SAND2019-1903C

Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources

Nicholas Jacobs*, Shamina Hossain-McKenzie*, Deepu Jose*, Danish Saleem†, Christine Lai*, Patricia Cordeiro*, Adarsh Hasandka†, Maurice Martin†, Christopher Howerter*

*Cyber Resilience R&D
Sandia National Laboratories
Albuquerque, USA
{njacobs,shossai,djose,cflai,pgcorde,cmhower}@sandia.gov

†Energy, Security, and Resilience Center
National Renewable Energy Laboratory
Golden, USA
{Danish.Saleem,Adarsh.Hasandka,Maurice.Martin}@nrel.gov

***Abstract*—As the power grid incorporates increasing amounts of distributed energy resources (DER) that provide new generation sources, new opportunities are created for improving operation of the grid while large challenges also arise for preserving grid reliability and security. To improve grid performance, DERs can be utilized to provide important support functionality, such as supporting frequency and voltage levels, especially if they are assisted by communication schemes as part of an advanced distribution management system (ADMS). Unfortunately, such connectivity and grid support functionality also creates additional cyber security risk with the potential for degradation of grid services, especially under conditions with high amounts of distributed generation. This paper will first discuss the communications needed by DERs to support system and interoperability objectives, as well as the security requirements and impact of securing these communications. Some common security mechanisms are discussed in relation to DERs, and a simulated 15-bus model of a distribution feeder is used to demonstrate aspects of the DER communications and impact to grid performance. These results help to advance understanding of the benefits, requirements, and mechanisms for securely implementing DER communications while ensuring that grid reliability is maintained.**

***Index Terms*—Distributed Energy Resources, Cybersecurity, Interoperability, Smart Grid, Grid Security**

I. Introduction

The electric industry is at a point where it is adding large amounts of new distributed generation sources in many geographically separated locations, in contrast to the historical paradigm of large, centralized generation facilities. This new paradigm of high numbers of distributed energy resources (DER) incorporated into the grid creates a difficult challenge for adequately controlling these resources, while also providing opportunities for new advanced control schemes to support grid performance and reliability, such as in advanced distribution management systems (ADMS).

With the increased amount of DER and distributed control within the bulk power system (BPS), the importance of securing, maintaining, and operating these assets will only increase in the coming years. While the operation of these DERs presents an opportunity for increased awareness and improved control of the grid, it also creates additional attack surfaces coupled with potentially high amounts of generation capacity that can severely degrade grid performance if compromised [2]. For instance, as reported in early 2015, over 800,000 microinverters in the state of Hawaii were updated remotely in a single day, representing about 60% of the state's solar capacity. This feat is an achievement demonstrating advanced capability for inverter maintenance, yet also raises a serious question on the security of the grid when such a capability exists [3]. This is not just an idle speculation, as shown in recent history. Numerous cases have shown that the infrastructure of the BPS can be attacked through cyber means, with the consequence of degradation to service and even potential for physical damage. One notable example took place in December 2015, when a large amount of the Ukrainian power grid was taken offline for several hours due to a cyber attack that targeted grid control systems [4].

Understanding the problem as well as avenues to address challenges give a way forward to achieving improved cybersecurity for DER. One such challenge faced by smart inverters is that they typically speak Modbus, a communications protocol initially developed and released in 1979 and which contains no built-in security mechanisms [6]. Because of this, it can be attacked in numerous common ways, such as described in

This material is based on work supported by the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) Project Module-OT: Modular Security Apparatus for Managing Distributed Cryptography for C&C on OT Networks.

[5], which presents various attack taxonomies for the Modbus protocol. Another protocol used often within the electric power industry is DNP3, which also has severe security limitations [8]. However, these limitations can be addressed by incorporating additional security mechanisms around the protocol communications, such as by utilizing transport layer security (TLS) to secure the transport layer of the communications [7].

Section II will describe the communications required for DER to support grid functions, the security requirements of these communications, and the cost of various security mechanisms that may be applied to ensure those security requirements are met, Section III will describe the system modeling and analysis used to show system and interoperability impact, and finally Section IV will provide conclusions.

II. Security Impact to DER Grid-Support Functionality

As DER penetration increases, grid-support functions, such as frequency or voltage support, are further motivated and enabled. These grid services assist with grid stability, power quality, and other grid performance needs. This is especially true in the case of microgrids and virtual power plants, where power quality considerations in the locality of the distribution system become much more critical than in classical power systems that are mainly supported by large generation facilities. With the evolution of the grid in recent years to better use technology and communications to support grid reliability and enable the implementation of extensive renewable energy resources, IEEE Std. 1547 provides specifications and requirements for interconnection and interoperability between DER and utility power systems to achieve such capabilities [9]. Furthermore, a reference logical model for DER was developed by the Electric Power Research Institute (EPRI) based on the wider reference model for the electric grid in the National Institute of Standards & Technology (NIST) Interagency Report, NISTIR 7628 [10]. This model, as shown in Fig. 1, describes the necessary logical connections for DER and helps to illustrate where DER communications are required to support grid operation [11].

