Exploring Emerging Cybersecurity Risks from Network-Connected DER Devices

D. Jonathan Sebastian
School of Electrical Engineering and Computer Science
Washington State University, Pullman, WA, USA
d.sebastiancardenas@wsu.edu

Adam Hahn
School of Electrical Engineering and Computer Science
Washington State University, Pullman, WA, USA
ahahn@eecs.wsu.edu

Abstract—**Future growth in Distributed Energy Resources (DERs) present growing cybersecurity risks as these devices acquire increased networking and remote control capabilities. In this work the cyber-physical risks of consumer-grade DER are described. The work focuses on studying those DER devices that are network enabled and could be exploited by remote entities. Since attacks can range in both the access mechanism and the outcome objective a set of metrics are proposed to classify the cyber-physical attributes of the intrusion, these metrics can later be applied to create a inclusive model that can be used to measure the cybersecurity risks in terms of typical power-system quantities in real-world systems.**

***Index Terms*— Cyber-physical Systems (CPS), Distributed Energy Resources (DER), cybersecurity, smart inverters.**

I. INTRODUCTION

Distributed energy resources are any set of generation units that are not part of the bulk energy system, and as such could be owned/operated by the utility/private operators or by individual end users [1]. Due to their relatively small size these systems are often connected at the distribution level and are modeled by aggregating the power generation into a single large generator.

Although DER generation agglomerates many technologies Photovoltaic Systems (PV) have received considerable attention due to their growing installed capacity and their unique generation characteristics. PV DER systems are notorious for having great variability, that in many cases is difficult to accurately predict, this has led to significant power swings in high penetration areas [2].

These power swings are often caused by natural events such as cloud transients, sunrise/sunset periods and are normally handled by adjusting the bulk generation output. However, if these events are coordinated to inflict damage by an external agent the system operation could be jeopardized.

To help raise awareness the National Electric Sector Cybersecurity Organization Resource (NESCOR) has enlisted a series of scenarios that could result in power system failures when DER devices are compromised [3]. These scenarios could worsen when the *grid support functions* proposed by the *Smart Inverter Working Group* (SIWG) go into effect. These *"grid supporting"* functions are designed to increase the efficiency and resilience of the grid by using Information Communication Technologies (ICTs), but could also create a vulnerable point if those devices are compromised.

The remote control and monitoring functionalities of DER devices is often encompassed under the Cyber Physical Systems (CPS) domain. Nevertheless, due to the growing market of Internet of Things (IoT) capable devices, manufacturers have created DER inverters that share electrical, ICT and IoT hardware, functionalities, mechanisms and unfortunately vulnerabilities.

These additional features include remote measurement of electrical variables and data storage mechanisms that are used to produce analytics [4]. These features are often implemented by applying the IoT reference model [5], [6]and adapting its layers to fit the DER infrastructure (see Fig. 1)

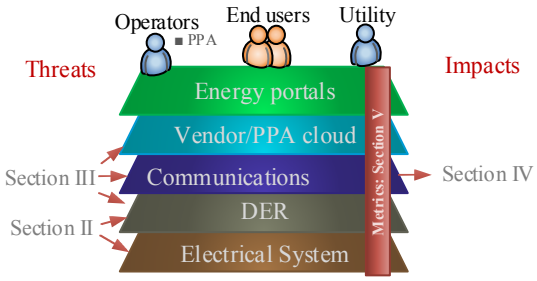

Fig. 1. DER conceptual architecture based on the IoT model.

In some cases, these extended functionalities include web-based or application-based configuration managers [7] that even though are intended to work inside Personal Area Networks (PAN) could have vulnerabilities that make them susceptible to Wide Area Network(WAN) attacks.

While the importance to DER cybersecurity has been identified by industry and government experts [8] [9], specific requirements for consumer-grade DER (autonomous) devices have not been created. Furthermore, IoT security requirements remain ambiguous and not fully defined [10] and DER devices are developed with insufficient security capabilities [11]. In the next sections an overview of vulnerabilities associated with smart inverters and how they can be exploited to cause damage to the grid will be presented.

