Title
Securing Solar for the Grid: Extreme Control Whitepaper

Author
Arnold, Daniel

Publication Date
2023-10-10

Peer reviewed

S2G Extreme Control whitepaper

Daniel Arnold
Research Scientist, Grid Integration Group
Lawrence Berkeley National Laboratory

September 13, 2022

Emerging standards outlining desired behaviors for Distributed Energy Resources (DER), such as IEEE 1547-2018, define several device-level control functions to regulate DER power injections/consumptions in response to locally sensed grid conditions. The ability to adjust settings of aggregations of DER with standardized embedded control functionality constitutes a mechanism which can, potentially, create undesirable or deleterious effects on the power grid. The purpose of this white paper is to highlight unintended effects stemming from improperly tuned embedded control functions in Distributed Energy Resources (DER), which could be exploited by a malicious entity as a means to attack the power grid.

Over the period of Oct. 2021 - Mar. 2022, a series of interviews with academics and industry and utility professionals were conducted to gain insight into the potential of aggregations of DER to be utilized as a vehicle to conduct a cyber attack. The consensus opinion, based on interviewee feedback, is that while this particular threat vector is not a immediate cause for concern, it is critically important to understand any vulnerabilities introduced into the system due to standardized control functionality.

This briefing is outlined as follows: an overview of academic literature exploring this problem is provided in the next section, followed by a brief discussion of device-level control functionality recommended in IEEE 1547-2018. Then, examples of deleterious grid conditions stemming from improperly tuned

settings in aggregations of DER will be presented. The paper concludes with several recommendations for future lines of research with the goal of: 1) helping to harden the power system against known exploits of DER embedded control functionality, and 2) identifying additional vulnerabilities.

The goal of this white paper is to highlight the potential for standardized control functionality of DER to be utilized as a means to create a cyber attack on the power grid and to encourage further research and discussions on ways to revise existing standards to attempt to ameliorate this potential problem.

1 Introduction

Increasing adoption of distributed energy resources (DER), specifically rooftop photovoltaic (PV) generation systems, is challenging many conventionally-held models and practices regarding the operation of the electric power system. While the presence of DER gives individuals and communities the ability to self-generate portion of their load and participate in providing services to the grid, they also make proper management of the power system more difficult as many DER are not utility-owned/operated. With the recent changes in regulations allowing DER to gain entry into wholesale markets [1], these challenges will undoubtedly increase as more DER asset owners and aggregators seek to take advantage of new revenue streams.

Technical specifications governing the testing, interconnection, and behavior of DER are necessary to ensure the safe and reliable operation of the power system as more renewable generation sources are brought online. Of particular interest is the functionality included in the relevant standards that outlines DER behavior in response to changes in local grid conditions sensed at the point of interconnection [2, 3, 4]. These autonomous control functions essentially enlist DER to help correct undesirable frequency, voltages, and power factors and (in theory) provide a mechanism to allow DER to mitigate power quality issues that they themselves can introduce in grids with high penetrations of renewables.

However, as architectures and topologies can vastly differ, the most notable standard, IEEE 1547, includes provisions allowing the autonomous control response of DER to be adjusted by the area electric power system (Area EPS) operator or other authorized entity (see Table 8 of [2]). This capability *remotely* to adjust the control response of individual DER may, at first glance, seem innocuous. However, when an Area EPS or other entity institutes small changes in large aggregations of devices the resulting affect on the grid can be quite profound. An excellent example of the extent to which remote updates to aggregations of DER can affect the power grid was demonstrated in Hawaii, where local utilities worked with a smart inverter vendor to remotely increase the frequency ride through capabilities of 800,000 inverters in a single day [5].

Of particular concern, the remote update capability of many DER presents a vulnerability that a malicious entity could purposefully exploit to introduce system instabilities or other harmful power quality conditions [6]. Security researchers have identified exploitable vulnerabilities in deployed inverter firmware

[7], foreign nations are actively targeting the US bulk power system [8], and in at least one instance, a US inverter control system has been successfully attacked [9].

While the remote update feature of DER undoubtedly include *cease to energize* (i.e., remote disconnect) capabilities, this document focuses specifically on updates to parameters of autonomous control functions (e.g., Volt-VAR control). The reason for this emphasis is that deleterious effects manifesting in the power system due to parameter updates in these controllers are more difficult to ascertain by monitoring updates sent to individual devices, as opposed to checking for device on/off (disconnect) commands. Commanded changes in setpoints or in control parameters might seem relatively small individually, but will have an out-sized effect on the system when applied to DER en masse. Thus, small changes to parameters of these controllers are difficult to clearly assess as harmful.