Regulations concerning interoperability requirements for DER have begun to be developed and implemented as well. In 2017, California updated its Electric Rule 21 to mandate new interconnection requirements for DER connecting to distribution systems with the state in order to ensure safe and reliable energy generation [12].

A. Security Principles

As DERs are incorporated into the grid, it is important to consider what security principles are needed to ensure security is maintained. Typical security principles used to guide such analysis are confidentiality, integrity, and availability, often referred to as the CIA triad, with a few others such as non-repudiation and authentication of import as well [13].

Confidentiality refers to the need that information be protected from disclosure to unauthorized parties, while integrity

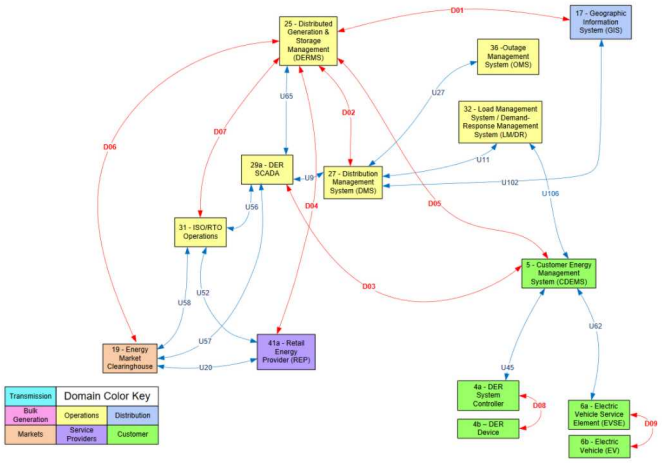

Fig. 1. EPRI DER Logical Reference Model, from [11]

ensures data is not modified or corrupted, and availability ensures that information can be acquired and used when needed. Examples of security breaches for each of these principles are information leakage or modification of data through a man-in-the-middle (MITM) or denial-of-service (DOS), respectively.

The relative importance of these principles may vary with different types of DER communications. Furthermore, security mechanisms used to ensure confidentiality, integrity, and availability also come with increased overhead and processing requirements which may impact DER communications and the ability to support grid services. These considerations will be discussed in a general fashion in the following sections.

B. DER Communications

As noted in the previous section, there are varying levels of importance for security principles depending on the message type and the constraints of that specific communication function. To best protect DER communications, this section discusses the specific services and communications used by smart inverters for grid-support functions, as specified by the Common Smart Inverter Profile (CSIP) and by information models put together by the SunSpec Alliance, an alliance of various participants in the distributed energy industry [14], [15]. Note that in this paper we will use the terms DER and inverter interchangeably, as this discussion concentrates on smart inverter functionality instead of other types of DERs.

In discussing security requirements for DER communications various features will be discussed, such as the security of data-in-motion, the authentication of clients and services, and the corresponding impact to DER interoperability.

1) Device Registration: Device registration is the basis of creating an identity for a device that can be verified for communications between the DER and utility, and thus is critical for DER security.

If the DER registration is not protected adequately, a rogue device may be able to act as a valid inverter and send incorrect data, alarms, and other information within the control

system. Even more worrisome, this breach could potentially be used as a pivot point into an ADMS control network. Alternatively, if registrations of valid devices are blocked due to incorrect implementation or denial-of-service conditions, numerous inverters may be unable to communicate and grid-support functions could be severely impacted. Because of these potential impacts, protecting the identity management of DERs is critical to ensure interoperability in a secure manner, with integrity and authentication being the most important properties. There is also minimal impact to grid functions for adding security to device registration information as this is not time sensitive and can be performed during installation or maintenance of equipment.

2) Group Management: DER group management is closely related to device registration, but is more concerned with configuration and maintenance of a group of DERs. This is a command setting that is sent to each inverter so that they are associated with certain control groups (can be more than one). Integrity of these commands to ensure group settings are not modified is the most important security attribute, but availability is also important when reconfiguration is required. Confidentiality is generally of lower importance in this instance, but can help limit the amount of openly available information on system structure. As it is assumed changes to group management are modified infrequently, the associated messages are not considered time sensitive and so additional integrity measures should not impact grid performance.

3) Connect / Disconnect: At various times the utility may need to connect or disconnect inverters from the grid. This is a command that is required for safety and maintenance purposes, yet will likely be sent rarely. Therefore, authentication, integrity, and non-repudiation of the command is critical to ensure it came from a valid source and was not modified in transit. When a DER is disconnected it will affect both profitability (less time producing power) and ability to support grid reliability. If such a command only affects a single DER, then the impact is minimal to the grid as a whole due to the limited capacity of DERs. On the other hand, the system impact could be significant if a whole group or large enough amount of DERs are affected. Also, local grid conditions on a distribution feeder may be affected more than the system as a whole, as seen in the example in Section III where the impact of the command being sent when it is not desired is briefly examined.