II. SMART INVERTER FUNCTIONS

DER devices can be implemented by using a Digital Signal Processor (DSP) —*the controller*, in conjunction with adequate power electronics circuitry [12]. However, with the introduction of smart inverters other pieces of hardware must be introduced to satisfy the communication requirements.

To satisfy market requirements, Microcontrollers (MCUs) with network communication capabilities have been introduced. These devices enable the device to exchange data with the outside world but can also serve as the entry point for large-scale attacks [13]. The typical architecture of a smart DER device is shown in Fig. 2.

From Fig. 2 is possible to observe the linkage between the cyber world and the physical grid. Thru this network interface

the device becomes visible to the outside world, which includes the customer, the vendor, the third-party operator (PPA) and finally the utility company (see Fig. 1 and Fig. 3).

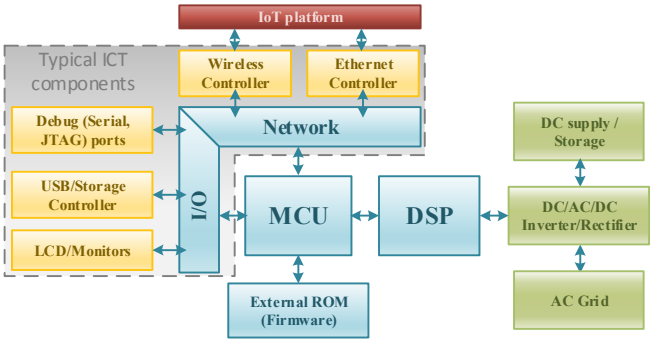

Fig. 2. Typical Smart Inverter Architecture.

Each of these access mechanisms increases the attack surface to which the DER device is exposed, creating the risk for abusing the grid support functions. In order to model these cyber risks a multi-layer approach will be described in the next sections.

Current smart DER functionalities are mostly unstandardized and depend more on market factors than technical functionalities. This has resulted in multiple vendor-specific functions that use custom settings and operational techniques and therefore are incompatible with other vendor implementations [14]. In order to address these problems SIWG has set a plan to standardize a set of common functions that must be supported by DER devices.

This standardization plan, among other things seeks to create a platform that provides grid support, enables data exchange and communication by using open standardized protocols. However due to the rapid market growth that the industry is experiencing a staggered approach was elected to minimize delays in deployment due to regulatory burdens.

During this staggered plan three phases are currently considered, each addressing immediate, mid-term and long term goals. The first phase has been in development since 2011, and is under implementation by several standardization bodies. Among many others IEEE 1547a, UL 1741 SA, IEC 61850 and California Rule 21 are in the process of being published or setting the regulatory provisions, with most requirements expected to go into full effect at the end of 2017 [15].

According to SIWG the first phase geared towards addressing critical autonomous functions, phase 2 is designed to address the communication capabilities of the devices, while advanced DER functions are to be introduced in phase 3. In the next sections a brief introduction to each phase will be given.

A. *Phase 1.*

Phase 1 goal is to standardize basic functions in smart inverters, compliant with IEEE 1547 2014. It reflects the necessity of providing basic grid support functions under transients, the core functions are:

- ***Have frequency ride-through settings:*** Enables the DER device to continue to operate when there are frequency oscillations
- ***Have voltage ride-through settings***: Enables the DER device to continue to operate when there are frequency oscillations.
- ***DER devices must support momentary de-energization***: a mode where the DER must cease to energize the area but must not trip. (*hot standby*)
- ***Support for adjusting excursion settings:*** settings to support DER re-energization following an excursion event.
- ***Support for adjusting dynamic Volt-Var Operation***: Change Power factor according to voltage levels;
- ***Support for adjusting ramp rates***: Setting to configure the power ramp rates $\Delta P/\Delta t$
- ***Support for adjusting fixed Power Factor***: Fixed power factor settings
- ***Inherent functions***: core functions, e.g. defining the maximum equipment capabilities (P, Q, ramping limits).