As is true with any control system, proper calibration or tuning of control parameters is crucial to ensure correct performance. numerous works have emerged showing that proper configuration of individual devices is crucial for the stable operation of the DER population. Jahangiri et al. [10] discussed the phenomenon of "hunting" in voltages in systems with VV control. Farivar et al. [11] modeled the interaction between system voltage magnitudes and PV inverter VV functions as a feedback control loop which explicitly tied the slopes of VV controllers of inverters to unstable (highly oscillatory) reactive power injections. Although the instability threshold depends on the network characteristics, instability is reached when the slopes of the VV control curves become too steep. Numerous other works have also modeled the inverter/grid interaction as a first-order feedback controller and arrived at similar stability conditions [12, 13, 14, 15, 16].

This paper is structured as follows. In Section II, an overview of autonomous control functionality in IEEE 1547 will be provided. Section III will discuss two use cases of how improper smart inverter settings can create power quality issues in distribution networks Section IV will discuss recommendations for future research needs, emphasizing efforts to identify unknown vulnerabilities in DER autonomous control functions via the use of artificial intelligence.

2 IEEE 1547 Overview

Section 5 of the IEEE 1547 standard puts forth requirements for reactive power and voltage/active power control. A complete overview of these capabilities is beyond the scope of this document, but a brief description is warranted here. It should be noted that while the standard allows agreements between the Area EPS operator and the DER operator to override requirements outlined in Section 5 of the standard, it is likely such agreements will not replace the standard requirements for the large majority of DER, at least in the immediate future.

2.1 Reactive Power Capabilities of DER

IEEE 1547 specifies several mutually exclusive modes of reactive power control. These are:

- Constant power factor mode
- Voltage-reactive power mode (also known as Volt-VAR)
- Active power-reactive power mode
- Constant reactive power mode

While constant power factor mode with a unity power factor settings is the recommended default operating mode of installed DER, other modes of operation can be enabled if mutually agreed upon by the Area EPS and DER operators. Constant power factor mode and constant reactive power mode are somewhat self-explanatory: the DER will maintain a constant power factor or reactive power, respectively. The target power factor or reactive power level/mode can be adjusted locally or remotely with the approval of the Area EPS operator.

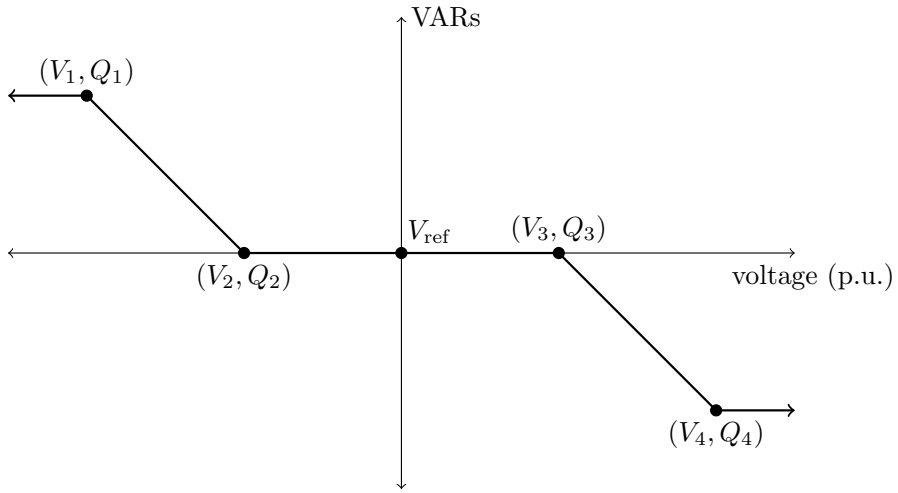

Figure 1: Inverter Volt-VAR curve. Positive values denote VAR injection. v_{nom} is the nominal voltage value.

Voltage-reactive power mode (a.k.a. Volt-VAR control) and active power-reactive power mode are more complicated mechanisms that adjust reactive power as a function of locally sensed voltage and reactive power output (respectively) according to piecewise linear characteristics. The characteristics themselves are depicted in Figs. 1-3, where it is clear that the piecewise linear characteristic curves are parameterized by a set of points (V_i, Q_i), (V_i, P_i), which define the shape of the function. Default settings for both category A

and B DER [1], as well as ranges of allowable settings are provided in Tables 8 and 9 of the IEEE 1547 standard (shown in Figs. 2 - 4, respectively). Similarly to Constant power factor and Constant reactive power modes, settings for Voltage-reactive power and Active power-reactive power control modes can be adjusted locally or remotely with the approval of the Area EPS operator. It is worth noting that Table 8 of the IEEE standard (Fig. 2) explicitly mentions the link between system instabilities and improperly chosen Volt-VAR settings in footnote **c**.

