and the latter one is selected as about 1 s for the suitable operation of grid protection and switchgear devices. And for this reason, DER units are assigned to take minimum 3 s to support static reactive power to the power grid during autonomous control. Furthermore, data processing time constant (τ_c) is considered for the remote-control unit in view of remote communication and data processing, reasonably it is about 2 s. Fig. 2 shows the decentralized coordination strategy between DER and DVC units based on grid voltage and time constants. It shows that the static reactive power support from DVC and DER units can be coordinately controlled through time delay constants. The time constants including synchronous generator exciter time constant, and transient current decay time constant are similar for both units. But a time constant is additionally included in the DVC units which can delay the static reactive power support by the DVC units. Subsequently, DER units are preferred for the static reactive power support because of voltage security. The selection of this time constant is the DSO decision where the static voltage support from DVC unit can be before or after the traditional voltage supporting devices. In this paper grid measurement time constant is selected such that DVC supports static reactive power to the grid before the traditional devices and reduces the number of switching operations of the OLTC and SVR units. In case of dynamic reactive power support, DVC units are primarily activated (e.g. DVC unit supports dynamic reactive power when grid voltage falls to 0.92 p.u., whereas DER unit support at grid voltage lower than 0.88 p.u.) and improves the voltage quality of the DPS, additionally, it reduces the active power curtailment in DER units. The grid voltage values at DVC units during dynamic reactive power support is selected by considering emergency demand response regulated by ANSI C84.1. [24]. Per IEEE 1547:2018, DERs can be disconnected (considering low voltage ride

Fig. 2. Coordination of reactive power support from DER and DVC units

Fig. 3. Modification of voltage-reactive power curve in DER units

through) from the power grid when the bus voltage is lower than 0.88 p.u. Therefore, in order to prevent the DERs from disconnection, voltage lower bound is chosen as 0.88 p. u. The rating of DVC units is estimated based on the Q-V relationship of a distribution system and it can support at least 10% (0.1 p. u) voltage regulation.

III. CYBER VULNERABILITIES IN DER UNIT

The mostly used communication protocols for data exchange in the distribution system are Distributed Network Protocol (DNP3) and IEC 61850-Manufacturing Message Specification. In which, DNP3 experiencing issues in lack of protocol security including authentication and validation mechanisms. The latter one operates over standard TCP/IP and has no encryption. Hence, both communication protocols could be vulnerable to the man-in-the-middle attack. In addition, DER is becoming consumer owned and the owners may not be fully aware of cyber security problems and threads.

The impact analyses for the DER unit during the various cybersecurity scenarios are listed in [12]. It has evidenced that the access control in DER units could provide higher impact to the DPS. It is noted that through access control threat agent can modify the control value of active and reactive powers of the DER units. It is assumed that the SCADA or master computer or IP address of the DER unit control is hacked by the threat agent then the threat agent may modify the reactive power control. The possible attacks are listed below:

A. Modifying the Voltage-Reactive Power Curve Pattern

The reactive power support to the power grid by DER units stick with the generalized volt-var curve as regulated through IEEE 1547-2018 in view of grid stability, and power losses. In

this scenario, thread agent can modify the volt-var curve pattern by accessing the master computer in the utility or distribution management control system. The curve can be modified either by change-in slope or changes in voltage dead band as shown in Fig. 3. As a result: (i) it could generate grid oscillatory actions by hasty and large changes in reactive power to the grid, led to harm the DPS (ii) increases the number of switching actions of voltage regulators in the system, (iii) raise the percentage of period that bus voltages outside the stipulated voltage bandwidth.

B. Malfunction in Sensor Units of Inverter Control System

This kind of scenario can be happened during the cyber-physical attack on the sensors (i.e. hall effect voltage and current sensors can be controlled through violent electromagnetic signal) (or) sensor failure due to natural behaviors (i.e. breakage due to thermal stress). It can increase the inductive reactive power delivery to the grid based on the nature of the fault (i.e. omission, gain, saturation and bias). This type of failure could: (i) forces the system as weak grid, (ii) massively increase the number of switching operations of voltage regulators in the system, sometimes VRs goes out of range (iii) produces large voltage transients during the change-in reactive power value and it may misguidedly activate the switchgear components in the system.

