IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 29, 2020, accepted February 24, 2020, date of publication March 25, 2020, date of current version April 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983313

Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations

D. JONATHAN SEBASTIAN CARDENAS[1], (Student Member, IEEE), ADAM HAHN[1], AND CHEN-CHING LIU[2], (Life Fellow, IEEE)

[1]School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163, USA
[2]The Bradley Department of Electrical and Computer Engineering, Virginia Tech University, Blacksburg, VA 24061, USA

Corresponding author: Adam Hahn (a.hahn@wsu.edu)

This work was supported in part by the U.S. Department of Energy under Award DE-IA0000025, in part by the Grid Modernization Laboratory Call (GMLC) under Project GM0100, and in part by the National Council of Science and Technology (CONACYT), Mexico.

ABSTRACT The growing number of consumer-grade network-enabled Distributed Energy Resources (DER) installations introduces new attack vectors that could impact grid operations through coordinated attacks. This work presents a cyber-physical model and risk assessment methodology for analyzing the emerging nexus between Internet of Things-based energy devices and the bulk transmission grid. The cyber model replicates the device-level interconnectivity and software components interaction found within these architectures to understand the feasibly of coordinated attacks, while the physical model is used to assess the attack's impacts on the grid. The manuscript questions the validity of previous papers' claims regarding IoT-based grid attacks by addressing key limitations in both the power grid and cyberinfrastructure models of those works. The resulting methodology is then evaluated using the Western Electricity Coordinating Council (WECC) electrical model coupled with DER's operational statistics from California. The results suggest that current DER penetration rates are not yet significant enough to present serious risk, but continued DER growth may be problematic. Furthermore, the work identifies policies that mitigate these risks through increased device diversity and cybersecurity requirements.

INDEX TERMS Cybersecurity, distributed energy resources, Internet of Things.

I. INTRODUCTION

The overall penetration level of Distributed Energy Resources (DERs) is growing significantly due to ongoing cost decreases and greater public interest towards renewable energy. However, this requires the introduction of new planning, management, reliability, and cybersecurity strategies to address upcoming challenges. Among the pending issues is analyzing the risks of large-scale DER deployments when these become part of large scale networks, like the Internet of Things (IoT).

Emerging standards depend on the smart grid and communication-enabled DER units to maintain adequate grid parameters of individual units based on the system status. The functional operation and security requirements of such systems are being addressed by multiple bodies including UL, SunSpec, and the IEEE, along with government-backed policies (e.g. California Rule 21 and Hawaii's Distributed Generation Interconnection Plan (DGIP) [1]).

Grid operators' primary job is maintaining a continuous system operation subject to physical constraints. Depending on the DER penetration level system operators implement mitigation plans that account for variations in power due to the intermittent nature of renewables. However, there is a lack of procedures for determining and sizing reserves to handle artificial disruptions. This is particularly true for markets where renewables have high penetration rates (instantaneous or installed capacity values) [2], [3].

As identified by other authors, as DER becomes more prevalent, new risk factors will emerge as the devices are increasingly interconnected with networked consumer devices, vendors, aggregators, utilities and other smart grid technologies. This paradigm is a substantial shift from the traditional Supervisory Control and Data Acquisition (SCADA) security approach, in which security depends heavily on the isolation of critical networks.

The distributed nature of DER presents challenges as devices are increasingly owned and controlled by outsiders, while utilities have insufficient oversight to mandate strong security levels for these devices. An array of new technical

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

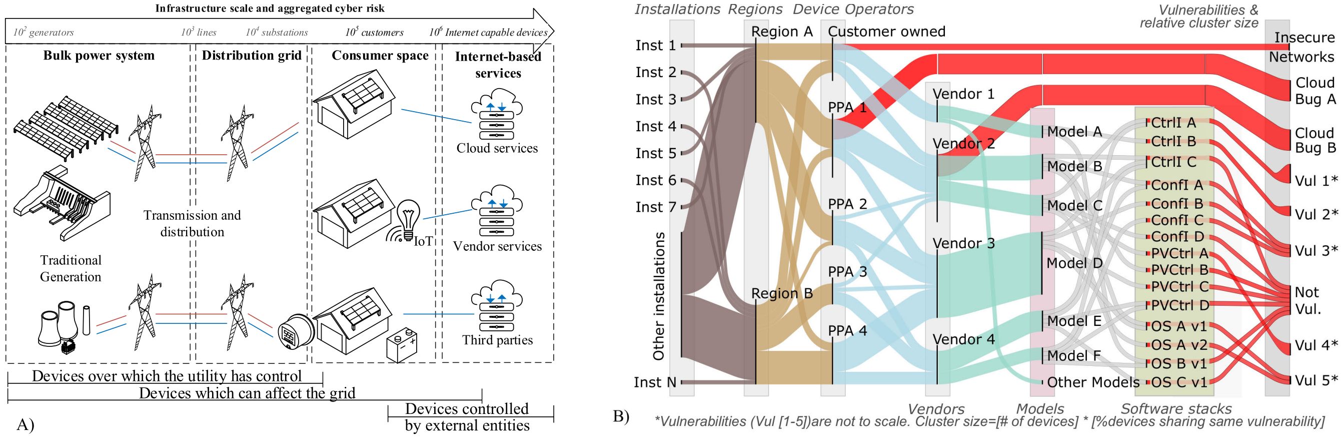

FIGURE 1. A depiction of network dependencies between the grid, vendors, third parties and underlying software.

challenges must be addressed by the utility to manage this emerging risk, specifically the development of new methodologies to identify, measure and mitigate threats to grid operations on DER-targeted attacks.

Addressing this challenge requires that utilities implement novel approaches to identify the impact of attacks on independently owned DER. While attacks to individual devices are insignificant to grid operations, as an aggregated body they introduce significant risks. However, utilities in the near future are not expected to have a complete risk profile associated with each device. Therefore, probabilistic methods of risk assessment will need to be developed.

The contributions of this work are 1) Proposal of new cyber-physical models for DER devices based on their unique properties 2) Evaluation of the proposed models using real-world data and 3) Real-world effects simulations. The reported results expand or refute some of the published work (see section II). Additionally, it is expected that some of the proposed models (such as the network delay-model) can be applicable to other cyber-physical domains. The contributions of this work start in section III, where security risks are identified based on characteristics of DER deployments and underlying infrastructure. In section IV and V, a methodology for analyzing these risks is proposed, both in the cyber and physical domain. Finally, in section VI the proposed models are applied to a real-world system and the results are discussed. Lastly, recommendations to limit the effects of a cyber-attack are provided.

II. RELATED WORK

Traditionally power systems are studied and evaluated under the assumption of naturally occurring events. In some cases, the studies are broadened to address future expansions or to consider rare large-scale events. For example, in [4] the benefits and drawbacks of high-penetration levels of Photo-Voltaic (PV) systems are analyzed. It analyses the stability of the grid under a variety of fault conditions, including sudden PV loss. Although the authors find limited grid impacts, the events are assumed to be non-malicious. In [5] the authors emphasize that hidden risks due to malicious large-scale attacks in DER deployments are present, yet their effects and causes remain largely unexplored.

The concept of hidden risks can be observed in Fig. 1a, where DER devices are interconnected beyond the boundary of a typical utility's cybersecurity management, leaving them more exposed to attacks. An example of such exploitation can be found in [6], where a dynamic attack on demand-side load is used to exceed the power system limits. Similarly, in [7] the authors expand on the concept to assert that a physical-interface can be used to launch cyber-physical attacks.