2.2 Active Power Capabilities of DER

The modulation of active power as a mechanism to regulate voltage is recommended as a mandatory capability in Category B DER. The Voltage-active power mode (also known as Volt-Watt control) is disabled by default, but can be enabled at the discretion of the Area EPS operator. When activated, this mode allows the DER to limit maximum active power as a function of locally sensed voltage according to a piecewise linear characteristic. An example of a Voltage-active power characteristic function is depicted in Fig. 3, where it is clear that the shape of the function is determined by the set of points (V_i, P_i). Default settings for the Voltage-active power control mode, as well as ranges of allowable settings are provided in Table 10 of the IEEE 1547 standard. Similarly to control modes for Reactive power control, settings for Voltage-active power can be adjusted locally or remotely with the approval of the Area EPS operator.

3 Vulnerabilities

This section highlights known vulnerabilities stemming from manipulations of settings of Volt-VAR and Volt-Watt controllers in aggregations of DER (specifically photovoltaic systems). Simulations of DER and electric grid behavior were conducted using a python-based software package that models DER dynamics, Volt-VAR, and Volt-Watt capabilities in python and interacts with OpenDSS to resolve network power flows [2].

Volt-VAR and Volt-Watt functions (depicted in Figs. 1 3) compute reactive and active power set-points, respectively, as functions of deviations of locally sensed voltages from a nominal value (typically 1 p.u.). Let $f_{p,i}(v_i)$ and $f_{q,i}(v_i)$ denote the Volt-VAR and Volt-Watt piecewise characteristic curves for a DER at node i. Consistent with [17] we adopt a simplified dynamic model of a photovoltaic smart inverter for the subsequent stability analysis, illustrated in Fig. 5.

As is shown in the figure, the grid voltage v is the input to the VV and VW controllers. The maximum available active power from the solar array, $\bar{p}$, is also input into the VW controller, which along with v, determines the maximum

[1] please refer to IEEE 1547 standard [2] for definitions of Category A and B DER
[2] `https://secpriv.lbl.gov/project/ceds-cigar/`

Table 8—Voltage-reactive power settings for normal operating performance Category A and Category B DER

Voltage-reactive power parameters	Default settings		Ranges of allowable settings	
	Category A	Category B	Minimum	Maximum
V_{Ref}	V_N	V_N	0.95 V_N	1.05 V_N
V_2	V_N	V_{Ref} – 0.02 V_N	Category A: V_{Ref} Category B: V_{Ref} – 0.03 V_N	V_{Ref} [c]
Q_2	0	0	100% of nameplate reactive power capability, absorption	100% of nameplate reactive power capability, injection
V_3	V_N	V_{Ref} + 0.02 V_N	V_{Ref}[c]	Category A: V_{Ref} Category B: V_{Ref} + 0.03 V_N
Q_3	0	0	100% of nameplate reactive power capability, absorption	100% of nameplae reactive power capability, injection
V_1	0.9 V_N	V_{Ref} – 0.08 V_N	V_{Ref} – 0.18 V_N	V_2 – 0.02 V_N[c]
Q_1[a]	25% of nameplate apparent power rating, injection	44% of nameplate apparent power rating, injection	0	100% of nameplate reactive power capability, injection[b]
V_4	1.1 V_N	V_{Ref} + 0.08 V_N	V_3+0.02 V_N[c]	V_{Ref} + 0.18 V_N
Q_4	25% of nameplate apparent power rating, absorption	44% of nameplate apparent power rating, absorption	100% of nameplate reactive power capability, absorption	0
Open loop response time	10 s	5 s	1 s	90 s

[a]The DER reactive power capability may be reduced at lower voltage.
[b]If needed DER may reduce active power output to meet this requirement.
[c]Improper selection of these values may cause system instability.

Figure 2: Table 8 from IEEE 1547 standard [2]. Note the explicit mention on system instabilities resulting from improper settings in the last footnote.

amount of reactive power available for injection/consumption $\bar{q}$ that is then input to the VV controller. The active and reactive power setpoints produced by the VW and VW controllers are then low pass filtered by $H_O(s)$ to produce the active and reactive power injections that are injected into the grid. These filters serve to limit the rate at which the active and reactive powers injected by PV systems can change and do not represent physical constraints of the smart inverter devices themselves [4].

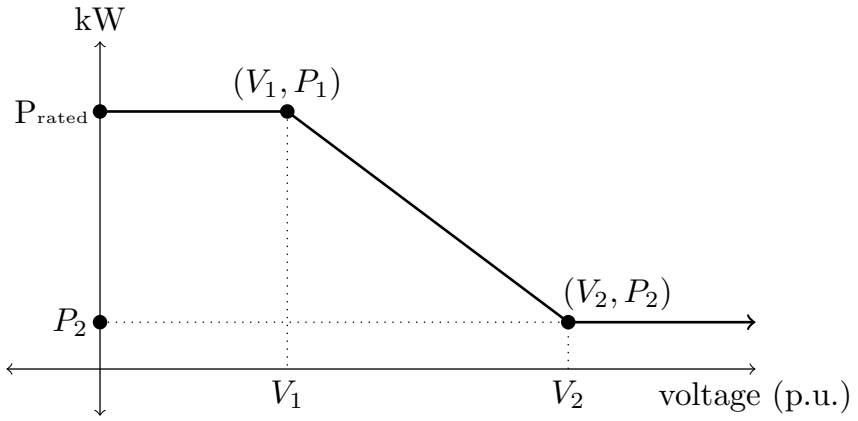

Figure 3: Inverter Volt-Watt curve. Positive values denote watt injection. v_{nom} is the nominal voltage value.