4) Scheduling Power Values and Modes: A DER can support a variety of grid-support functions. For instance, a smart inverter can be configured to a certain power mode, possibly as part of a control group. The common power modes include Low/High Voltage Ride Through, Low/High Frequency Ride Through, Volt-Var Control, Fixed Power Factor Control, Volt-Watt Control, and Frequency-Watt Control [14].

Each of these modes has control settings and values that must be set. When configuring the inverter, the relevant power values need to be configured as well. For example, with Volt-Var control the control points that define the Volt-Var curve must be defined. There is potential impact from incorrect settings, so authentication and integrity of these commands are very important. Moreover, the impact of adding security to this specific communication is negligible for the most part. Some additional latency could potentially impact the performance of the ADMS if an ADMS updates control points based on system conditions, although such impact should be relatively small. This is examined in closer detail in Section III for the case of Volt-Var shifting as developed in [19].

5) Operational Status: An inverter needs to be able to report status, as this information is important for awareness into the health of the grid. If maintenance of an inverter is required, this is one mechanism by which an operator is made aware of the issue. Pieces of information included in operational status include information such as Operational State, Connection Status, Alarm Status, and Energy Storage Capacity [14].

This information may inform response actions, so it must be passed along intact. If used in operational planning and response, this information must be available. The confidentiality of this information is not generally as important, but it may impart knowledge of grid status and operations to an attacker. Note that a small delay on the order of seconds will not severely impact response actions and the consequences of false alarms and incorrect state information may be severe, including but not limited to a loss of trust in these reporting mechanisms.

6) Monitoring Data: There are several data measurements that are useful to record and use in advanced grid management functions. These include measuring Real Power, Reactive Power, Frequency, Voltage, Current, Power Factor, DC Voltage, DC Current, and DC Power [14].

These measurements may be used for better management of a distribution system, so it is critical that they are correct. Incorrect readings and information may lead to degradation of service and serious effects to the grid, especially if an ADMS uses this information to inform system control. Furthermore, the availability of these measurements is critical for adequate situational awareness into grid conditions. Care should be taken to preserve the integrity and availability of this information, yet extensive delays in reporting need to also be minimized to ensure adequate response.

7) Nameplate Ratings: Nameplate ratings are constant ratings of inverter capabilities as given by a manufacturer, while adjusted settings are corresponding values that are modified over time to reflect aging and reduced performance of the inverter over its lifespan.

These ratings can be reported for knowledge and awareness of the limits of the inverter capacity. The impact of adding security to these communications is minimal as these updates are not time-sensitive and are infrequent. Note that in general, confidentiality of the nameplate ratings is not important as typically it is publicly available.

8) Alarms: As part of determining operational status and providing situational awareness, an inverter can determine if grid conditions have passed alarm thresholds such as Over/Under Current, Over/Under Voltage, Over/Under Fre-

quency, Voltage Imbalance, Current Imbalance, Low Input Power, Phase Rotation, and more [14].

When an alarm condition is measured, the inverter reports the alarm back to the utility. When the issue has been solved, the utility will send a "normal" command back to the inverter to reset its alarm status. Some of the alarms will be evident locally without any access to the inverter (i.e., breakers opening in protection systems). Therefore, confidentiality is not as important as integrity and availability for this type of message. Integrity and availability are both critical, as false alarms and alarms that do not reach the utility could both have a severe impact on grid operations and response actions. It is important that these alarms reach the utility quickly to aid in determining the source of problems in the BPS, but a delay on the order of seconds should not severely impact response ability [1].

9) Maintenance: Another type of communication that does not fall into any of the previous categories but is important to consider is DER maintenance. Over its lifecycle, an inverter may require reconfiguration and updates to its functionality and firmware. As this maintenance can fundamentally change the functionality of a DER, it is critical to ensure that such updates are legitimate through appropriate authentication and integrity mechanisms, often by checking signatures of updated firmware to ensure that no illegitimate modifications to the code have occurred. The impact to grid-support functions from applying these techniques is minimal as maintenance is out-of-band of grid control operations. However, care should be taken to minimize the operational costs associated with securely managing the infrastructure required while also minimizing risk of malicious maintenance and update events.

C. DER Cybersecurity

As highlighted in Section II-A, the security principles of confidentiality, integrity, availability, non-repudiation, and authentication are important to consider for protecting DER communications. The various logical interfaces, as summarized in EPRI's DER Logical Reference Model, pictured in Fig. 1, capture critical functional requirements of DERs. As discussed in the previous section, these functional requirements inform DER communication needs and types when integrating DERs into the overall system, and security must be addressed in a holistic manner to minimize cybersecurity risk.