Two papers that explored these threats are available at [8] and [9]. In [8], the authors propose a scenario where IoT-based load controllers can be used to cause abnormal grid conditions. The authors present a series of attack scenarios that are evaluated under a variety of grid studies. Although the attacks are realistic, some flaws regarding their evaluation methods were identified by [10]. In [9], the authors propose to use Internet-enabled devices to create load "shocks" that can adversely impact the grid. In their proposal, demand variations are triggered by malicious code that alters the computational demands of PCs and peripherals. The authors propose a series of mechanisms that can be used to gain location and timing awareness to maximize impact. In [11], the authors determined the feasibility of attacks against the market by disrupting the Demand Response (DR) signals (i.e. offering artificially low prices during high demand periods), such attacks could exceed the system capabilities and cause localized blackouts. Furthermore, these IoT-derived vulnerabilities have been identified as a significant growing risk by the quadrennial Department of Energy (DOE) security report [12].

In [13] the authors identify key issues with DER deployments and provide a series of product improvements that must be integrated into new systems in order to prevent cyber-attacks. In [14] a Cybersecurity Framework (CSF) compatible with the National Institute of Standards and Technology (NIST) guidelines is presented, the guide has been integrated into a web tool to be used by federal, private and utility scale organizations. The tool guides organizations through the process of satisfying key regulatory domains, with security assessment (e.g. managing risk, threats, and vulnerabilities) being one of the pillars.

Excluding the aforementioned works, most other articles do not model the cyber-factors that determine a system's vulnerability level, either by assuming that a system of devices has been already compromised or that such compromise is trivial to achieve. This contrasts with the more rigorous research techniques applied to traditional control networks, such as SCADA and associated communications infrastructure. For example, in [15] a graph-based model to assess the security risk of individual devices is introduced, where the operator is responsible for "assigning vulnerability weights to each entry point". In [16] a game-theoretic approach is used to model a per device risk. It uses a set of operator-assigned weights used by the game-theory model. Both proposed models ([15], [16]) are bias-prone due to their operator-assigned weight components. In [17] a power-based metric is used to assign the weights but the model has a ''bulk-power system'' applicability.

In summary, DER and IoT-based distributed attacks have focused on determining the effects without analyzing the underlying causes (see Table 1). Fortunately, it seems that some techniques developed for bulk-power system infrastructure can be adapted to this new field. Such adoption, however, is not direct due to their underlying connectivity differences (closed, regulated networks vs open, unregulated). To assess these risks, this paper presents a novel approach where the *cumulative risk* for a wide variety of attack scenarios is determined by calculating the maximum amount of devices which can be controlled by a single entity, this is expressed as the *attacker's controllable power* EAC_{pwr}. This number is computed by using a graph-based model to recreate the mutual dependencies (in the cyber-domain) of a given device and determining the largest cluster size. For simplicity, these individually assessed clusters are combined under the assumption that all attack-vectors have the same probability of occurrence.

TABLE 1. An overview of previous work contributions and identified weaknesses.

Cited work	Physical domain	Cyber domain
[4]	Extensive grid evaluations performed	It assumes natural occurring events.
[15], [16], [17]	Analyze and address grid cyber-security. Most are oriented towards bulk-power systems	Present graph-based cyber models. Based on game-theoretic approaches, some approaches create biases
[11]	Market operations can be affected by incorrect DR signals	
[12], [5]	Acknowledge the presence of hidden risks in DER and IOT enviroments	Addressing IoT cybersecurity is a critical task
[6], [7]	Dynamic load attacks can disrupt grid operations, their effect will be dependent on the # of affected units	No cyber modeling was performed
[8]	+Grid operations can be impacted by IoT-based load attacks but cases were evaluated too strictly	
[9]	+IoT attack model is power and time dependent	Augmented IoT attacks can leverage the internet info to maximize attack
Overview: Studies have identified risks for the power grid across multiple cyber-physical (C-P) domains. Nevertheless, IoT/DER-focused research remains underexplored. This work attempts to fill such a gap by proposing C-P models that are based on real-world data.		

III. DER CYBERSECURITY RISKS

As mentioned earlier, DER systems are highly interconnected network structures that link devices, applications, and services across multiple domains. A depiction of such dependencies is shown in Fig. 2, where not only individual devices can be mapped to administrative agents (i.e. third-party or vendors) but also to the under-laying hardware and software components. Such diagram reveals the means in which vulnerabilities can affect devices across multiple domains. In this section an in-depth review of the DER grid capabilities, communication and hardware/software risks will be discussed.

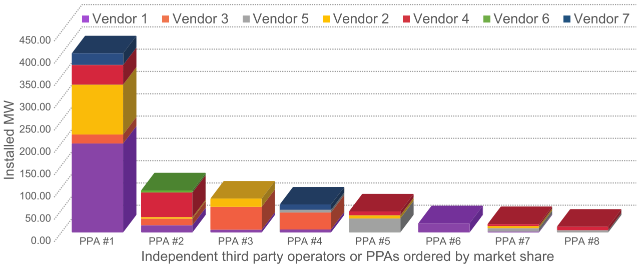

FIGURE 2. Cross PPA/Vendor dependencies.

A. DER'S GRID CAPABILITIES

On-field DER units exhibit a variant degree of functions and management capabilities. Due to the inclusion of *smart inverter grid support functions* administrative agents (i.e. utilities) can exert granular control over individual devices, by imposing dynamic rules that are dependent on the actual grid state. Some key functions include volt/var control, reactive power control and power curtailment. Although these functions are intended to increase grid manageability, function abuse could lead to events that are both complex to identify and mitigate.

B. DER COMMUNICATION RISKS

Network-enabled DER controllers have rapidly gained acceptance since their introduction in 2009 [18]. However, such networking capabilities also increase their attack surface. For example, LAN-WAN (Local Area Network - Wide Area Networks) isolation can be broken by deficient firewall rules or vulnerable equipment [7], [19]. Furthermore, certain technologies (such as Bluetooth) have limited security mechanisms that can be exploited if the attacker is within close proximity. Such attacks can be particularly damaging if multiple devices are within the medium's receive/transmit distance limit (e.g. solar farms, community installations). In addition, certain designs, such as centralized cloud management solutions can become highly desirable entry vectors (i.e. for pushing a compromised SW update), particularly when those interfaces are hard-coded or weakly enforced ([20], [21]).

In the next paragraphs, a brief discussion on DER-related infrastructure vulnerabilities will be presented.

Access mechanism risk factors

- **Communication security:** The security mechanisms used to protect the connection will directly determine whether an attacker could compromise these resources [22], [23]. Since most DER operational markets, do not mandate security mechanisms the existing security can only be expected to match those typically found in IoT devices, which are not perfect [24].
- **Aggregator's communications:** Field devices communicate with aggregator's portals to constantly monitor and schedule day-to-day operations [25]. Although multi-level access mechanisms are usually in place, administrative-level permissions could be abused by unauthorized parties. Additionally, weak aggregator-vendor interfaces can introduce security vulnerabilities.
- **Vendor's cloud-based communications:** Similar to aggregators, vendors provide users with tools to remotely manage their assets, these tools also provide configuration and firmware updates. However, these tools can also be used for malicious purposes if their security mechanisms are compromised.

Deployment characteristics risk factors

- **Inter-Device proximity:** Physical proximity may play an important role in future worm/virus spreading characteristics. Although most viruses rely on the host CPU to operate, recent articles suggest that malware can utilize and peripherals such as network controllers (i.e. Wi-FI) to launch attacks [26].
- **Smart Inverter penetration levels:** Inverters have a varying degree of 'smartness' as many legacy inverters have no communication interfaces, while newer ones provide both wired and wireless connections. Therefore, the degree to which inverters within a region are 'communication-enabled' will directly influence the risk.
- **Aggregator/Vendor market cap**: Targeted attacks can compromise all devices that share a common design flaw (e.g. a vulnerability). Such vulnerability can be present in the device's firmware or at the vendor's cloud-level. Therefore, a vendor with a large market cap implies that a larger set of devices can be exploited by a single vulnerability.
- **Software aging component:** The typical IoT device is expected to receive software updates for a period of three years, while the service life of a DER device is likely to exceed ten years [27]. This situation could lead to the eventual proliferation of insecure devices as attacks increase/improve while the device ages.
- **Shared software components:** The number of shared software components (and thus lack of software diversity) can increase the risk level of succumbing against a single zero-day attack for a large set of devices.