Table 9—Active power-reactive power settings for normal operating performance Category A and Category B DER

Active power-reactive power parameters	Default settings		Ranges of allowable settings	
	Category A	Category B	Minimum	Maximum
P_3	P_{rated}		$P_2 + 0.1\ P_{rated}$	P_{rated}
P_2	$0.5\ P_{rated}$		$0.4\ P_{rated}$	$0.8\ P_{rated}$
P_1	The greater of $0.2\ P_{rated}$ and P_{min}		P_{min}	$P_2 - 0.1\ P_{rated}$
P'_1	The lesser of $0.2 \times P'_{rated}$ and P'_{min}		$P'_2 - 0.1\ P'_{rated}$	P'_{min}
P'_2	$0.5\ P'_{rated}$		$0.8\ P'_{rated}$	$0.4\ P'_{rated}$
P'_3	P'_{rated}		P'_{rated}	$P'_2 + 0.1\ P'_{rated}$
Q_3	25% of nameplate apparent power rating, absorption	44% of nameplate apparent power rating, absorption	100% of nameplate reactive power absorption capability	100% of nameplate reactive power injection capability
Q_2	0			
Q_1	0			
Q'_1	0			
Q'_2	0			
Q'_3	44% of nameplate apparent power rating, injection			

NOTE— P_{rated} is the nameplate active power rating of the DER.
P'_{rated} is the maximum active power that the DER can absorb.
P_{min} is the minimum active power output of the DER.
P'_{min} is the minimum, in amplitude, active power that the DER can absorb.
P' parameters are negative in value.

Figure 4: Table 9 from IEEE 1547 standard [2].

3.1 Voltage Instabilities

Several efforts in academic literature have identified the link between Volt-VAR settings and voltage instabilities in networks with high penetrations of DER. In a seminal effort, Farivar et al. [11] modeled the interaction between system voltage magnitudes and PV inverter VV functions as a feedback control loop which explicitly tied the slopes of VV controllers of inverters to unstable (highly

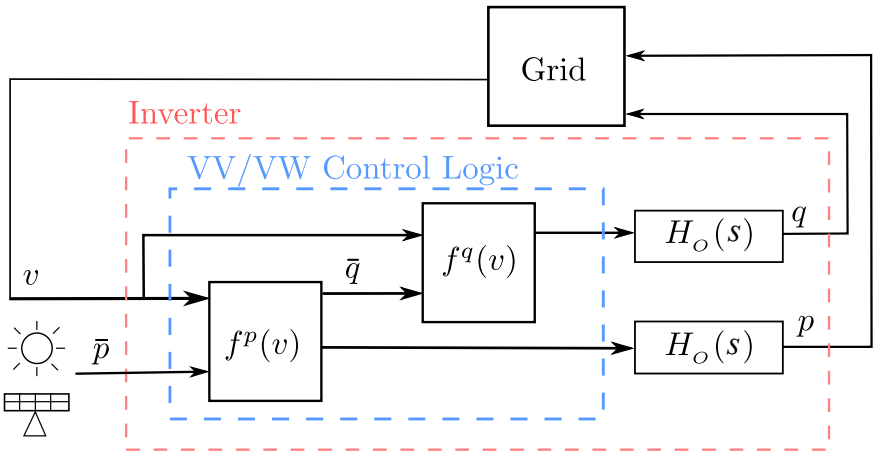

Figure 5: Block diagram of VV and VW control logic of an inverter.

oscillatory) reactive power injections. The analysis showed that the instability threshold depends both on the network characteristics and the "steepness"" of the Volt-VAR piecewise linear characteristics. Numerous other works have also modeled the inverter/grid interaction as a first-order feedback controller and arrived at similar stability conditions [12, 13, 14, 15, 16]. Notably, in [14, 16] the analysis was also extended to consider both Volt-VAR and Volt-Watt controllers.

Based on the model presented in Fig. 5, one can use tools from systems theory to derive a stability criterion for the feedback interaction of aggregations of DER with VV/VW capabilities (see Appendix, Eq. (13)). Consistent with the aforementioned work, the stability threshold is a function of the network topology ($\boldsymbol{R}$,$\boldsymbol{X}$) and the steepest regions of the piecewise linear VV and VW characteristics ($\boldsymbol{C_p}$,$\boldsymbol{C_q}$). With this in mind, it is straightforward to demonstrate how these functions could be utilized to destabilize the feedback interconnection. For example, with regard to Figs. 1, 2, one could choose $V_3 = V_4 = 0$, $V_1 = V_2 - 0.02V_N$, and $V_4 = V_3 - 0.02V_N$ to remove the deadzone and steepen the curve. The attack could then be instantiated by assigning V_{ref} to be slightly larger or smaller in magnitude than the recent average voltage seen by individual DER. An example of the voltage instabilities (oscillations) created via smart inverters using logic similar to the previous discussion is shown in Fig. 6 in the top subplot.