In this section, some example security mechanisms are discussed to demonstrate various measures by which the security principles of Section II-A can be preserved. The impact to a distribution system of applying these controls to DER is also discussed. Note that each security measure may address a different security principle, so a combination of them is ideal. If possible, the use of several to create defense-in-depth is desired.

1) Role-Based Access Control: Both DER and the networking infrastructure they utilize (such as network gateways) should have role-based access control (RBAC). In this way, permissions are split into specific roles that have to be granted explicitly to users. Generally, these include roles such as administrators, engineers, and various other types of users, each with specific read/write/execute permissions that are tailored to their specific role. Another form of access control that may be used is identity-based access control, where authentication and permissions are done on an individual basis based on identity. As this security measure is for access to the DER itself, it should not affect communications for grid support and thus will have minimal impact on grid performance.

2) Port Security: Network communications are done on logical ports for each device. Security best practice is to lock down and secure all unused ports to ensure that unauthorized access or backdoors cannot communicate. This is done through a firewall that blocks all ports except those explicitly whitelisted. The processing overhead of this comes from the checks on whether a given message is for a port that is allowed to communicate, which takes very little time and so should have negligible impact on grid services. The main overhead in implementing this security measure is in maintaining and updating rules for port security as needed, but such maintenance should be minimal as DER communications should only use a couple standard ports that do not change, such as port 502 for Modbus or port 20000 for DNP3.

3) Strong Passwords / Passphrases: The use of passwords is a common mechanism for login authentication, and best practice when using them is to require a password of at least 12 characters of sufficient complexity. Even better is a sufficiently long passphrase, as this is easier to remember and is often complex enough for adequate security. When implementing a password mechanism for login, it is best to require that upon installation any default passwords must be reset. Again, as this is part of the login process to access a device, it will have minimal impact on a DER. For further protection, use Multi-Factor Authentication as described next.

4) Multi-Factor Authentication: The security best practice for login authentication is to use Multi-Factor Authentication. In other words, it is best to use a mechanism that requires at least two of the following: something you know (password), something you are (biometrics), or something you have (token). This has become quite common in recent years, and as it is part of the login process to access a device it would have minimal impact on DER communications. However, additional overhead and cost would be required to setup and maintain the infrastructure required for Multi-Factor Authentication.

5) Least Privilege: Users should have the least amount of access they require. This ensures that a single user can only cause minimal damage to the distribution system. This is an administrative process, so it has no impact on the operation of a power system.

6) Intrusion Detection Systems / Intrusion Prevention Systems: Having the ability to detect and/or prevent actions from degrading grid performance, such as preventing an undesired command to disconnect generation, comes through inspection of traffic and system state to determine if communication is legitimate or not. This can be done through an intrusion detection system (IDS) using context-based or signature-based detection to find and potentially block anomalies. This requires some additional processing time, which may impact the level

of latency in a network. However, in general an IDS can be designed to have minimal impact on network latency and thus should have minimal impact on grid performance.

7) Selective Encryption: Various pieces of protocols contain information that may be good to protect through encryption, such as various parts of protocol headers, register numbers, and other information that could be used to craft malicious packets. This can be done by encrypting those pieces of information or entire packets through an encryption algorithm such as the Advanced Encryption Standard. This additional encryption will add processing delays which might impact DER communications and grid performance, although such impact is expected to be minimal.

8) Cryptographic Integrity: Encryption helps preserve confidentiality but does not ensure that a message has not been altered. Ensuring integrity of messages is done through mechanisms such as Message Authentication Codes that use cryptographic checks to ensure that data has not been modified. These checks go further than the use of error correction codes by thwarting the manipulation of a message followed by a recalculation of the error correction codes to match the maliciously modified messages. This is critical for preserving integrity of information and will come with processing overhead, but in the context of DER communications should have minimal impact to grid performance.

9) In-Line Blocking Devices: In-line blocking devices can be used in networks to permit traffic only of certain types or in certain directions only, such with the use of data diodes or hardware firewalls. These add some small delay to communication times, but the impact should be minimal to grid services.

10) Logging: Logs should always be captured of actions and traffic, as this aids in forensic analysis and can be used by intrusion detection systems or by operators to detect anomalies and changes in system state. Processing overhead for logging is minimal, but a certain amount of memory will need to be set aside to store logs for a predetermined amount of time.

These are just a few security measures that are good to keep in mind when securing distributed assets such as DER systems. Overall, they will have some impact on the latency of the required communications, but that impact should be on the order of milliseconds. The following section will further examine how additional latency impacts the performance of a distribution grid in maintaining system voltage and discuss why small amounts of latency in DER communications are not expected in general to have a large impact on grid performance.

III. Analyzing System and Interoperability Impact

To demonstrate impact of additional communication and processing times associated with applying security measures to DER communications, this section shows performance of DER supplying voltage support in a simulation of a distribution feeder. Three additional cases are shown where a disconnect signal is sent to inverters to demonstrate the impact of an unexpected loss of generation capacity in this distribution feeder. In this section, first the model used for this analysis is described and then the results of simulating various communication delays and configurations are shown and discussed.