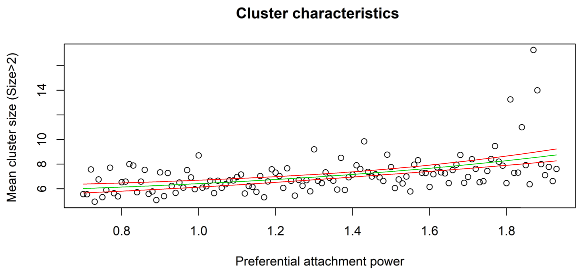

FIGURE 3. Mean cluster size (Vendor $\bigcup$ 3rdP) vs P, with a 90% confidence range (in red).

Examples of these shared components can be observed in Fig. 1 where multiple:
Operating Systems: *{OS A, OS B, ...}*,
Control Applications: *{Ctrl A,..., PVCtrl A, ...}*
Configuration tools: *{ConfI A, ConfI B, ...}*
Network stacks: *{Drivers, Protocol handlers}*
coexist across multiple devices.

IV. RISK MODELING OF END-USER DER DEVICES

Most product development cycles follow incremental improvement rounds, which are broken when sudden technological breakthroughs occur. This foments stable markets (participant-wise) that evolve slowly, unless a new, innovative participant disrupts a market, or financial factors affect participants. Furthermore, studies have shown that people tend to buy products based on company history, personal recommendations, or well-played advertisement campaigns [28]. These factors, lead to markets that behave like oligopolies, where a limited set of vendors and products dominate a market for extended periods of time.

These market tendencies have also been observed inside Power Purchase Agreements (PPA)-based deployments (see figure 2) and other IoT-based load-controlling devices [10]. Such market distributions inherently foster a lack of diversity that may impact its cyber-security properties [29].

A. MODELING VENDOR AND THIRD PARTY PROVIDERS INTERACTION

As outlined by section III-B DER systems can have multiple participants within a service area: *{utilities, consumers, vendors, third parties, and PPA operators}* ∈ *Service_area*. Utilities can interact with all members, but they can be considered as a secure entity due to strict regulatory requirements. In contrast, customers are not required to comply with any requirement, creating security risks (to be explored on section V.1), however individual, targeted attacks are unlikely to cause major issues. On the other hand, vendors and other third parties (including PPA operators) are unregulated, but can have an influence over a large set of devices (later analysis shows that the largest clusters represent the highest risk). To account for these characteristics, a power-law model [30] for analysing these vendor-third party interaction is proposed.

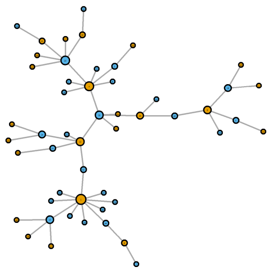

FIGURE 4. Sample Vendor/Third-party cluster, n = 51, 23 PPAs, 28 Vendors, $P = 1.54$.

Based on the observed DER deployment characteristics, a weighted *Barabasi-Albert* preferential attachment (PA) algorithm was selected to recreate the power-law characteristics of the market. The Barabasi-Albert preferential attachment algorithm is a random network generator which seeks to model scale-free networks. It is based on the premise that certain nodes (i.e. hubs) become popular and thus new, emerging nodes will likely get attached to them. Once the algorithm is completed it generates a degree distribution (over the nodes) that follows a power-law distribution. The Barabasi-Albert model employs two steps to replicate its scale-free properties. The algorithm starts with a base network topology (a graph **G**, $G = (\mathbf{V}, \mathbf{E})$ to which the new nodes (V_{new}) and edges ($E_{new} = [V_{new}, V_i \in G]$) will be iteratively added. The new link (or links) added in each step will link V_{new} to an existing $V_i \in G$, the target node (V_i) will be picked by a using a weighted model, the classic model for picking a node i (probability (Π)) is given by:

$$\Pi(V_i) = \frac{deg(V_i)}{sum_{x=1}^{x=n_{total}} deg(V_x)^P} \tag{1}$$

Based on Eq. 1, the nodes with the highest Π value are the most-likely to be selected and the process is repeated. The algorithm has two parameters: (P), the attachment probability; and $l(x)$, the links distribution (number of links added at each step),. Based on this, the P factor was randomly set in the range of 0.8 - 2.0 (to replicate market data), with up to one link added at each step. The (1) link per step was used to simulate that vendors and third parties have only one link between them. Notice that this limit does not imply that each node will have only one link, it rather implies that two nodes can have at most 1 link between them.

Since not all utilities have detailed market information (as compared with [1]) a probabilistic-model; is proposed, this probabilistic model generates random connectivity graphs in which properties can be compared to real-world conditions. Such parameters can be tuned to better represent actual market properties. In the proposed example (see Fig. 4), the random model generator simulates that 1000 nodes are added to the market during each run, each run is executed with a random P value. In this simulation, each node represents a participant, therefore a graph coloring algorithm with a two color threshold is proposed to classify between vendors and third parties. All nodes with degree = 0 are dropped and the generated clusters are saved. The properties of these clusters are compared with actual market conditions (i.e. to pick the best P value, a plot of cluster size vs P is given in 3). The link distribution is also tuned to recreate the market characteristics. The parameters that can be evaluated to set the tuning parameters are:

- Number of participants: vendors and third-parties (3rdP).
- Distribution/Average number of vendors participating with a third party.
- Distribution/Average number of third parties participating with vendors.

Figure 4 shows one of the largest randomly generated clusters (p = 1.54), this will be our starting model for evaluating large scale clustering vulnerabilities between interconnected entities in the next section.

B. MODELING PRODUCT\VENDOR\THIRD-PARTY CONNECTIVITY

Figure 4 represents the communications backbone between vendors and third-party operators, however other smaller clusters are present in our simulated model that must be evaluated. To achieve this operation a second round of preferential attachment is proposed. This second round creates a new node (representing a product) and attaches it to 1 vendor and up to 1 third party operator (linkage probability over a tuple l = vendor = 1,third party <1). To accomplish this task, first a random vendor is picked using the preferential attachment model (with $P = P_v$, where P_v is the vendor attachment factor), then a third party operator is randomly picked (also using preferential attachment) from the set of third parties that are connected to the vendor (with $P = P_t$, where P_t is the third-party attachment factor).

The factors P_v and P_t allow the model to replicate the observed market conditions. For example, Table 2 shows the market distribution for DER devices installed in California, USA [31]. Such vendor distribution can be replicated in the proposed model by using a custom factor of P_v (See Fig. 5). Similarly real-world data can be used to recreate the third

TABLE 2. Device characteristics, per vendor.

Vendor	$Avg.\ S_{site}$ $[kVA]$	$Avg.\ S_{device}$ $[kVA]$	S_{total} $[MVA]$	**Market share** $\%MW$
SMA America	12.41	8.93	436.74	22.74
Advanced Energy	465.56	250.74	185.29	9.65
Power One	7.52	5.41	166.23	8.65
Enphase Energy	5.26	0.21	147.90	7.70
Yaskawa Solectria	134.03	60.90	137.52	7.16
Sun power	6.25	4.77	128.94	6.71
Fronius USA	6.40	5.63	119.15	6.20
PV powered	23.45	19.53	100.09	5.21
Xantrex Tech.	30.58	24.72	99.57	5.18
SolarEdge Tech.	6.66	4.97	28.92	1.51
Kaco	7.45	6.48	21.26	1.11
Others	128.23	20.68	350.20	18.23
Totals	-	-	1921.85	100

party attachment properties (e.g. by using data available in [31] to produce records alike Table 3). Again, such third party market distributions can be simulated by setting P_t (See Fig. 6) and setting the linkage probability $l = \{1, TPC\}$, where TPC denotes the probability of an end-device being connected to a third party (*third party connectivity ratio*).