3.2 Voltage Imbalances

It is also possible to create a network voltage unbalance (VU) by exploiting standardized smart inverter functionality and the single-phase nature of residential DER. Such an attack may seek to trip VU relays and/or cause sensitive equipment to trip offline [18]. Similar to [19], in this situation it is assumed that the adversary has already gained access to a subset of network DER and

seeks to maliciously re-configure their control logic to disrupt distribution grid operations.

VU is one of the main power quality concerns for distribution utilities, with standards and/or requirements establishing VU limits [20, 21]. Historically, the major cause of VU has been the unequal distribution of single-phase loads within a three-phase distribution network [18]. Recently, however, the addition of single-phase residential photovoltaic (PV) generation had further raised the level of concern [22]. Previous work has examined VU in low-voltage networks, primarily due to inherent unequal load distribution [23, 24, 25].

Manipulating the settings of smart inverter VV and VW control to create voltage imbalances in the system is also a straightforward process. In this case, consider the following set of voltage values that define the intersection of piecewise linear segments in Fig. 1:

$$\hat{V} = [V_1, V_2, V_3, V_4] = [0.98, 1.01, 1.01, 1.04]. \quad (1)$$

Given this VV curve, an adversary could create a voltage imbalance via an assignment similar to the following: $V_a = \hat{V} - 0.1$, $V_b = \hat{V} + 0.1$, and $V_c = \hat{V} - 0.1$, where V_a refers to the VV curves for all inverters on phase A, etc.. An example of the voltage imbalance created via smart inverters using logic similar to the previous discussion is shown in Fig. 6 in the bottom subplot.

4 Conclusions

The overall premise of this white paper is that small adjustments in aggregations of smart inverter control functions can lead to deleterious grid conditions. Existing control standards may introduce unintended behaviors in aggregations of DER that could be exploited in a cyber attack. Improperly chosen settings in smart inverter autonomous control functions can lead to deleterious grid conditions. Here, two vulnerabilities were discussed. The first potential exploit of the ability to remotely update smart inverter settings is to adjust the VV/VW curves to destabilize the feedback interconnection of the smart inverter population and the electric grid. The result of this manipulation is the manifestation of oscillations in DER power injections, resulting in oscillating voltages. The second exploit is to heterogeneously adjust VV/VW settings across different phases in multiphase systems, resulting in voltage imbalances. In both cases, simple heurestic rules were presented outlining how to create these conditions when portions of the smart inverter-driven DER are maliciously adjusted.

Future work is needed to further understand the nature of the vulnerabilities presented in this work and to assess if control functions being put forth in emerging standards introduce other vulnerabilities in DER populations. We propose two complementary lines of research to make progress on addressing this problem.

First, additional simulation studies should be conducted to investigate ways in which autonomous control functions in IEEE 1547 can be exploited via cyber intrusion to adversely affect the power grid, and to identify a set of power system

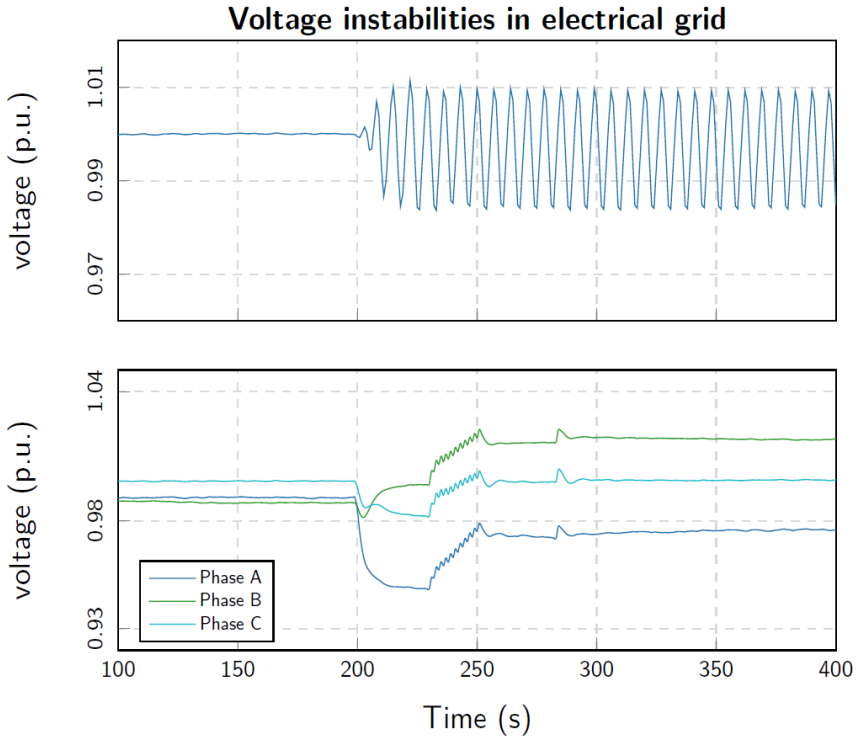

Figure 6: Example of unstable oscillations (top) and voltage imbalances (bottom) that can be created via manipulations of VV/VW settings in smart inverters.