C. Modifying the Reactive Power Control Value of DER Units

In this scenario, thread agent can increase or decrease the reactive power (either inductive or capacitive) of the DER units (either single location or entire system) up to the maximum capacity of the DER unit. The thread agent can increase the reactive power either low or full capacity of the DER unit. If it is low (say less than 50%), then it can't be easily captured since it may not affect the active power generation in the units, however, it impacts the DPS as like as malfunction in sensor units. In case of maximum capacity, active power generation of the unit is curtailed abruptly and DER units may get tripped from the power grid. As a result: (i) large voltage transients during change-in reactive power value, (ii) it could curtail the active power of other DERs connected in the nearby locations, (iii) increase the number of switching actions of voltage regulators in the system and could

Fig. 4. Test distribution power system

VRs goes out of range, (iv) economic losses to the consumers or utility, (iv) increased power losses in the system.

IV. RESULTS AND DISCUSSION

The investigation of cyber and physical attack on DER reactive power control is tested through a 12.47 kV Southern California commercial distribution power system as shown in Fig. 4. The both Matlab/Simulink and ETAP simulation platforms are utilized to model the test system and time domain analysis is conducted with practical load profile and cloudy solar generation profile (one day with the sample size of 1 minute). Totally 140 buses are employed in the test system and the length of the system is measured as about 5.3 miles. Fifteen solar generation (DER) units are located at the different part of the system and each unit is rated at 200 kW, hence the total DER penetration of the system is calculated as 20.5%. The reactive power of such DER units is controlled by generalized IEEE volt-var control through the remote communication by the utility. In view of communication infrastructure, all DER units are divided into three groups by their locations. The reactive power of the DER groups is controlled as follows, DERs connected in group-1 follows the voltage in bus-34; group-2 follows the voltage in bus-85 and DERs connected in group-3 follows the voltage in bus-140. Moreover, test system contains an OLTC transformer connected in the substation and one SVR (connected at Bus-7) and one SCBs (connected at Bus-121) rated at 1000 kVAR are connected in the different zones of the system. The voltage dead band for OLTC unit is selected as 0.05 p.u. centered around 1.0 p.u. value, and intentional time delay is set as 60s. The safe operating grid voltage range for the test system is considered between 0.95 p.u. and 1.05 p.u. of the nominal

power grid voltage. However, the voltage dead band for SVR is selected between 0.98 p.u. and 1.02 p. u. in view of all bus voltages inside the stipulated bandwidth. The whole test system is simulated in both Matlab/Simulink and ETAP software for a day with the generalized voltage control and various cyber and physical attacks in the reactive power control in the DER units. Finally, DVC units are incorporated in the test system and is investigated with the aforesaid fault scenarios. The time constant for transient current decay, synchronous machine excitor, data processing and communication, and local grid measurement are considered as 1.5s, 1.5s, 2s, and 2s, respectively.

A. Generalized Voltage Control with VRs and DERs

The SCB is switched between 14h and 22h (i.e. peak load period) via time-based autonomous control. The initial tap position of both tap changer units (OLTC and SVR) is assumed to be at tap-0 position. The maximum active power of each solar unit generates up to 0.78 p.u. (shown in Fig. 4) and they irregularly deliver power to the grid. The solar units are followed the generalized volt-var curve and the simulated results are shown in Fig. 5. It reveals that the bus voltages are regulated through DERs, SVR, OLTC and SCB. Further, voltage transients are occurred due to the sudden variation in generation and load profile, however it has been regulated through the voltage regulators and DER units with the least time delay of 5s. It is inferred that the switching actions of SVR and OLTC units has taken as 139 and 5 tap changing operations, respectively in a day.

B. Cyber-Attacks on Reactive Power Control in DER Units

i. Modifying the slope of the voltage-reactive power curve

In this scenario the generalized volt-var curve is modified into shallow and steep curve as shown in Fig. 3a in all three groups of DER units. Both shallow and steep curves are simulated in a whole day and compared with the generalized curve results. From the results, it is inferred that the shallow curve increased the switching actions of SVRs as 141 tap

Fig. 5. Generalized grid voltage control (IEEE 1547-2018)

Fig. 6. Modifying the slope of the voltage-reactive power curve pattern in DER units

changes and voltage outside the stipulated bandwidth period is relatively high as shown in Fig. 6a. In case of steep curve, the number of switching operations of SVRs is reduced to 119 tap changes. However, it creates the grid oscillatory behavior in

the system and produces large voltage transients as shown in Fig. 6b. These transients create the issues with the load, DER units and switchgear components in the distribution system. The test results show that modifying the slope of the voltage-reactive curve pattern could create the major influence on the power grid.