A. DER System Model

To demonstrate impact in a realistic distribution system using communication-assisted grid support, a 15-bus reduced-order model of a rural distribution feeder from the state of New Mexico is utilized, as was developed in [17]. This model was chosen due to its relatively high amount of photovoltaic (PV) penetration, as it has 11.2 MW of PV generation capacity from three inverters and 2.6 MW of peak load. Also, as a reduced-order model of a real distribution feeder, this model is a good representation of distribution systems with high amounts of PV generation. This model is shown in Fig. 2.

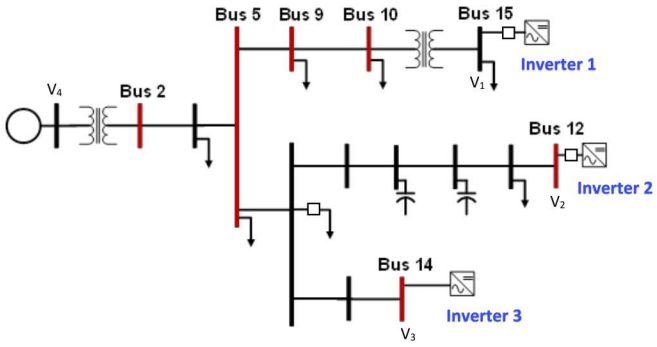

Fig. 2. Model of Distribution System with PV, adapted from [17]

The three inverters in this model provide voltage support through Volt-Var control, with the initial settings for this control shown in Fig. 3. The ratings of the three inverters represented in this feeder are shown in Table I. Note that the various voltage and power ratings represent various sizes and types of DER generation sources. Also, note that the Volt-Var curves are set so that the max reactive power supplied by each inverter is 25% of its overall rated capacity, while its real power setting, P, is set and maintained at 50% of the rated power for each inverter.

TABLE I
Inverter Specifications

Generation	Rated Power	Nominal Voltage
Inverter 1	258 KVA	480 V
Inverter 2	10 MVA	12,470 V
Inverter 3	1 MVA	12,470 V

A modification was made to this reduced-order model from its original configuration to better demonstrate variation and impact to the feeder regarding aspects of the DER communications. This is done by adding an additional 1.8 MW load, which brings the overall peak load in this system to 4.4 MW. This load is configured to connect to the distribution

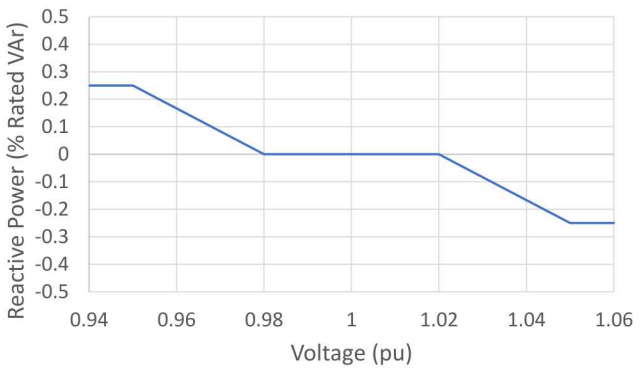

Fig. 3. Volt-Var Curve for Inverters to Support System Voltage by Injecting the Appropriate Amount of Reactive Power Dependent on Local Voltage

system two minutes into a simulation to represent a sudden large change in system load. This creates an immediate drop in voltage across the distribution feeder that each inverter responds to by injecting reactive power according to its Volt-Var settings. Note that due to the high amount of generation capacity in this model, excursions outside ANSI Range A (0.95 pu - 1.05 pu), as specified in [18], do not occur in these simulations and so only the amount of deviation from nominal voltage is used as a measure of system performance in these results.

B. Hierarchical Volt-Var Control

An ADMS is represented in this model by incorporating a Volt-Var shifting algorithm to update the Volt-Var curve settings at each DER to better minimize voltage deviations across the distribution feeder as a whole. This algorithm was developed in [19], and is used here to represent the impact of communication assisted grid support. For this ADMS implementation, root mean square (RMS) phase-to-phase voltage measurements are taken in four locations across the feeder. Specifically, these voltage measurements are taken locally at the three inverters and at the substation that connects the distribution feeder to the transmission grid, as shown in Fig. 2. The Volt-Var shifts in the hierarchical controller are configured to shift the Volt-Var curve to the left or right by 0.001 pu if the minimum or maximum system voltages fall outside the range of 0.99 pu to 1.01 pu, or 1% of the nominal system voltage. These Volt-Var updates are calculated once every five seconds and then communicated to the three inverters. Further discussion of the various settings, configurations, and concerns for this hierarchical Volt-Var control algorithm is contained in [19], and further discussion on communication requirements for advanced inverter control and the impact of various aspects of a communication channel can be found in [20].