topology characteristics that are more vulnerable to certain types of malicious parameter adjustments. Dynamic and quasi-static time series simulations of power grids with smart inverter dynamics and autonomous control functions can provide an environment in which different settings of IEEE 1547 control functions can be tested. The main benefit of this effort will be helping to determine additional vulnerabilities/exploits in standardized control functions. This will be critical to ensuring new vulnerabilities are not introduced as part of DER standards activities and will lower the risk of adoption of DER smart inverter capabilities.

The second line of research which could be used to address DER-introduced vulnerabilities contained in emerging standards is to investigate the creation of a software tool to determine appropriate parameters of smart inverter control functions on a network specific basis. Parameters for smart inverter control functions can be chosen to maximize hosting capacity, minimize power quality issues, and make the system maximally resistant to the effects of cyber attacks on DER. To achieve this, artificial intelligence and optimization techniques can be leveraged to determine appropriate parameters of smart inverter control func-

tions for different networks. The software tool should ensure settings in DER are maximally resilient to cyber attacks while maintaining operational objectives (e.g., hosting capacity, etc.). Providing a toolset/guidance on how smart inverter control settings should be determined as to not cause adverse grid conditions will lessen risk to EPS operators and encourage the use of advanced inverter functionality.

5 Appendix

5.1 Volt-VAR and Volt-Watt Stability Criterion

Let the graph $\mathcal{G} = (\mathcal{N} \cup \{0\}, \mathcal{L})$ represent a balanced radial distribution feeder, where $\mathcal{N}$ is the set of nodes (excluding the substation) and $\mathcal{L}$ is the set of line segments, where $|\mathcal{N}| = |\mathcal{L}| = n$. For a given bus $i \in \mathcal{N}$, let $\mathcal{L}_i$ (where $\mathcal{L}_i \subseteq \mathcal{L}$) denote the collection of line segments from node 0 (e.g. the substation) to node i. The *DistFlow* equations [26] capture the relationship between power flowing in line segment $(i, j) \in \mathcal{L}$ and the voltage magnitude drop between nodes i and j:

$$P_{ij} = p_j^c - p_j^g + r_{ij} c_{ij} + \sum_{k:(j,k)\in\mathcal{L}} P_{jk} \tag{2a}$$

$$Q_{ij} = q_j^c - q_j^g + x_{ij} c_{ij} + \sum_{k:(j,k)\in\mathcal{L}} Q_{jk} \tag{2b}$$

$$v_j^2 - v_i^2 = -2\big(r_{ij} P_{ij} + x_{ij} Q_{ij}\big) + \big(r_{ij}^2 + x_{ij}^2\big) c_{ij}^2, \tag{2c}$$

where v_i^2 is node i squared voltage magnitude, P_{ij} and Q_{ij} denote the active/reactive power flowing in line segment (i, j), r_{ij} and x_{ij} are line segment (i, j) resistance and reactance, and c_{ij} are losses. For node i, active (reactive) power consumption is denoted by p_i^c (q_i^c) and active (reactive) power generation, due to DER, is denoted by p_i^g (q_i^g).

Consistent with [27, 11], we neglect losses in (2a) - (2c) which is achieved via setting $c_{ij} = 0$ for all $(i, j) \in \mathcal{L}$. Furthermore, as $v_i \approx 1$ we approximate $v_j^2 - v_i^2 \approx 2(v_j - v_i)$. Let $\beta(j)$ denote the set of all nodes descended from j (including j itself). With these changes, the *DistFlow* model becomes:

$$P_{ij} = \sum_{k\in\beta(j)} \big(p_k^c - p_k^g\big) \tag{3a}$$

$$Q_{ij} = \sum_{k\in\beta(j)} \big(q_k^c - q_k^g\big) \tag{3b}$$

$$v_i - v_j = r_{ij} P_{ij} + x_{ij} Q_{ij}. \tag{3c}$$

The now linearized system of (3a) - (3c) can be more compactly represented via substituting (3a) and (3b) into (3c) and making successive substitutions of voltages from upstream nodes yielding node i voltage as a function of feeder head voltage v_0. If one defines the following vectors:

$$\mathbf{v} = [v_1, \ldots, v_n]^\top, \quad \mathbf{v_0} = v_0 \mathbf{1} \tag{4a}$$