TABLE 3. California's PPA operators (third parties) market share [32].

3rd party	Market share %
SolarCity/Tesla	31.3%
Sunrun	18.3%
Vivint	15.2%
Sunpower	5.2%
Lennar Homes of California	4.0%
Sunnova	3.2%
Sungevity	2.0%
Others	20.7%

As it can be observed from figures 5 and 6 the market distributions generated by the preferential attachment model are comparable to those observed by real market data (in red). Notice that for simplicity, the models are developed in terms of the *% market share* which is computed according to *installed capacity*. Advanced models can also be created by determining market share based on the *number of field devices* and then appending the capacity of each device into the model. Also note that, due to the model's random nature, it does not follow a precise exponential distribution for simulations that include a small number of nodes. This effect can clearly be observed in Fig 8 and Fig. 7 where some *market share* values (represented by points) significantly deviate from the expected value (represented by lines).

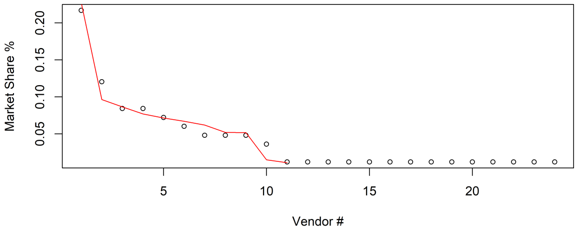

FIGURE 5. A comparison between real-world vendor market shares (red) vs those generated with $P_V = 1.63$, product nodes= 3000.

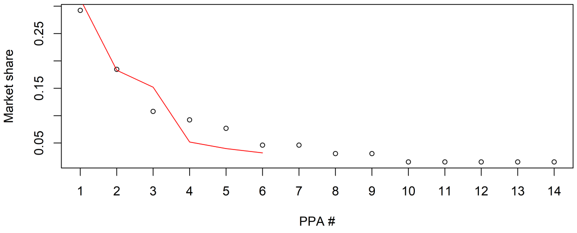

FIGURE 6. A comparison between real-world third party market shares (red) vs those generated with $P_T = 1.63$, product nodes= 3000.

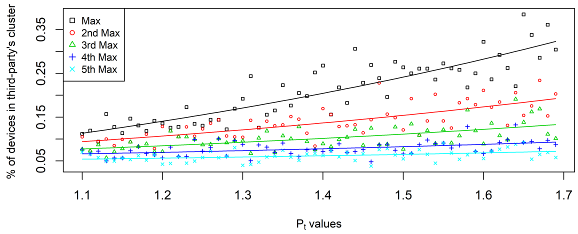

FIGURE 7. Percentage of models attached to the largest (5) third-party clusters.

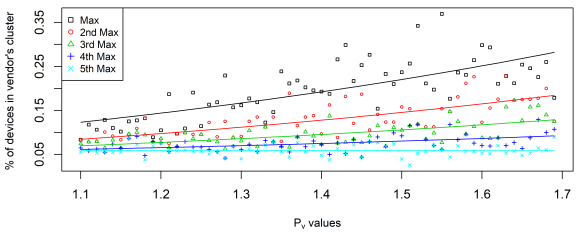

FIGURE 8. Percentage of models attached to the largest (5) vendor clusters.

An interesting note to this model, is that similar product nodes can be aggregated together to represent a device model, or a *device class*, a device class is a common set of devices that share the same common vendor, third party linkages, and have a determined number of members (product-nodes). This second round of preferential attachment model tends to prefer those participants that are already members of a {vendor}-{third party cluster}, reinforcing the concept that a small number of highly interconnected systems tend to appear in DER environments, a concept which will be explored in the next section.

V. RISK ASSESSMENT METHODOLOGY

In this section, a methodology (Fig. 9) for determining the expected amount of DER that can be controlled by a coordinated attack based on a variety of cyber-physical system factors is presented.

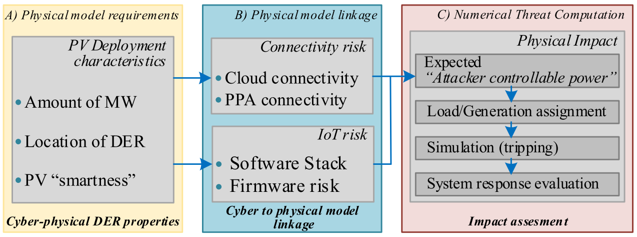
A) Physical model requirements
PV Deployment characteristics
• Amount of MW
• Location of DER
• PV "smartness"
Cyber-physical DER properties
B) Physical model linkage
Connectivity risk
• Cloud connectivity
• PPA connectivity
IoT risk
• Software Stack
• Firmware risk
Cyber to physical model linkage
C) Numerical Threat Computation
Physical Impact
Expected "Attacker controllable power"
Load/Generation assignment
Simulation (tripping)
System response evaluation
Impact assesment

FIGURE 9. Overview of the proposed methodology.

Since future DER units are expected to have an active role in power delivery by using grid support functions more detailed models will be needed. As a first step, reactive power from DER units is represented as a negative complex power load ($-S$). This technique is an extension of the approaches published in [4] and [33] which demonstrate methods for evaluating DER risks in power systems by representing them

Algorithm 1 Feeder NEM Dissaggregation

```
Result: Compute feeder load and masked generation
Given: penetration rate ($P_r = Rated\ PV/Rated\ Load$) for service Area_i
For Each: $feeder \in \mathcal{A}rea_i$
    $X = NEM_{feeder}/(1 - P_r)$
    $Load_{feeder} = X$
    $DER_{feeder} = P_r * X$
```

as negative *active-power* loads and aggregating them to the nearest generation bus.

A. PHYSICAL MODEL REQUIREMENTS

A steady-state model can be used to model and asses the effects of small scale or slowly evolving cyber-originated disturbances. However, sudden large-scale cyber-attacks could lead to significant sudden power imbalances, whose effects could be equivalent to large generation or load tripping events. Therefore it would be ideal to represent the system under a time-variant model that accurately models the system response. Such a model should include the physical and cyber characteristics of DER generation, as well as the grid dynamics. These factors will be discussed in the next sections.

B. PHYSICAL MODEL

Energy consumption is often reported as *Net Metered Energy*, or (NEM), a quantity which aggregates the actual amount of total load and the energy being produced behind-the-meter. Hence, NEM can be modeled as $NEM = Consumed_{Load} - Dist.\ Generation$. Based on this equation, DER supply can be modeled as a negative complex power ($-S_{DER}$) load which value will depend on the primary energy source (i.e. solar intensity) and configured parameters. On a larger scale, a feeder NEM can be modeled as:

$$NEM_{feeder} = Load_{feeder} - DER_{feeder} \tag{2}$$

In [4] the authors proposed aggregating DER units according to their installation ZIP code and then aggregating each zip code's output power into the nearest medium voltage bus. Although this approach can be precise, it requires advanced tracking mechanisms that record both the electrical and cyber characteristics. To simplify this requirement an equally-distributed, per-region (e.g. a service area) DER penetration ratio is proposed. This ratio can be derived from utilities or state-level penetration levels (i.e [34]). The designed algorithm works as follows:

Additionally, the negative load can be located at the middle or end of the feeder by inserting a stray impedance between the interconnection bus and the new generator. The stray impedance value must be representative of typical feeders in the area, this model has been described in detail by [35].

During an attack simulation, a certain *EACpwr* of Distributed Generation (DG) value is taken offline across the entire system and the electrical system response is assessed. Additional scenarios can be studied by including their respective actions and models. Other interest scenarios could include evaluating the operation of protective equipment such as Under-frequency Load Shedding (UFLS) and distance relays.