Communication delays are represented in this model by delaying the ADMS voltage measurements and Volt-Var setting updates. This delay, which is called t_d, is for one-way communication between the ADMS and an inverter, or vice versa. That is, for a certain t_d, the voltage measurements are delayed by t_d and the Volt-Var updates are also delayed by t_d.

C. Impact to Grid Performance

To calculate the system performance in minimizing voltage deviation, the system voltages used by the ADMS are recorded to demonstrate varying voltage levels across the feeder over a span of five minutes, which is the time used for all the simulated cases. The overall, average system voltage V_{sys} is calculated as shown in (1) as a way to represent performance across the distribution feeder as a whole, whereas $\{V_1, V_2, V_3, V_4\}$ demonstrate performance in their respective locations within the feeder. Recall that $\{V_1, V_2, V_3, V_4\}$ are the per-unit RMS phase-to-phase voltages measured at the inverters and at the substation, as shown in Fig. 2.

$$V_{sys} = (\frac{1}{4}) \times (V_1 + V_2 + V_3 + V_4) \tag{1}$$

Table II shows the average voltage deviations over a five minute simulation for each voltage measurement and the overall system voltage across the feeder for a range of scenarios. These cases show various levels of communication delays due to additional processing overhead, such as by applying additional security mechanisms as discussed in Section II-C, as well as several cases where inverters are disabled to show potential impact from loss of generation capacity, such as in the case where a malicious command is sent to disconnect inverters.

As shown in Table II and in Fig. 5, additional amounts of communication delay will gradually impact the ability to minimize deviations in system voltage across the distribution feeder. This impact to performance will occur fairly evenly across the system, as seen by the relative degradation in V_1-V_4.

In cases where individual inverters are disconnected, the voltage local to the disconnected generation sources will be impacted more severely, as shown by the relatively higher amount of voltage deviation from nominal local to the inverters that have been disconnected, as seen in Table II. In all cases, the voltage levels at the substation are minimally affected, solely because of its far greater capacity to maintain nominal voltage levels.

Several features of these results are of special interest. First, note in Table II and in Fig. 4 the advantage of adding communication-assisted control to minimize voltage deviations across the feeder. This is seen in the performance of the Volt-Var control alone compared to when it includes shifting of the Volt-Var curve. It is for these reasons that communication-assisted grid-support functions are useful in the first place.

Additionally, since the Volt-Var shifting algorithm is performed at a much slower rate than the internal, local controls of the inverter, the impact of communication delay is minimal, as seen in Fig. 5 and Fig. 6. In other words, while the amount of voltage deviation across the feeder does increase slightly as communication latency increases, the inverter is still able

TABLE II
AVERAGE ABSOLUTE PER-UNIT VOLTAGE DEVIATION FROM NOMINAL

Scenario	V_1	V_2	V_3	V_4	V_{sys}
Volt-Var	0.0110	0.0116	0.0118	0.0005	0.0087
Volt-Var with V-V Shift	0.0092	0.0097	0.0101	0.0004	0.0074
Volt-Var with V-V Shift and $t_d = 0.1s$	0.0092	0.0097	0.0101	0.0004	0.0074
Volt-Var with V-V Shift and $t_d = 1s$	0.0092	0.0098	0.0101	0.0004	0.0074
Volt-Var with V-V Shift and $t_d = 5s$	0.0096	0.0101	0.0104	0.0004	0.0076
Volt-Var with V-V Shift and $t_d = 10s$	0.0102	0.0107	0.0110	0.0005	0.0081
Volt-Var with V-V Shift and $t_d = 15s$	0.0106	0.0111	0.0114	0.0005	0.0084
Volt-Var with V-V Shift and $t_d = 20s$	0.0108	0.0114	0.0116	0.0005	0.0086
Volt-Var with V-V Shift and $t_d = 25s$	0.0109	0.0115	0.0118	0.0005	0.0087
Volt-Var with V-V Shift, Inverter 1 disconnected	0.0113	0.0096	0.0100	0.0004	0.0076
Volt-Var with V-V Shift, Inverter 2 disconnected	0.0127	0.0139	0.0136	0.0006	0.0097
Volt-Var with V-V Shift, Inverter 1 & 2 disconnected	0.0199	0.0142	0.0139	0.0006	0.0118