ii. Modifying the voltage dead band of the voltage-reactive power curve

In this instance the voltage dead band of the generalized volt-var curve is modified as shown in Fig. 3b in all DER groups and results are shown in Fig. 7. It has showed that the voltage dead band shifted to lower voltage side, increases the number of switching actions (i.e. 171 switching operations whereas 139 for generalized curve) of SVR unit as shown in Fig. 7a, and consequently increase the period that grid voltages are outside the stipulated voltage safety limit. Furthermore, voltage dead band shifted to upper voltage side produces the grid oscillatory actions in the power grid as shown in Fig. 7b.

iii. Malfunction in current sensor in DER units

In this case, an omission fault is injected at a current sensor in group-1 DER units at 12.4h and consequently reactive power is delivered into the grid (as about 45%) as shown in Fig. 8b and impacts are given in Fig. 8a. It revealed that supplying increased inductive reactive power from certain DERs in DPS can affect the number of switching actions of VRs, i.e. SVR tap changing actions increased to 221 instead of 139 in generalized operation (shown in Fig. 5b). Further, it has

(d) Modification in deadband of volt-var curve
Fig. 11. Cyber-attack scenarios with the presence of DVC units in the system

increased the period that grid voltages are outside the stipulated voltage bandwidth. Some periods, it has produced the grid oscillatory behavior by other DERs connected in the system. This case also resembles the cyber-attack on reactive power value with the intention to slightly modify the values up to 20 to 50% of unit capacity.

iv. Modifying the reactive power control value

The maximum of 100% inductive reactive power is intentionally supplied in group-1 DER units at 12.4 h (consider as cyber-attack) and results are presented in Fig. 9. It showed that sudden change in reactive power immediately create the transients in grid voltage and subsequently tends to reduce the grid voltages in the system. As a result, DER units connected in group-1 suddenly reduces their active power generation to zero and get tripped from the grid (shown in Fig. 9b). Consequently, the number of switching actions of VRs get increased (shown in Fig. 9a) and increases the period that grid voltages outside the stipulated voltage bandwidth. If this scenario is considered in all the groups, the effect is even worse, and it could lead to blackout the entire distribution system.

In summary, Modification in slope of the curve (shallow curve) and modification in voltage dead band (voltage dead band towards the lower voltage side) result in an increase in

the number of switching operations of SVR unit and an increase in the period that grid voltages are outside the safety region. It is observed that the number of switching operations of OLTC, SVR units are increased with the volt-var curve inclined towards the flat (i.e. no reactive power support).

Modifications in slope of the curve (steep curve) and modification in voltage dead band (voltage dead band towards the higher voltage side) result in voltage oscillations in the grid. It is verified that more voltage oscillations are generated with the volt-var curve inclined towards steeper curves (i.e. high reactive power support for the given change in voltage).

Supplying inductive reactive power to the grid than capacitive reactive power (considering 40% of the DER units are affected) produce large voltage transients during the faults and afterward increase the switching operations of the OLTC and SVR units.

V. VOLTAGE CONTROL WITH DVCs IN DISTRIBUTION SYSTEM

In this case, power grid voltage is regulated through DVCs, VRs and DER units. As discussed, DVCs provide static and dynamic grid voltage support and is based on the non-linear volt-var curve. In test system, two DVCs (each rated at 500 kVar) are connected at bus-39 and bus-126, respectively. The test system is simulated for the grid voltage control with the presence of DVC, DER units and other VRs, and results are shown in Fig. 10. It has showed that the number of switching actions of VRs are marginally reduced (i.e. SVR tap changing actions reduced to 102 from 139, and OLTC switching actions reduced to 3 from 5). Further, it has merits: (i) reduction in period that grid voltages are outside the stipulated voltage bandwidth, (ii) voltage transients is reduced during the abrupt variation in load and DER generation profile.

In addition, the various cyber and physical attack scenarios are simulated with the presence of DVC units and the results are presented in Fig.11. It has revealed that modification in volt-var curve pattern does not produce grid oscillatory actions with the presence of DVC units in the system as shown in Fig. 11a. Further, change in reactive power (inductive and capacitive) in DER units also do not significantly affect the bus voltages with the presence of DVC units as compared to the system without DVC units (presented in Fig. 11b and Fig. 11c). Fig. 11d shows that inclusion of DVC unit results in a reduction in the switching operations of OLTC and SVR units compare to the conventional system during modification in voltage dead band of the volt-var curve. The above results indicate that DVC units are effectively regulate the voltage and improve the stability of the power system during unexpected failures as well as cyber and physical attack scenarios.