B. *Phase 2.*

This phase addresses the communication requirements that will enable utilities to communicate with DER devices in order to remotely configure the grid support functions. Current consensus is to use IEEE 2030.5 as the method for transmitting application messages [16]. This phase is under development/implementation and will also introduce additional grid support functions.

Current regulations on stage 2 consider the need for a secure communications channel between the utility and DER device, they are focused on creating a mechanism for remote inverter management. However, they don't regulate the mechanisms through which end users or third party operators gain access into the device, leaving the details to device vendors.

These unregulated access mechanisms could cause problems in the near future and as such regulators have suggested that requirements might dynamically change over the next five years [16].

C. *Phase 3.*

Phase 3 is under development and is expected to take 5-10 years before it goes into effect. It's expected to provide real-time scheduling control and capacity planning, some of the expected functionalities are:

- Manage, limit, and/or curtail real power to avoid or mitigate distribution congestion, equipment overloads, or power quality issues.
- Ability to schedule real power, provide "available" reactive power for quality/reliability support on a feeder.
- Provide reactive power for transmission/voltage support near a substation
- Provide operational (spinning and non-spinning) real power reserves (normal operations and microgrids)
- Provide AGC frequency support.
- Provide autonomous frequency support (Frequency-Watt).
- Compensate for renewable energy (rapid load) fluctuations.
- Reduce peak loads (demand response) – Create (planned) islanded microgrids – Provide black start capabilities

III. Cyber Security of DER Devices

A multilayer DER model is proposed to represent the different mechanisms through which an attacker can gain access into a device by allowing to evaluate multiple entry points simultaneously, with each entry point having its own attack model.

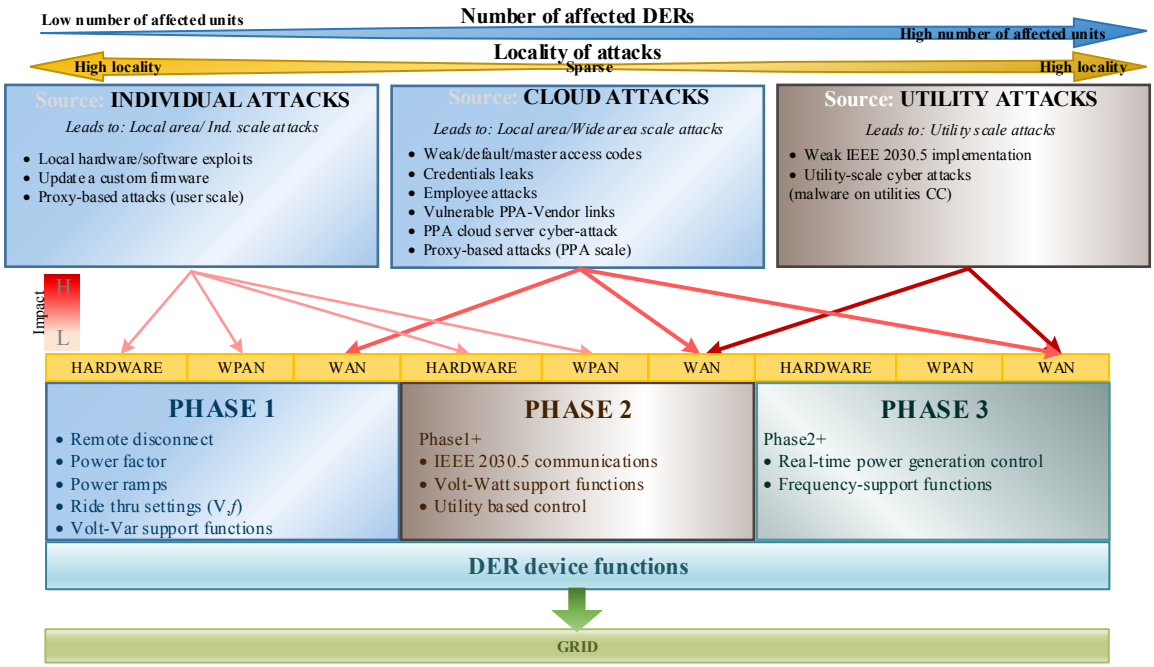

Fig. 3. Smart Inverter connectivity model.