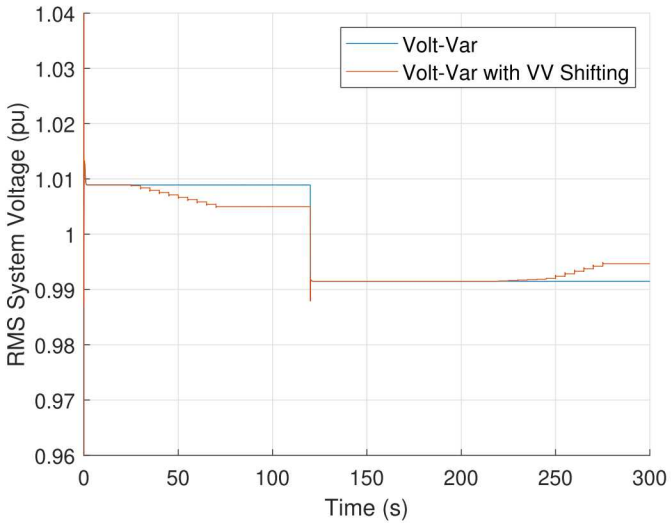

Fig. 4. Average System Voltage With and Without Communication Assisted Volt-Var Shifting

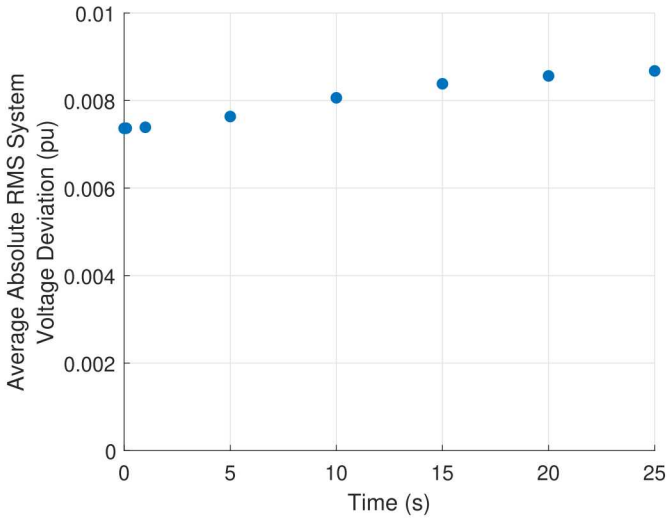

Fig. 5. Average Absolute System Voltage Deviation from Nominal for Various Amounts of Communication Delays

to support system voltage and is merely delayed in updating its settings.

Furthermore, as seen in Table II and in Fig. 7, the impact of disabling specific inverters depends on several factors, such as the inverter capacity, the amount of DER penetration, and other characteristics of the distribution system. For instance, disconnecting inverter 1 has minimal impact on overall system voltage due its relatively small capacity, whereas disconnecting inverter 2 has a larger impact to the system. Furthermore, when disconnecting inverter 1 and/or 2, the effects to voltage is mainly local, as seen in higher amounts of voltage deviations in V_1 & V_2 relative to the rest of the distribution system.

IV. CONCLUSION

As DER penetration increases in the power grid, new control functionality is required to maintain grid performance. Adding communications to ADMS improves situational awareness of grid conditions and the ability to support grid operations, but also creates additional risk of degradation to grid performance from cyber attack. This is especially true in cases where multiple DERs are affected, which is a possibility in the environment of the Smart Grid and networked control systems. To ensure that in the future the expected higher penetration levels of DERs in the power grid assist in maintaining system performance and do not end up degrading grid reliability, it is highly recommended that DERs include common security mechanisms to ensure they can be operated securely and the potential impact of losing large amounts of distributed generation capacity is minimized. To address these concerns, the security implications of the required DER communications for grid-support have been examined in this paper and analysis provided that shows that additional communication latency

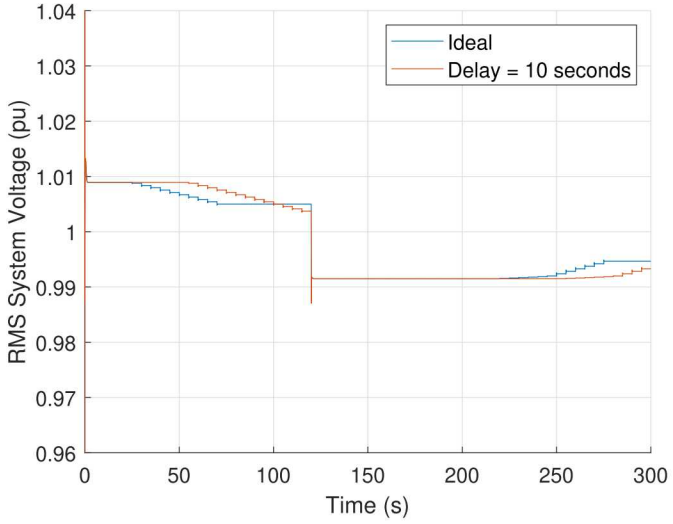

Fig. 6. Average System Voltage for Volt-Var Control with Volt-Var Shifting with Ideal and Delayed Communication Times