VI. CONCLUSION

This paper has investigated the dynamic behavior and voltage stability assessment of the distribution power system under the various cyber and physical attacks on reactive power control at DER units. It was observed that modification in volt-var curve pattern could produces dynamic oscillatory actions in the grid and could lead to blackout/brownout.

Further, malfunction in sensor units and change in inductive/capacitive reactive power in the DER units can: (i) create large voltage transients and immensely reduces or increases the power grid voltages; (ii) increased the number of switching actions of VRs, (iii) increased the period that grid voltages are outside the stipulated voltage bandwidth. As a potential solution, this paper reveals that incorporating required number and rating of DVC units in the system could neutralize the adverse effects during the fault scenarios and improve the voltage security in the distribution system

VII. ACKNOWLEDGEMENT

The authors gratefully acknowledge Southern California Edison and ETAP Inc. for providing the circuit data information and simulation support, respectively.

VIII. REFERENCES

- [1] Renewable 2018, "Global status report -A comprehensive annual overview of the state of renewable energy, 2018.
- [2] J. Johnson, D. Saleem, "Distributed energy resource cybersecurity standards," NREL Cybersecurity & Resilience Workshop, Denver, Colorado, 9 October 2017.
- [3] T.T. Ku, C.H. Lin, C.S. Chen, and C.T. Hsu, "Coordination of transformer on-load tap changer and PV smart inverters for voltage control of distribution feeders," IEEE Trans. Ind. Appl., vol. 55, no. 1, Jan./Feb. 2019.
- [4] B. Kang et al., "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," IEEE Emerging Technologies & Factory Automation Conf., pp. 1-8, Luxembourg, 2015, pp. 1-8.
- [5] S. Al-Rubaye, A. Al-Dulaimi, S. Mumtaz and J. Rodriguez, "Dynamic pricing mechanism in smart grid communications is shaping up," IEEE Communications Letters, vol. 22, no. 7, pp. 1350-1353, July 2018.
- [6] R. Das et al., "Distribution automation strategies: evolution of technologies and the business case," in IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 2166-2175, July 2015.
- [7] M. N. Kurt, Y. Yilmaz and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," IEEE Trans. Information Forensics and Security, vol. 13, no. 8, pp. 2015-2030, Aug. 2018.
- [8] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," IEEE Trans. Cybernetics, vol. 48, no. 12, pp. 3432-3439, Dec. 2018.
- [9] S. T., S. D. Sudarsan, J. Starck and T. R. Vittor, "Cyber security strategy for distribution management system and security architecture considerations," CIRED - Open Access Proceedings Journal, vol. 2017, no. 1, pp. 2653-2656, 2017.
- [10] The New York Times: Hackers are targeting nuclear facilities, homeland security dept. and F.B.I. say. Available at <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>, July 6, 2017.
- [11] Rafał Leszczyna, "Standards on cyber security assessment of smart grid, International Journal of Critical Infrastructure Protection, vol. 22, pp. 70-89, September 2018.
- [12] Electric Power Research Institute, Technical report, "National Electric Sector Cybersecurity Organization Resource - Electric sector failure scenarios and impact analysis", September 2014.
- [13] IEEE Std 1547™-2018, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, 15 February 2018.
- [14] T. Stetz, F. Marten and M. Braun, "Improved low voltage grid integration of photovoltaic systems in Germany," IEEE Trans. Sustainable Energy, vol. 4, no. 2, pp. 534-542, April 2013.
- [15] A. Joseph and T. R. Chelliah, "A Review of Power Electronic Converters for Variable Speed Pumped Storage Plants: Configurations, Operational Challenges, and Future Scopes," IEEE J. of Emerg. and Selected Topics in Power Electron., vol. 6, no. 1, pp. 103-119, March 2018.
- [16] 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, July 2017.
- [17] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber-attacks on transient stability of smart grids with voltage support devices," IEEE Power and Energy Society General Meeting (PES), pp. 1-5, Vancouver, BC, 2013.
- [18] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28-39, 2016.
- [19] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," IEEE Power and Energy Society General Meeting, pp. 1-6, Detroit, MI, USA, 2011.
- [20] B. Chen, Z. Lu and H. Zhou, "Reliability assessment of distribution network considering cyber-attacks," IEEE Energy Internet and Energy System Integration Conf., pp. 1-6, Beijing, 2018.
- [21] Y. Isozaki et al., "Detection of cyber-attacks against voltage control in distribution power grids with PVs," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 1824-1835, July 2016.
- [22] A. Teymouri, A. Mehrizi-Sani and C. Liu, "Cyber security risk assessment of solar PV units with reactive power capability," IEEE Industrial Electronics Society Conf., pp. 2872-2877, Washington, DC, 2018.
- [23] A. Joseph, K. Smedley and S. Mehraeen, "Secure high der penetration power distribution via autonomously coordinated volt/var control," IEEE Trans. on Power Deliv., (Early Access).
- [24] ANSI C84.1-2016, American national standard for electric power systems and equipment- voltage ratings (60 Hertz), June 2016.
- [25] <http://www.greentechmedia.com/articles/read/western-utilities-call-for-smart-solar-inverters>.
- [26] Keyue Smedley, "Power System Optimization" 2013 PSMA - EPRI Workshop, March 16, 2013 Long Beach California, Page 285.
- [27] D. F. Teshome, W. Xu, P. Bagheri, A. B. Nassif and Y. Zhou, "A reactive power control scheme for der-caused voltage rise mitigation in secondary systems," IEEE Trans. Sustainable Energy, Vol. 10, No. 4, pp. 1684-1695, October 2019.