$$\mathbf{p^c} = [p_1^c, \ldots, p_n^c]^\top, \quad \mathbf{p^g} = [p_1^g, \ldots, p_n^g]^\top \tag{4b}$$

$$\mathbf{q^c} = [q_1^c, \ldots, q_n^c]^\top, \quad \mathbf{q^g} = [q_1^g, \ldots, q_n^g]^\top, \tag{4c}$$

then the system of (3a) - (3c) can be recast in vector form:

$$\mathbf{v} = \mathbf{v_0} + \mathbf{R}\big(\mathbf{p^g} - \mathbf{p^c}\big) + \mathbf{X}\big(\mathbf{q^g} - \mathbf{q^c}\big), \tag{5}$$

where $\mathbf{R}$ and $\mathbf{X}$ are completely positive matrices [11] and

$$R_{ij} = \sum_{(h,k)\in\mathcal{L}_i \bigcap \mathcal{L}_j} r_{hk} \tag{6a}$$

$$X_{ij} = \sum_{(h,k)\in\mathcal{L}_i \bigcap \mathcal{L}_j} x_{hk}. \tag{6b}$$

Defining $\mathbf{Z} = [\mathbf{R}, \mathbf{X}]$, $\mathbf{s}^c = [\mathbf{p}^c, \mathbf{q}^c]^\top$, and $\mathbf{s}^g = [\mathbf{p}^g, \mathbf{q}^g]^\top$, (5) can expressed compactly as:

$$\mathbf{v} = \mathbf{v_0} + \mathbf{Z}\big(\mathbf{s}^g - \mathbf{s}^\mathbf{c}\big). \tag{7}$$

We now develop a dynamic model of smart inverters, modeled by Fig. 5, connected to the distribution grid. Without loss of generality, we assume the presence of a VV and VW capable smart inverter at each node in the system. To begin, let $\mathbf{f}(\mathbf{v}) = [\mathbf{f}_p(\mathbf{v}), \mathbf{f}_q(\mathbf{v})]^\top$ denote the collection of inverter VV and VW functions at each node in $\mathcal{G}$, where:

$$\mathbf{f}_p(\mathbf{v}) = [f_{p,1}(v_1), \ldots, f_{p,n}(v_n)]^\top \tag{8a}$$

$$\mathbf{f}_q(\mathbf{v}) = [f_{q,1}(v_1), \ldots, f_{q,n}(v_n)]^\top, \tag{8b}$$

where both $f_{p,i}(v_i)$ and $f_{q,i}(v_i)$ are locally Lipschitz with constants $C_{p,i}$ and $C_{q,i}$, respectively. Define the matrices

$$\mathbf{C}_p = \text{diag}([C_{p,1}, \ldots, C_{p,n}]) \tag{9a}$$

$$\mathbf{C}_q = \text{diag}([C_{q,1}, \ldots, C_{q,n}]) \tag{9b}$$

$$\mathbf{C}_s = \begin{bmatrix}\mathbf{C}_p & \mathbf{C}_q\end{bmatrix}^\top. \tag{9c}$$

Under the additional assumption that active and reactive power consumption due to system loads change slowly with respect to inverter control actions, (7) can be recast in the following form:

$$\mathbf{v} = \mathbf{Z}\mathbf{s} + \underbrace{\mathbf{v_0} - \mathbf{Z}\mathbf{s}^\mathbf{c}}_{\bar{\mathbf{v}}}, \tag{10}$$

where the superscript has been dropped from $\mathbf{s}$ for convenience and $\bar{\mathbf{v}}$ is treated as constant. Consistent with Fig. 5, the dynamics of the inverter, which consist of nonlinear Volt-VAR & Volt-Watt controllers in series with first order low pass filters, can be expressed as [16]:

$$\mathbf{T}\dot{\mathbf{s}} = \mathbf{f}(\mathbf{v}) - \mathbf{s}, \tag{11a}$$

$$\mathbf{v} = \mathbf{Z}\mathbf{s} + \bar{\mathbf{v}} \tag{11b}$$

where $\mathbf{T} \in \mathbb{R}^{2n\times 2n}$ is a diagonal and positive definite matrix that collects low pass filter time constants. Substituting (11b) into (11a) yields the desired dynamics in terms of the state variable $\mathbf{s}$:

$$\mathbf{T}\dot{\mathbf{s}} = \mathbf{f}(\mathbf{Z}\mathbf{s} + \bar{\mathbf{v}}) - \mathbf{s}. \tag{12}$$

For simplicity, assume all DER smart inverter low pass filters have equivalent time constants (or, $\mathbf{T} = \mathbf{I}$). As proven in [17], the system of (12) is stable if the following criteria is satisfied:

$$\left\|\mathbf{C}_s\mathbf{Z}\right\|_2 \leq 1. \tag{13}$$

References

[1] "FERC Order No. 2222: Fact Sheet," Available: https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet, Federal Energy Regulatory Comission, accessed: Sept. 2022. [Online].