The information outputted by the models can later be used to determine the quantity of compromised units and the effects on the grid. The next list illustrates how different attack scenarios can create effects at different power system scales:

- ***Effects visible in a single unit:*** Compromising one unit by targeting the hardware/software layers
- ***Effects visible in a neighborhood:*** Compromising a set of localized units that are under certain range with respect the attacker position (by exploiting local communication links).
- ***Effects visible across multiple utilities / distribution areas:*** Compromising a set of devices that share the same vendor, PPA connectivity medium, by exploiting a software vulnerability (network attack)
- ***Effects visible in a distribution area:*** Compromising a set of devices that are controllable by the utility.
- ***Effects visible on multiple regions:*** Compromising a set of devices that share the same software, firmware, hardware configurations, by exploiting a common vulnerability (IoT-based network attack)

An introduction of how these attacks could be used by an attacker will be introduced on the following sections.

A. Hardware-based attacks / Individual device attacks

DER hardware attacks can range from physical tampering to firmware replacement. Physical tampering includes adding or removing connections that enable hidden features such as debugging capabilities. They can also be used to produce false measurement readings or to bypass a security function. Firmware attacks on the other hand use the software layer to access the device functionality. Firmware attacks are considered difficult to perform but can help an attacker to better analyze the device architecture.

Although hardware-based attacks are considered as individual attacks, they can be used to discover generic vulnerabilities that are applicable to other devices that share the same hardware/software combinations. For example, if an attacker is able to find a buffer overflow vulnerability in the HTTP server of a particular device, it is likely that that vulnerability is applicable to all devices that have the same or lower HTTP server version (this includes same make/model combinations, but could also work across different vendors).

Although software vulnerabilities have received widespread coverage in recent years, and some DER vendors have implemented industry accepted security mechanisms there are secondary means through which an attacker might gain device control. Current practices tend to protect the software running inside the MCU, however peripherical controllers also run custom firmware's that might not comply with the power grid security standards [17].

These insecure controllers could be used by attackers to compromise the device, and could in theory go undetected from the main system. Depending on the compromised controller capabilities functions such as remote control of the device could be achievable without the main MCU being aware (i.e. firmware with embedded malware). These types of attacks can be easier to perform when manufacturers publish their firmware files publicly, but can also be performed when firmware files can be extracted from a device (see Fig. 4).

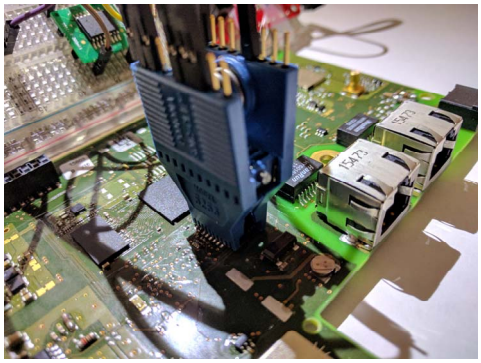

Fig. 4. Firmware dumping in a consumer-grade smart inverter

B. Local Area Attacks

Local Attacks exploit the local connectivity options typically offered on consumer grade devices. Consumer grade devices are often overlook due to their perceived low generation impact. However, currently there are about 4.5 GW of solar energy being produced in California by small scale DER units [18], with about 36.7% of them capable of communication capabilities [18].

Total solar generation numbers indicate that statewide penetration level is about 13% [19], with some areas experiencing penetration levels above 25% [18]. This can create a scenario where an attacker can compromise several units within a small geographical area.