Anto Joseph received the bachelor's degree in electrical and electronics Engineering from Anna University, India, in 2008, the M. Tech degree in Power Electronics and Drives from Bharath University, Chennai, India, in 2011 and the Ph.D. degree from Hydropower Simulation Laboratory, Indian Institute of Technology Roorkee, India in July 2018.

From 2011 to 2014, he was with the St. Joseph University in Tanzania, Tanzania as a Lecturer.

From August 2018 to November 2018, he was working as a Research Associate in Power Electronics Laboratory, Ajou University, Suwon, South Korea. He is currently working as a Post-Doctoral Researcher in Power Electronics Laboratory, University of California Irvine, California, USA. His current research interests include voltage control and security in power distribution system, fault diagnosis & fault tolerant operation of electrical drives, and boost power electronic converter topologies.

Keyue Ma Smedley (S'87-M'90-SM'97-F'08) Keyue Smedley received her B.S. and M.S. degrees in electrical engineering from Zhejiang University, Hangzhou, China, in 1982 and 1985, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, CA, in 1987 and 1991, respectively.

She is currently a professor in the Department of Electrical Engineering and Computer Science at the University of California at Irvine, the Director of the UCI Power Electronics Laboratory, and a cofounder of One-Cycle Control, Inc. Dr. Smedley's research interest includes high-efficiency dc-dc converters, high-fidelity class-D power amplifiers, four-quadrant three-phase and single-phase converters (covering PFC rectifiers, active power filters, inverters, VAR generation), switching capacitor converters, and utility-scale fault current limiters. Her technology has been integrated into commercial products spanning from audio amplifiers to V/VAR control, power grid dynamic voltage control, power quality control, renewable generation, energy storage system, mobile power,

microgrid, etc. Her soft switching and regenerative clamping circuits are widely used in industry. Her current research activities include power grid modeling for high penetration renewables, solar power integration, power quality control, etc.

Dr. Smedley's work has resulted in more than 200 technical publications, more than ten US/international patents, two start-up companies, and numerous commercial applications. Dr. Smedley is a recipient of UCI Innovation Award 2005. She was selected as an IEEE Fellow in 2008 for her contributions in high- performance switching power conversion. Her work with One-Cycle Control, Inc., won Department of the Army Achievement Award in the Pentagon in 2010.

Shahab Mehraeen (S'08–M'10–SM'20) received the B.S. degree in electrical engineering from Iran University of Science and Technology, Tehran, Iran, in 1995, the M.S. degree in electrical engineering from Esfahan University of Technology, Esfahan, Iran, in 2001, and the Ph.D. degree in electrical engineering from Missouri University of Science and Technology, Rolla, in 2009.

Prior to his PhD, he worked for power generation industry for four years in power plant retrofit projects and control systems. He joined the Louisiana State University, Baton Rouge, LA, USA, in 2010. His current research interests include micro grids, renewable energies, power systems dynamics, protection, and smart grids. In addition, he conducts research on decentralized, adaptive, and optimal control of dynamical systems. Shahab Mehraeen is a National Science Foundation CAREER awardee and holds a U.S. patent on energy harvesting and a few more pending.