1) SYNCHRONOUS VS ASYNCHRONOUS ATTACK MODELING

The previously described load model assumes that attackers can simultaneously attack all of the compromised devices. However, in real-world conditions, the attacker's attack sequence is subject to a combination of communication delays and variable response times across multiple devices. To account for this asynchronous behavior a $\Delta P/\Delta t$ model over a *Truncated Gaussian Distribution* (TGD) is proposed. The TGD must satisfy two parameters: 1) the truncated area under the curve must be equal to the amount of power being compromised (ΔP), and 2) its truncated width represents the time-period over which the devices are attacked (Δt). Under this approach, the random variable is bounded within the $[-3.3\sigma\ +3.3\sigma]$ range, a range that encompasses 99.9% of the probabilistic space.

2) DISCRETE LOAD COMPOSITIONS

The TGD-based method can be used to model realistic timing behaviors on a per-feeder level. However, maintaining and simulating multiple, concurrent TGD curves could be computationally-prohibitive. Therefore, as an alternative, an area-dependent, discrete DER_{feeder} value is proposed, the discrete value that can be controlled (on/off) at time t_{op}. Where, t_{op} is computed according to its order in a *bin packaging* algorithm running on top of the TGD-method. Under this formulation, the bin packaging problem tries to allocate discrete bins (representing individual DER_{feeder} values) into multiple fixed-size containers that represent the area under the TGD curve. Although optimal solutions to this algorithm are considered NP-complete, non-optimal solutions based on first-fit algorithms provide sufficiently valid results (see Fig. 17). Furthermore, by using this approach randomness in both time and location domains is achieved.

C. CYBER DOMAIN TO PHYSICAL THREAT COMPUTATION FOR DER DEVICES

According to Fig. 1 each field device can be mapped to individual transmission regions, third parties, as well as individual vendor's hubs. But they can also be mapped to software and location-defined hubs, each of these hubs will have an associated set of risk factors that will influence their impact in this section a breakdown of this factors will be introduced with the aim of translating this risks into numerical grid threats.

1) COMPUTATION OF SERVICE PROVIDER THREATS

Section IV introduced a preferential attachment model that can be used to recreate the dependency links between end-user devices and service providers (vendor and third

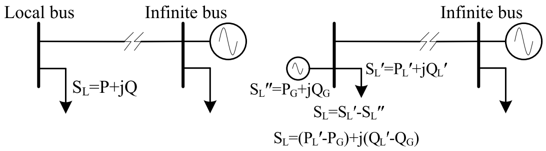

FIGURE 10. Traditional load model vs proposed system.

parties). By analyzing figures 7 and 8 it can be deduced that the largest service providers have the largest number of attached devices and therefore are the largest risk factors. The number of members in a hub will be denoted by Hub_V for vendors, and Hub_T for third parties.

Notice that other risk-limiting factors must be considered before a formal model is proposed, for example, not all products have the same average output power (see Table 2), which can have a correlation with installation types (and management practices). Furthermore, not all products are cloud-connected or actively connected to the Internet. Such complexities must be taken into account before the potential hub impact can be determined. To assist with this task two simplified models that can be used to compute the amount of risk, in terms of *EACpwr* are proposed.

a: VENDOR HUBS

Vendor hubs are not necessarily internet-enabled, with a sample taken from [31] indicating that only 35-40% of devices are internet-enabled, furthermore due to firewalls this value can be lowered. To address this issue, the value can be set based on network reachability tests. Notice that the proposed model (eq. 3) assumes that the PA model was constructed using market share in terms of installed capacity and therefore all nodes (which represent products) are assumed to have the same capacity.

$$EACpwr_V = \#DER * Max(Hub_V) * Int_r * SAPO[W] \qquad (3)$$

where:
$\#DER$ = Number of Installed DER units
$Max(Hub_V)$ = Largest vendor hub, obtained from preferential attachment model [%]
Int_r = Percent of network-reachable devices [0-1]
$SAPO$ = System-wide Average Power Output (i.e. ≈ 2500 W) [W]

In some cases, where the utility only records the system-wide installed capacity (instead of detailed records), the $\#DER$, $SAPO$ terms can be substituted by:

$$SIC = \#DER * SAPO \quad [W] \qquad (4)$$

$$SPL = SIC/System\ Demand(rated) \quad [\%] \qquad (5)$$

where:
SIC = System-wide Installed Capacity [W]
SPL = System-wide penetration level [W]

b: THIRD PARTY HUBS

Most third parties services depend on internet connectivity to function correctly, furthermore it is likely that firewalls are configured to accept connections from these third parties. Such assumptions simplify the $EACpwr_T$ model to:

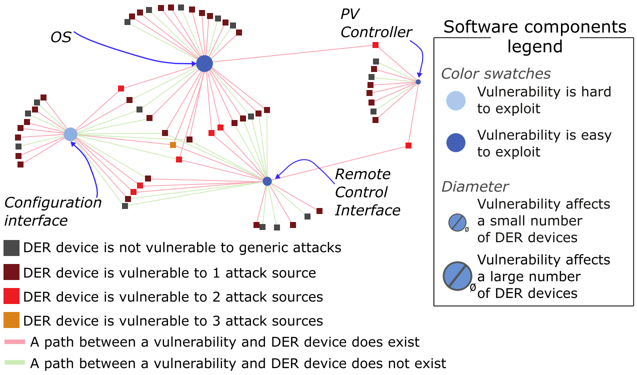
OS
PV Controller
Configuration interface
Remote Control Interface
Software components legend
Color swatches
Vulnerability is hard to exploit
Vulnerability is easy to exploit
Diameter
Vulnerability affects a small number of DER devices
Vulnerability affects a large number of DER devices
DER device is not vulnerable to generic attacks
DER device is vulnerable to 1 attack source
DER device is vulnerable to 2 attack sources
DER device is vulnerable to 3 attack sources
A path between a vulnerability and DER device does exist
A path between a vulnerability and DER device does not exist

FIGURE 11. Typical software components found in smart inverters, showing a sample set of vulnerabilities.

$$EACpwr_T = \#DER * Max(Hub_T) * TPC * SAPO \quad [W] \qquad (6)$$

where:
$\#DER$ = Number of Installed DER units
$Max(Hub_T)$ = Largest third party hub, obtained from preferential attachment model [%]
TPC = Third party connectivity ratio [0-1]
$SAPO$ = System-wide Average Power Output (i.e. ≈ 1800 W) [W]

Although the $Max(v)$ and $Max(Hub_t)$ in equations 3 and 6 assume a single a single hub is evaluated, the under laying graph construction allows to model several *what if cases*, such as:

- **What if,** the top 3 vendors are compromised:
  $Max(3v) = Max(Hub_V) \cup 2^{nd}\ Max(Hub_{(V)}) \cup 3^{rd}\ Max(Hub_{(V)})$
- **What if,** the top vendor and the top third party are compromised:
  $Max(v+t) = Max(Hub_V) + Max(Hub_t)$
- **What if,** the a $vendor_i$ is compromised thru a *third party$_j$*:
  $Max(v\&t) = Max(Hub_{V_i}) \cup Max(Hub_{T_j})$

2) COMPUTATION OF SOFTWARE-BASED THREATS

As shown in Fig. 1, each device can contain multiple software (SW) components that are fused together during product development. This creates a direct analogy with IoT environments, where an IoT system is usually composed of multiple software packages (i.e. a software stack) running on top of an IoT-based operative system. A graphical overview of the core software components in a DER device is shown in Fig. 11. This figure shows the four basic software components: a) The OS, which provides the basic foundation for bridging the hardware and software layers, including low-level network

TABLE 4. (i) Largest DER vendor-hub risk. (ii) Largest DER software-hub risk. (iii) Largest DER 3rd party-hub risk.