The attacks can be carried by misusing the local network connectivity interfaces available in consumer grade devices. These can be due to default credentials on DER devices, open Wi-Fi networks to which DER devices are attached or by exploiting open ports through the wired LAN network. However, it's important to know that commercial-grade DER devices are also susceptible to attacks if the main controller system has vulnerabilities, this could result in a larger yet concentrated attack.

Although it is usually assumed that local attacks require the nearby presence of an attacker, attacks can also be performed through secondary proxy points. Proxy attacks use secondary systems to gain access to the LAN, currently PCs, routers and surveillance systems have demonstrated their ability to carry these types of attacks [20, 21].

Another vulnerable point inside DER devices are the secondary controllers responsible for network communications, these can include Bluetooth, Wi-Fi modules as well as network stacks inside the MCU firmware (see Fig. 1). In [17] the authors describe an attack that be carried inside the firmware of the Wi-Fi interface without the main MCU being aware, this could in theory lead to Man in the Middle (MiM) attacks or to command injection.

Furthermore, in [22] the authors demonstrate the proof of concept of a self-replicating worm through a Zig Bee based controller. That article exposes that when a density threshold of vulnerable devices is reached a local attack can transition into wide area attack, capable of infecting large cities.

These secondary controller attacks depend on attacking firmware's that are independent from the main MCU firmware, and are usually shared with millions of other devices [23]. These firmware's can be obtained by performing hardware attacks or by downloading the firmware's from the vendor portals [24].

C. Network/cloud connectivity attacks

Although in the near future utilities are expected to use secure communications channels (as outlined in IEEE 2030.5) device vendors and PPA currently have remote access to devices through Internet-based links. These Internet-based communications are based on the IoT connectivity model and could be the target of attackers (see Fig. 4).

The IoT technologies are intended to provide remote monitoring/control capabilities to end users [6], however they expose the DER device to vulnerabilities of IT infrastructure. The monitoring capabilities are designed to improve overall usability of the product and offer the user the capability of monitoring their power output, with some models specifically supporting remote parameter control.

This remote parameter control options, could be used by attackers to cause widespread disturbances. The number of compromised systems is likely to be dependent on specific model/vendor combinations that share the same vulnerability and access mechanisms.

One core layer of the IoT model is the data abstraction layer that provides a bridge between the data being produced and the application responsible for accessing it. This layer is often referred as the *cloud* and enables multiple users to access data through a common platform, the platform can have multiple end-user views that can be tailored to satisfy multiple consumer, supervision, and management needs. However, it also concentrates a large set of devices that could be controlled by an attacker, to put this in perspective, in the state of California about 550 MW are managed by three largest PPA companies [18] all of which have some sort of cloud management solution [25, 4].

Also due to the network capabilities the IoT security problems are inherited into DER devices. This is due to rapid time-to-market requirements that force vendors to use open-source software that satisfies the necessities of clients while at the same time reduces costs. Open-source software is great in many aspects, but it also enables attackers to exploit vulnerabilities that applicable to a vast number of devices.

Even if open source programs receive constant security upgrades, this updates might not be always be available to end users due to customizations done by the vendor. This can leave DER devices unprotected, particularly if those devices are not updated often (per user fault) or the product support time-frame has ended (software support is typically available for 3 years, while hardware lifespans are expected to be 10 years [26]). This could create insecure devices as attacks increase/improve while the network software ages, a clear example of non-updated vulnerabilities was observed with the *WannaCry* ransomware attack that affected windows machines in 2017.

IV. Attacks on smart inverter functions

As mentioned in the introduction, grid support functions are designed to improve the grid operations. However, if an attacker successfully compromises the communication channels then these grid-support functions could be used against the utility to cause disturbances. Based on the proposed grid-support functions described on section II a list of possible function-based attacks and outcomes is shown on Table 1.