[2] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, Institute of Electrical and Electronics Engineers, IEEE 1547-2018, April 2018.

[3] *Rule 21 Interconnection*, Available: https://www.cpuc.ca.gov/Rule21/, California Public Utilities Commission, Std.

[4] B. Seal, "Common Functions for Smart Inverters, 4th Ed." Electric Power Research Institute, Tech. Rep. 3002008217, 2017.

[5] P. Fairley, "800,000 Microinverters Remotely Retrofitted on Oahu in One Day," Available: https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu, accessed: Jun. 2019. [Online].

[6] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, pp. 5326–5340, Oct. 2021.

[7] W. Westerhof, "Practical Proof - Horus Scenario," Available: https://horusscenario.com/practical-proof/, accessed: Jan. 2021. [Online].

[8] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (Alert TA18-074A)," Available: https://us-cert.cisa.gov/ncas/alerts/TA18-074A, U.S. Cybersecurity & Infrastructure Security Agency, accessed: Jan. 2021. [Online].

[9] "Risks Posed by Firewall Firmware Vulnerabilities," Available: https://www.nerc.com/pa/rrm/ea/Lessons\%20Learned\%20Document\%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf, North American Electric Reliability Corporation, accessed: Jan. 2021. [Online].

[10] P. Jahangiri and D. C. Aliprantis, "Distributed volt/var control by pv inverters," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3429–3439, April 2013.

[11] M. Farivar, L. Chen, and S. Low, "Equilibrium and dynamics of local voltage control in distribution systems," in *Proc. IEEE Conf. Decis. Control*, Dec 2013, pp. 4329–4334.

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

[13] J. H. Braslavsky, L. D. Collins, and J. K. Ward, "Voltage stability in a grid-connected inverter with automatic volt-watt and volt-var functions," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 84–94, 2019.

[14] K. Baker, A. Bernstein, E. Dall'Anese, and C. Zhao, "Network-cognizant voltage droop control for distribution grids," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 2098–2108, 2018.

[15] A. Eggli, S. Karagiannopoulos, S. Bolognani, and G. Hug, "Stability analysis and design of local control schemes in active distribution grids," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1900–1909, May 2021.

[16] S. S. Saha, D. Arnold, A. Scaglione, E. Schweitzer, C. Roberts, S. Peisert, and N. G. Johnson, "Lyapunov stability of smart inverters using linearized distflow approximation," *IET Renew. Power Gener.*, vol. 15, no. 1, pp. 114–126, 2021.

[17] D. Arnold, S. S. Saha, S.-T. Ngo, C. Roberts, A. Scaglione, N. G. Johnson, S. Peisert, and D. Pinney, "Adaptive control of distributed energy resources for distribution grid voltage stability," *IEEE Transactions on Power Systems*, pp. 1–1, 2022.

[18] A. Von Jouanne and B. Banerjee, "Assessment of voltage unbalance," *IEEE Transactions on Power Delivery*, vol. 16, no. 4, pp. 782–790, 2001.

[19] C. Roberts, S.-T. Ngo, A. Milesi, S. Peisert, D. Arnold, S. Saha, A. Scaglione, N. Johnson, A. Kocheturov, and D. Fradkin, "Deep reinforcement learning for der cyber-attack mitigation," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2020, pp. 1–7.

[20] "American national standard for electric power systems and equipment—voltage ratings (60 hz)," *ANSI C84.1-2016*, 2016.

[21] "IEEE recommended practice for monitoring electric power quality," *IEEE Std 1159-2019 (Revision of IEEE Std 1159-2009)*, pp. 1–98, 2019.

[22] A. Dubey, S. Santoso, and A. Maitra, "Understanding photovoltaic hosting capacity of distribution circuits," in *2015 IEEE Power & Energy Society General Meeting*. IEEE, 2015, pp. 1–5.

[23] F. Shahnia, P. J. Wolfs, and A. Ghosh, "Voltage unbalance reduction in low voltage feeders by dynamic switching of residential customers among three phases," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1318–1327, 2014.

[24] M. Savaghebi, A. Jalilian, J. C. Vasquez, and J. M. Guerrero, "Secondary control scheme for voltage unbalance compensation in an islanded droop-controlled microgrid," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 797–807, 2012.

[25] S. Acharya, M. S. El-Moursi, A. Al-Hinai, A. S. Al-Sumaiti, and H. H. Zeineldin, "A control strategy for voltage unbalance mitigation in an islanded microgrid considering demand side management capability," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2558–2568, 2018.

[26] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Trans. Power Del.*, vol. 4, no. 1, pp. 735–743, Jan 1989.

[27] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Trans. Power Del.*, vol. 4, no. 2, pp. 1401–1407, 1989.