(a)

Properties	factors	Cum. %
$S_{California}$	26049MW	100.00%
SIC*	8512MW	32.68%
$MaxHub_V$	22.74%	7.43%
Int_r	20.9%	1.55%
Int_r	36.1%	2.68%

(b)

Properties	factors	Cum. %
$S_{California}$	26049MW	100.00%
SIC*	8512MW	32.68%
Int_r	20.9%	6.83%
$MaxHub_S$	39.00%	2.66%

(c)

Properties	factors	Cum. %
$S_{California}$	26049MW	100.00%
SIC*	8512MW	32.68%
3rd party operated	31.85%	10.41%
$MaxHub_t$	31.30%	3.26%
TPC	95%	3.09%

*SPL is assumed to be equal to the installed capacity as recorded by California's roof top solar installations datbase (NEM + CSI programs)

communications. b) a configuration interface (*ConfI*) which handles the device settings, c) a controller interface (*CtrlI*) which handles the smart inverter functions, and d) a PV controller (*PVCtrl*) that governs the low-level inverter logic.

Although software components developed in-house might introduce zero-day vulnerabilities, this risk is increased when the industry relies on public software libraries that are shared and can thus create large pools of vulnerable devices. Possibly leading to large-scale cyber-attacks (e.g. the Mirai botnet [24]). To illustrate this issue, Fig. 11 was constructed by randomly creating devices (represented by square boxes) that employ 1 or more of the basic SW components (represented by connected edges). Then by randomly classifying some edges as vulnerable edges (in red) we obtain a graph that models the shared-software risk. This image shows how multiple vulnerabilities can affect a single device, for example, certain devices can have 1-or more vulnerabilities that are applicable to it (devices with no vulnerabilities have been omitted). The ability to exploit and mounting an attack will depend on 1) the number of devices sharing the same component (represented by the hub size), 2) the version and configuration requirements required to exploit them, and 3) the ability of remotely exploiting it. This third line of defense will usually be dependent on the reachability of the component, with the OS and remote listeners being more accessible than internal software components.

Many researchers have unsuccessfully tried to predict the outcome of a zero-day event, however infection rates, mechanisms, and effects can vary widely. Therefore, in this work, we have considered unpractical to model the software relationships. Nevertheless, an upper-bounded hub size can be estimated by identifying the most common software component and assuming a vulnerability will be exploitable (e.g. a zero-day vulnerability).

$$EACpwr_S = \#DER * Max(Hub_S) * SAPO \quad [W] \tag{7}$$

where:
$Max(Hub_S)$ = Most common software component*Most common version

VI. CASE STUDY

For the first part of this section, the current risk level for the state of California was analyzed. In this specific example, the 2019 California average demand value in conjunction with the latest penetration records available at [31] were used as the base scenarios. Starting from those records, and the data shown in Tables 2 and 3 the risk levels were computed by assuming various network-reachability levels (using Eqs. 3- 7). The results presented in tables 4(i)-(iii) indicate that the overall risk is low but could increase as the penetration levels or connectivity levels increase.

For the second part of this work, the WECC system was selected. It covers the US southwest which has the highest solar potential [36]. With California alone, exhibiting the largest penetration levels in the continental US [37]. The results of this work are based on the 2012 high-load summer scenario which had an estimated peak load of 66,939 MW in the California region (vs the 71,329 MW actually measured during that summer [34]). As required by NERC the base-model can withstand typical $(n-1)$ failure scenarios and therefore can tolerate the effects of everyday contingencies, such as a 3-phase fault inside a critical substation (see Fig. 12).

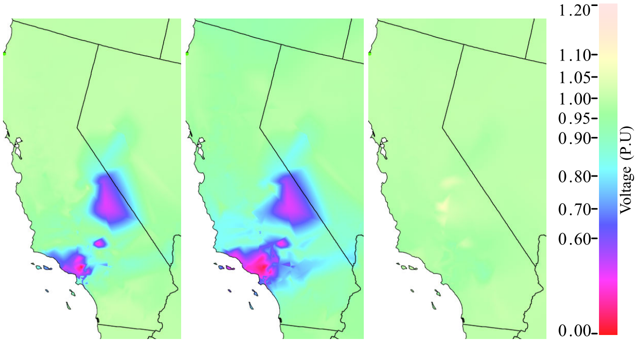

FIGURE 12. Effects of a 3ph fault inside a critical substation bus [24147 — Sylmar] at t = 0, t = .058 and t = .150 seconds.

The operating scenario was simulated in PSLF®. The solution parameters where set as follows: *{Unsteady steady rate =.0001, step width = 1/4 cycle, tolerance = .0005, Maximum solution iterations = 200}*. For this work, an unstable condition is said to occur when the simulator fails to converge during a transient study and no further processing can be performed.

Another example of a critical component is the Grand Coulee Power plant, with a capacity of 6465 MW [38].

For this work, four scenarios are assumed. The first two cases consider that a cyber attack towards DER infrastructure occurs. While a third case assumes a DER attack coincides

TABLE 5. (i) 35% renewables, attack targets largest vendor and largest third party. (ii) 45% renewables, attack targets largest vendor and 2-largest third parties. (iii) 45% renewables, attack targets largest vendor and largest third party.

(a)

Properties	factors	Cum. %
$S_{California}$	66,939MW	100.00%
SIC†	23,428MW	35%
SIC$_{DER}$	70%	24.5%
$Max(Hub_V)$	33%	8.08%
Int_r	0.85	6.87%
$Max(Hub_T)$	30%	7.35%
TPC	0.98	7.2%
$\%EACpwr$	-	14.0%

† Total renewable generation includes non-inverter based resources

(b)

Properties	factors	Cum. %
$S_{California}$	66,939MW	100.00%
SIC†	30,122MW	45%
SIC$_{DER}$	70%	31.5%
$Max(Hub_V)$	33%	10.40%
Int_r	0.85	8.84%
$Max(Hub_T)+$ $2nd\ Max(Hub_T)$	50%	15.75%
TPC	0.98	15.44%
$\%EACpwr$	-	24.3%

(c)

Properties	factors	Cum. %
$S_{California}$	66,939MW	100.00%
SIC†	30,122MW	45%
SIC$_{DER}$	70%	31.5%
$Max(Hub_V)$	33%	10.39%
Int_r	0.65	6.75%
$Max(Hub_T)$	30%	9.45%
TPC	0.98	9.26%
$\%EACpwr$	-	16%

TABLE 6. Scenario parameters for Loss of distributed PV.

Attack type	System penetration level	$\%EAC$ Pwr_V	$\%EAC$ Pwr_T	$\%EAC$ Pwr	Affected MW	$\%Nodes$ $f_{min} <$ $59\ Hz$	$\%Nodes$ $f_{Max} >$ $61\ Hz$	$\%Nodes$ $V_{min} <$ $.1\ PA$	$\%Nodes$ $V_{min} <$ $.5\ PA$	$\%Nodes$ $V_{min} <$ $.8\ PA$	v_{max} PA
Vendor +Third party	35%	6.87%	7.2%	14.1%	6,127	0	0	0	0	3.3	1.0694
Vendor +2 third parties	45%	8.84%	15.44%	24.3%	10,722	28.5	38.1	1.2	9.1	36.9	1.2010
Vendor+third party + relay misconfig.	45%	6.75%	9.26%	16.1%	7,000	17.5	2.7	1.3	8.2	44.9	1.2870

*The reported variables are the maximum/minimum values observed during the entire simulation and may have occurred at different instants. Frequency (f) values were sustained for 3 cycles, voltage (V) values were sustained for 1 cycle. Voltages are in multiples of pre-attack values. Hub sizes are calculated assuming 100% of devices will be smart inverters

with a malfunction in a protective device. While the final scenario considers the asynchronous time characteristics of real-world attacks.