In Table 1, the first column describes the function being attacked, the second column provides a rough estimate of DER devices that support this function (analysis based on data available at [18]). The attack scale columns describe both the ***attack source*** *— origin of the cyber-attack and its scale* and the ***attack target***— *the scale of the repercussions in the electrical grid.*

Table 1 was derived from cases and perceived risks described in [27], [28], [29] and [30] . The outcomes of the attacks assume that a varying number of DER devices that feature the same function capabilities can be compromised. The reported outcomes are intended to be descriptive in nature and appropriate quantification of the risks will require power system studies and the application of metrics discussed on section V.

TABLE I
POSSIBLE OUTCOMES OF A GRID SUPPORT FUNCTION DURING A MISCONFIGURATION ATTACK

Grid Support Function	Current Support	Source: / Target:	Attack Scale Cyber/*Electrical* scale: Individual DER Attack / *Individual DER unit*	Local Area Attacks / *Local neighborhood*	IoT-based vulnerability attack / *Distribution/transmission system*
VAR adjustment *(+) or (-)*	Most models		Higher monetary compensation	Localized higher/lower voltages values	Higher/lower than usual voltages in grid
			Higher/lower voltage	Damage to clients devices (overvoltage)	Damage to utilities devices
			PV inverter damage	Transformer damage (current reversal, overloading, accelerated aging)	Run away taps on transformers
					Capacitor bank/voltage regulators overload
MW adjustment (+) or (-)	Most models		Higher monetary compensation	Lower/higher than estimated demand	Higher/lower than usual voltages in downstream grid
			PV inverter damage	Transformer damage (overloading)	Damage to utilities devices
Freq. adjustment *(+) or (-) (Independent from system frequency)*	Some models		Short circuit due to phase differences	Localized voltage swings (local transformer)	System wide voltage swings
			PV inverter damage	PV inverter damage	Damage to utilities devices
				Local protections equipment malfunctions	WAN protective device failures
Freq. adjustment *(+) or (-) (Load incorrect frequency response curves)*	Some models		Short circuit due to phase differences	Localized voltage swings (local transformer)	System wide voltage swings
			PV inverter damage	PV inverter damage	Damage to utilities devices
				Transformer damage	WAN protective device failures
					Cascade operation of protective devices (blackout, grid separation)
Islanding Detection- Increase Sensibility	Some models		Repetitive isolation of the DER device from the grid	Limited PV output	Sudden loss of PV power
					The grid support function becomes useless.
Islanding Detection Decrease Sensibility	Some models		PV inverter damage from trying to supply load in island condition	Possibility of islanding an area during low load conditions	Possibility of multiple islands forming during low load conditions
					Resync without islanding conditions being identified

V. PROPOSED METRICS

Based on the previously discussed sections, analytical approaches must be developed to measure the impacts of the attacks. These impacts will be dependent on the amount and magnitude of the physical quantities that are being disrupted. These themselves will vary according to the number and location of compromised devices. A set of proposed metrics that can be used to measure the physical and cyber impacts are defined on Fig. 5. The appropriate descriptions to these proposed metrics are given on the next sections.

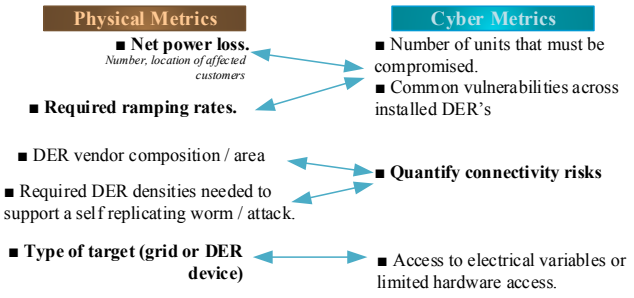

Fig. 5. Relationship between cyber-physical metrics.

1) *Power Lost Impact*

Based on the current DER functions and connectivity levels a remote disconnection event can be triggered by the attacker. The actual amount of generation that could be lost will be dependent on the amount of installed power and the percentage of units that the attacker controls. The amount of power could be further classified according to NERC's CIP-002-5.1a *impact rating* criteria [31]. This document could serve system operators as a reference for identifying critical zones. Additional sub-metrics could include number of affected DER units within an area (density), number of service areas affected (sparsity).