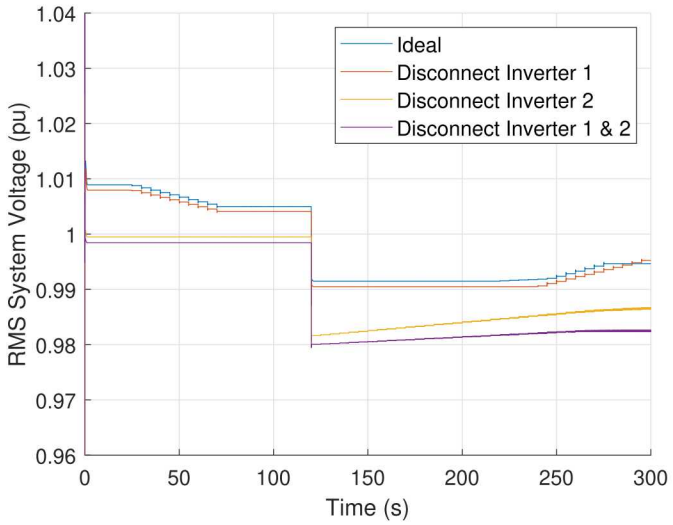

Fig. 7. Average System Voltage when Inverters are Disconnected from the Distribution Feeder

from these security measures should not severely impact grid performance. This information helps in understanding what is required to securely implement communication-assisted grid-support functions. Future work could extend this analysis to other modes of operation for DER and the communications associated with them, such as DER support of system frequency through grid-support functions such as Frequency-Watt Control. Further analysis into aspects of the distribution control with additional security measures and more extensive analysis on cyber aspects of various attack classes and the corresponding types of impacts to grid reliability that could be expected from failing to secure DERs is warranted.

ACKNOWLEDGMENT

The authors would like to thank Adam Summers and Jay Johnson for their assistance in obtaining and using the simulation model in Section III, as well as the rest of the Module OT team and the anonymous reviewers for their valuable comments and advice.

REFERENCES

[1] "Modern Distribution Grid Decision Guide Volume III," U.S. Department of Energy Office of Electricity Delivery & Energy Reliability, Tech. Rep., Jun. 2017.

[2] P. Fairley, "How Rooftop Solar Can Stabilize the Grid," Jan. 2015. [Online]. Available: https://spectrum.ieee.org/green-tech/solar/how-rooftop-solar-can-stabilize-the-grid

[3] ——, "800,000 Microinverters Remotely Retrofitted on Oahu - In One Day," Feb. 2015. [Online]. Available: https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

[4] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS Industrial Control Systems, Mar. 2016.

[5] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the Modbus protocols," *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, Dec. 2008.

[6] "Modbus Application Protocol Specification, V1.1b3," Apr. 2012.

[7] "Modbus/TCP Security Protocol Specification," Jul. 2018.

[8] "IEEE 1815-2012 - IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," Oct. 2012. [Online]. Available: https://standards.ieee.org/standard/1815-2012.html

[9] "IEEE 1547-2018 - IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces." [Online]. Available: https://standards.ieee.org/standard/1547-2018.html

[10] "Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology Interagency Report, Tech. Rep., Sep. 2014.

[11] F. Cleveland and A. Lee, "Cyber Security for DER Systems,," Electric Power Research Institute, Tech. Rep., Jul. 2013.

[12] "California Rule 21 Interconnection." [Online]. Available: http://www.cpuc.ca.gov/Rule21/

[13] W. Stallings, B. Lawrie, M. D. Bauer, and A. K. Bhattacharjee, *Computer Security: Principles and Practice*. Pearson Education, 2012.

[14] "Common Smart Inverter Profile (CSIP), Version 2.1," SunSpec Alliance, Tech. Rep., Mar. 2018. [Online]. Available: https://sunspec.org/download/

[15] "SunSpec Information Model Specification," SunSpec Alliance, Tech. Rep., Apr. 2015. [Online]. Available: https://sunspec.org/download/

[16] "IEEE 2030.5-2018 - IEEE Standard for Smart Energy Profile Application Protocol," Dec. 2018. [Online]. Available: https://standards.ieee.org/standard/2030_5-2018.html

[17] J. Johnson, A. Summers, R. Darbali, J. Hernandez-Alvidrez, J. Quiroz, D. Arnold, and J. Anandan, "Distribution Voltage Regulation using Extremum Seeking Control with Power Hardware-in-the-Loop," *IEEE Journal of Photovoltaics*, vol. 8, no. 6, pp. 1824–1832, Oct. 2018.

[18] "ANSI C84.1-2016," Oct. 2016. [Online]. Available: https://www.nema.org/Standards/Pages/American-National-Standard-for-Electric-Power-Systems-and-Equipment-Voltage-Ratings.aspx

[19] J. E. Quiroz, M. J. Reno, O. Lavrova, and R. H. Byrne, "Communication Requirements for Hierarchical Control of Volt-VAr Function for Steady-State Voltage," in *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Apr. 2017.

[20] M. J. Reno, J. E. Quiroz, O. Lavrova, and R. H. Byrne, "Evaluation of Communication Requirements for Voltage Regulation Control with Advanced Inverters," Sep. 2016.