All of the scenarios assume future DER penetration levels of either 35% or 45%. These scenarios are in accordance with California's 50% target set by 2030 (with an interim 30% renewable energy goal set for 2020 [39]). Both Scenarios assume that 70% of this renewable generation will come from network-enabled, DER-based generation. The exact factors (percentages) considered for each attack are summarized in Tables 5(i)-(iii). Notice that internet reachability for vendor-based attacks is set much lower than the reachability levels of third-party services. This is to account for the economic-driven factors of constant monitoring by third parties

In all scenarios, the Total Expected Attacker Controllable Power (*EACPwr*), is assumed to be attainable by clustering the largest vendor and largest (or largest) third party hubs. These penetration percentages are based on expected future values ((from Tables 2, 3). The first three scenarios assume that 1) *%EACPwr* is controllable by the attacker, 2) attacked devices are located inside the California market, specifically within the Investor Owned Utilities, 3) simultaneous DER disconnection event occurs during the peak of DER generation output (a time synchronous-event is assumed). The cases are as follows:

A. COORDINATED DISCONNECTION OF PV (20%)

In the first scenario, 6,127 MW of power are lost instantaneously (14%). However, the effects are transitory, with minor voltage drops (see Fig. 13), the system can return to a stable operating point. Table 6 summarizes the percentage of buses that have severely violated the operating conditions (both in frequency and voltage terms), for this case only 3.3% of the nodes experienced low voltages for approximately 3 cycles.

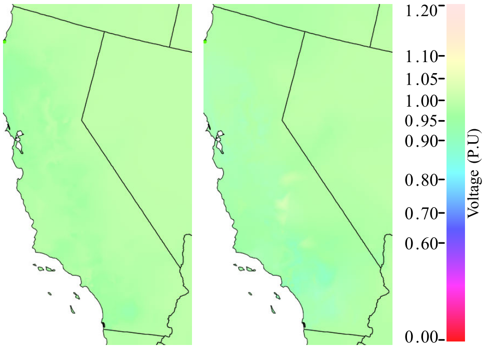

FIGURE 13. Initial V_{drop} at $t = 0$ a) during a 14%*EACPwr* trip (6,127MW) and b) during a 24% *EACPwr* trip in California [10,744MW].

B. COORDINATED DISCONNECTION OF PV (35%)

The second scenario causes a DER trip event that accounts for 10,722 MW (operating with a .85 leading power factor). If this amount of power is suddenly lost (equivalent to 6.1% of the available generation in the WECC), it causes an immediate voltage issue on the grid (see Fig 13). Even if these voltages are apparently less severe than those produced during a typical fault (see Fig.12) it triggers a set of events that ultimately led to an unstable system condition. Fig 14 shows the voltages and frequency swings occurring during the event.

Table 6 shows that a large percentage of the nodes exhibit abnormal frequencies that ultimately cause the system to

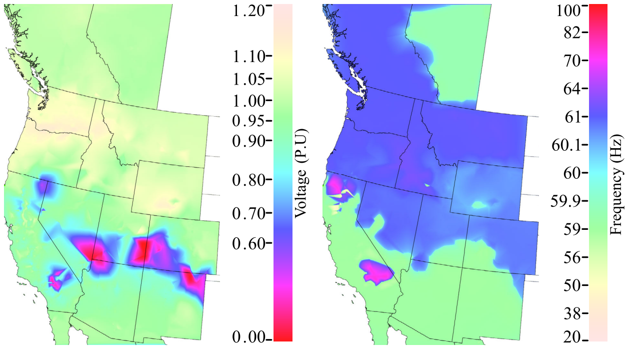

FIGURE 14. a) System Voltage at $t = 6.25s$ after the trip event in California, b) System frequency at $t = 9.5s$ after the attack event (scenario 2).

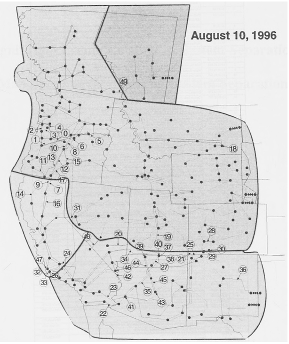

FIGURE 15. Island formation during the 1996 WECC Blackout.

break into several islands. This further causes several buses to become disconnected creating a cascading failure event.

The final observed frequencies for this event are shown in Fig. 14. As it can be observed the island formation resembles those of the 1996 blackout (Fig. 15).

C. CONCURRENT GRID EVENTS

The previous scenarios require a relatively high penetration ratio to cause a significant disturbance. However, these cases were evaluated under normal grid conditions which ignore the security requirements of a typical "$n - 1$" contingency evaluation. To address this issue, an scenario where three relay units have misoperated either as a result of a naturally occurring event or due to a cyber attack is assumed.

In the proposed scenario, the protection characteristics of the relays (which protect 3 lines, two originating at the same substation) are assumed to operate correctly under normal conditions, yet trip instantaneously when a power oscillation is incorrectly identified in zone 3. This was achieved by: 1) modifying the Z3 reach characteristics, 2) disabling the oscillation detection mechanism. Although the assumptions were done using modified settings (i.e. due to a cyber-attack), such events occur many more times than desired by the power industry [40], [41].

This attack lowers the system-wide penetration requirements to 23% (reusing the same $EACPwr's$ factors). Under

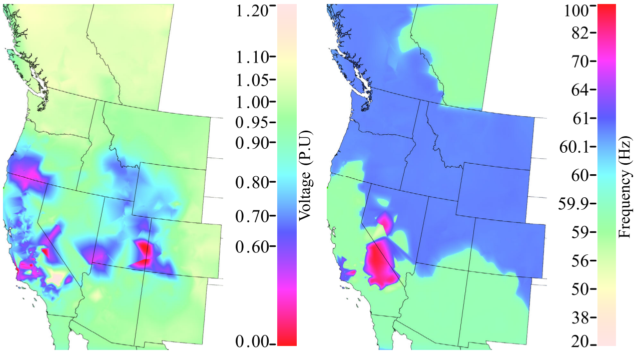

FIGURE 16. a) Voltage profile at $t = 6.50s$ after DG is tripped. b) Frequency profiles at $t = 14.318s$ after the event.

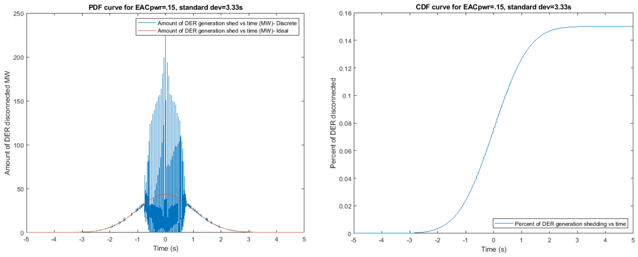

FIGURE 17. a)Ideal vs discrete PDF values attained b) Attained CDF for scenario 4.

this scenario ($\%EACPwr = 16\%$) the expected amount of lost DG is 7,000 MW (See Table 6). The result of these coordinated attacks results in an unstable operating condition. The final system frequencies can be observed in Fig. 16b. While the effects of a voltage swing can be observed in Fig. 16a.

D. EFFECTS OF A NON-COINCIDENT ATTACK

Under this scenario $\%EACPwr$ is assumed to be 15% (6.8GW), It considers a time and location TGD-modeled attack over a period of 10s in the state of California. The computed TGD was calculated with a $\sigma = 3.3s$ and an effective time range of $[-5, +5]$ s. The resulting curves (density and cumulative functions) are shown in 17. The outcome of this non-coincident attack also results in grid separation and an eventual lack of convergence. This result has been attributed to badly tuned electrical models (i.e. the PSLF model).