2) *Ramping rate Impact*

The remote disconnection of multiple DER devices could represent a significant power loss that might exceed the power ramping capabilities of the power system. Traditional PV installations are considered as a fluctuating asset, that under normal conditions exhibit a typical ramping rate of $1.1\%/min$ of their rated output [32] with small-individual units experiencing ramp rates of up to 50% in a few seconds [33]. Currently, power systems operators supply ramping rates as high as 3.7GW/Hour ($\sim 60\ MW/Min$) that are sufficient to handle the current amount of installed PV generation [34].

However, if a large amount of PV is instantaneously lost then the stability of the system could be compromised, the actual impact will be dependent on the amount of DERs controlled and the electrical system characteristics.

3) *Quantify connectivity risk*

Depending on the communication characteristics, connectivity levels, cloud services capabilities certain service areas could have a higher attack risk. In order to reduce the risk a diverse market must be encouraged, i.e. minimize the possibility that a single common vulnerability can be used to access a large set of devices.

4) *Type of outcome Impact*

Depending on the attack being developed the attacker can seek to damage the grid or cause equipment damage that would cause economic consequences to the DER owner as well as lower generation capacity in the medium-term horizon.

VI. CONCLUSION

This work provides an exploratory review of the risks of smart DER devices and identifies key metrics to evaluate the risk of these systems. It introduces the software and hardware

vulnerabilities present on current generation devices and ties them to their physical grid counterparts. Furthermore, it explores varying risk levels based on the number of devices that an attack could influence, as a severe impact may not occur unless many systems are simultaneously attacked.

Although smart inverter security is starting to improve, more standards must be created to ensure that non-utility owned DERs remain secure in non-controllable environments. Appropriate metric development is important to fully understand the cyber-physical risks. These metrics can be further improved by using detailed DER information, such as the one available in [18] and tying the information to standardized distribution and transmission test systems.

VII. ACKNOWLEDGMENTS

The authors would like to thank the DOE for their funding under project *Grid Modernization Laboratory Call (GMLC) Project GM0100* and CONACYT(Mexico)

VIII. REFERENCES

[1] NERC, "Distributed Energy Resources: Connection Modeling and Reliability Considerations," NERC Draft Report, Atlanta, GA, 2016.

[2] M. A. Eltawil and Z. Zhaoa, "Grid-connected photovoltaic power systems: Technical and potential problems—A review," Renewable and Sustainable Energy Reviews, vol. 14, no. 1, pp. 112-129, 2010.

[3] National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute, "Electric Sector Failure Scenarios and Impact Analyses," 2013.

[4] "MySolarCity portal," 2017. [Online]. Available: https://mysolarcity.com. [Accessed 08 May 2017].

[5] Cisco, "The Internet of Things Reference Model - Internet of Things World Forum," 2014.

[6] Roberto Minerva; Abyi Biru; Domenico Rotondi , "Towards a definition of the Internet of Things (IoT)," IEEE Internet Initiative , 2015.

[7] SMA, "Sunny Data Control Management Software for Sunny Beam and Sunny Boy Control," 05 March 2009. [Online]. Available: http://files.sma.de/dl/1364/SDC-TEN080642.pdf. [Accessed Oct. 2016].

[8] The Smart Grid Interoperability Panel Cyber Security Working Group, "NISTIR 7628: Guidelines for Smart Grid Cyber Security," NIST, 2010.

[9] F. Cleveland and A. Lee, "Cyber Security for DER Systems".

[10] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014.

[11] F. Bret-Mounet, "All your solar panels are belong to me," DEF CON 24, 15 Jul. 2016. [Online]. Available: https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Fred-Bret-Mounet-All-Your-Solar-Panels-Are-Belong-To-Me.pdf.

[12] Texas Instruments, "800VA Pure Sine Wave Inverter's Reference Design," Application Report, 2013.

[13] J. Qi, A. Hahn, X. Lu, J. Wang and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28-39, 2016.

[14] EPRI, "Common Functions for Smart Inverters," ELECTRIC POWER RESEARCH INSTITUTE, Palo Alto, California, 2016.

[15] S. Biybani, "Distributed Energy Resources (DER) Management with IEEE 2030.5™ Symposium," 11 Nov. 2016. [Online]. Available: http://standards.ieee.org/events/2016_der_presentations/rule21.pdf. [Accessed 25 Mar. 2017].

[16] C. S. I. I. W. Group, "IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters," 2016.

[17] Project Zero, Google, "Over The Air: Exploiting Broadcom's Wi-Fi Stack," 17 April 2017. [Online]. Available: https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html. [Accessed 20 April 2017].

[18] California Solar Statistics, "CSI Working Data Set," California Solar Initiative, 2017.

[19] Solar Energy Industries Association, "Solar Spotlight: California (Factsheet)," 04 Apr. 2017. [Online]. Available: http://www.seia.org/sites/default/files/CA%202016Q4.pdf.

[20] "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," Krebs on Security, 16 Oct. 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. [Accessed 25 Oct. 2016].

[21] D. Kushner, "The real story of stuxnet," IEEE Spectrum , pp. 48-53, March 2013.

[22] E. Ronen, C. O. A. Shamir and A.-O. Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," Cryptology ePrint Archive, Report 2016/1047, 2016.

[23] M. Kuman, "Millions of DSL modems hacked in Brazil, spread banking malware," 02 Oct. 2013. [Online]. Available: http://thehackernews.com/2012/10/millions-of-dsl-modems-hacked-in-brazil.html. [Accessed 12 Apr. 2017].

[24] "Broadcom b43 and b43 legacy firmware; Official Linux Wireless wiki," [Online]. Available: http://linuxwireless.org/en/users/Drivers/b43/. [Accessed 6 Mar. 2017].

[25] SunRun, "My Sunrun portal," 2017. [Online]. Available: https://www.mysunrun.com/. [Accessed 09 May 2017].

[26] California Energy Commission, "Guidelines for California's solar electric incentive programs (senate bill 1)," 2013.

[27] Y. P. Agalgaonkar, B. C. Pal and R. A. Jabr, "Distribution Voltage Control Considering the Impact of PV Generation on Tap Changers and Autonomous Regulators," IEEE Transactions on Power Systems , vol. 29, no. 1, pp. 182-192, 2014.

[28] R. Hudsona and G. Heilschera, "PV Grid Integration – System Management Issues and Utility Concerns," in PV Asia Pacific Conference, 2011.

[29] M. E. Baran and I. El-Markaby, "Fault Analysis on Distribution Feeders With Distributed Generators," IEEE TRANSACTIONS ON POWER SYSTEMS, vol. 20, no. 4, pp. 1757-1764, 2005.

[30] R. Bhandari, S. Gonzalez and M. E. Ropp, "Investigation of Two Anti-Islanding Methods in the Multi-Inverter Case," in Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008.

[31] NERC, "Cyber Security — BES Cyber System Categorization, Critical Infrastructure Protection," 2016.

[32] M. K. Hossain and M. H. Ali, "Statistical analysis of ramp rates of solar photovoltaic system connected to grid," in 2014 IEEE Energy Conversion Congress and Exposition (ECCE), 2014.

[33] D. Cormode, A. D. Cronin, W. Richardson, A. T. Lorenzo, A. E. Brooks and D. N. DellaGiustina, "Comparing Ramp Rates from Large and Small PV systems, and Selection of Batteries for Ramp Rate Control," SOLON America, University of Arizona..

[34] California ISO, "What the duck curve tells us about managing a green grid," 2016.

[35] Idaho National Laboratory, "Vulnerability Analysis of Energy Delivery Control Systems," U.S. Department of Energy, Idaho Falls, Idaho, 2011.

[36] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," NERC, 2016.