From Fig. 16 it can be observed that low voltages could cause legacy devices (non-ride thru enabled) to disconnect, leading to more cascading events. This effect can also be used to lower the amount of power that the attacker controls, e.g. by controlling 5,000 MW and indirectly causing an additional 2,000 MW to trip due to low-voltage disconnections. In Fig. 18 a time series representation of the tripped lines is shown, the coordinated attack caused 45 lines to trip.

VII. DISCUSSION AND PROPOSED MITIGATIONS

This paper evaluates the risk and impacts of attacks to IoT-based DER devices, utilizing real-world information

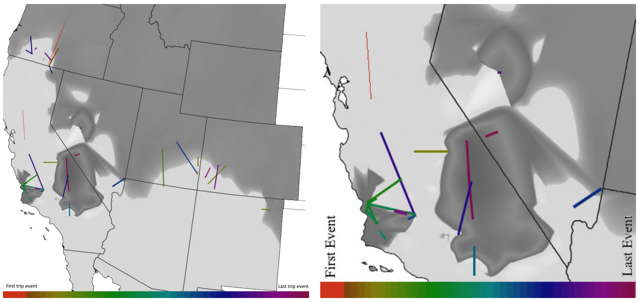

FIGURE 18. Timeline of trip events.

regarding the diversity of DER deployments and its underlaying grid (the WECC model). The results of the paper specifically contradict previous works, demonstrating that attacks targeting any single-entry vector, such as hijacking all devices within one central entity (e.g. PPA, vendor) or compromising Internet connectivity will have minimal impact to grid operations based on the current penetration rates. Specifically, the work questions the severity of the results obtained by [8] and [9]. Works which explored generic attacks to IoT-based devices rather than DER devices, their results strongly suggested that IoT-based attacks could have significant implications to the grid. However, both works failed to incorporate realistic methods/models that accounted for the attacks' propagation methods.

Furthermore, the presented results likely over-emphasize the risk, since the employed model lacks some of the grid security mechanisms, such as Remedial Action Schemes (RAS) and ignores corrective operator-based responses. Nevertheless, substantial increases in DER penetration will likely increase these risks. Other factors that might increase the risk are concurrent events such as badly tuned controls, misconfigured equipment, or by pushing incorrect settings to DER devices (via IEEE 2030.5). However, such attacks are deemed opportunistic, since they require the presence of an external agent.

Based on these studies, the authors suggest that the proposed risks will grow and require additional countermeasures to ensure adequate protection against such threats. Utilities need to model, evaluate and address the new emerging risks from external infrastructure, including IoT-controllable loads, DER and transactive energy mechanisms. Since utilities have little control over the external infrastructure policies must be designed to reduce the size of vulnerable clusters. This can be accomplished by developing policies that *1)* increase market diversity, *2)* limit the number of devices controlled by a single entity, *3)* establish risk assessments procedures, *4)* establish contingency and mitigation procedures, *5)* advocate for an increase in security mandates of DER infrastructure and, *6)* create monitoring and response programs that mitigate risks.

In this context, the Department of Homeland Security has published a set of strategic guidelines for addressing cybersecurity of IoT infrastructure [42]. Short term solutions include developing risk analysis based on worst-case scenarios as well as their mitigation strategies, the inclusion of mandatory software maintenance programs into existing warranty mandates, use of hardware-enforced fail-back mechanisms as well as promoting interest towards the security of distribution side components.

VIII. CONCLUSION

The work presented an overview of the IoT-based risks currently present in DER devices. These risks were incorporated into a risk assessing methodology that uses a probabilistic approach to compute the amount of an attacker's controllable power. The attacker's controllable power is then fed into a power system model to assess the physical grid impacts. The risks and proposed methodology were applied to two hypothetical scenarios where the 2020 and 2030 California's renewable energy targets are assumed to be fulfilled. Based on the results of these scenarios it is imperative to state that large distribution-side components must be included during power-grid security assessments. They should be ideally included as part of the technical risk evaluation process imposed by regulating bodies. Our current work assumes that a synchronized timing source is available to the attacker, and that devices can instantaneously react, further work must be developed to account for time deviations in time-driven attacks. The presented cases show that in the future, the grid may be vulnerable to large scale DER attacks, even if they are connected at the distribution levels. Finally, guidelines for reducing risks and mitigating IoT-based risks are identified. These guidelines are based on industry trends and will be generally applicable to a wide range of energy delivery systems.

ACKNOWLEDGMENT

The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

REFERENCES

[1] *IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters*, California Smart Inverter Working Group, Folsom, CA, USA, 2016.

[2] (2017). *California ISO Peak Load History 1998 Through 2016*. [Online]. Available: http://www.caiso.com/Documents/CaliforniaISOPeakLoadHistory.pdf

[3] DBA Energy Solutions, CA, USA. (2017). *CSI Working Data Set*. [Online]. Available: https://www.californiadgstats.ca.gov/downloads/

[4] S. Eftekharnejad, V. Vittal, G. T. Heydt, B. Keel, and J. Loehr, "Impact of increased penetration of photovoltaic generation on power systems," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 893–901, May 2013.

[5] F. Cleveland and A. Lee, "Cyber security for DER systems," CAISO, Folsom, CA, USA, Tech. Rep., 2017.

[6] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2015, pp. 1–5.

[7] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[8] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Secur. Symp.*, 2018, pp. 15–32.

[9] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf. (ACSAC)*, New York, NY, USA, 2017, pp. 303–314.

[10] D. J. Sebastian and A. Hahn, "IoT threats to the smart grid: A framework for analyzing emerging risks," in *Proc. Northwest Cybersecur. Symp.*, 2019, pp. 1–8.

[11] C. Barreto, A. A. Cárdenas, N. Quijano, and E. Mojica-Nava, "CPS: Market analysis of attacks against demand response in the smart grid," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, New Orleans, LA, USA, Dec. 2014, pp. 136–145, doi: 10.1145/2664243.2664284.

[12] DOE. (2017). *Quadrennial Energy Review, Transforming the Nation's Electricity System: The Second Installment of the Qer*. [Online]. Available: https://goo.gl/g7gC98

[13] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *Proc. Resilience Week (RWS)*, vol. 1, Nov. 2019, pp. 226–231.

[14] C. Powell, K. Hauck, A. D. Sanghvi, A. Hasandka, J. Van Natta, and T. L. Reynolds, "Guide to the distributed energy resources cybersecurity framework," NREL, Golden, CO, USA, Tech. Rep. NREL/TP-5R00-75044, 2019.

[15] S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol, "Model-based cybersecurity assessment with NESCOR smart grid failure scenarios," in *Proc. IEEE 21st Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Nov. 2015, pp. 319–324.

[16] E. Canzani and S. Pickl, "Cyber epidemics: Modeling attacker-defender dynamics in critical infrastructure systems," in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed. Cham, Switzerland: Springer, 2016, pp. 377–389.

[17] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "ARCADES: Analysis of risk from cyberattack against defensive strategies for the power grid," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 3, no. 3, pp. 119–128, Mar. 2018.

[18] SMA America LLC, Rocklin, CA, USA. (Oct. 2009). *SMA America Unveils New Sunny Beam PV System Monitor*. [Online]. Available: https://www.goo.gl/quwg5d

[19] C. Talos. (May 2018). *New VPNFilter Malware Targets at Least 500k Networking Devices Worldwide*. [Online]. Available: https://blog.talosintelligence.com/2018/05/VPNFilter.html

[20] F. Bret-Mounet. (Jul. 2016). *All Your Solar Panels Are Belong to Me*. https://goo.gl/GBVxPY

[21] P. Fairley. (Feb. 2015). *800,000 Microinverters Remotely Retrofitted on Oahu in One Day*. [Online]. Available: https://goo.gl/EziN5i

[22] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?" in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, New York, NY, USA, 2016, pp. 3748–3760.

[23] R. P. Fernandes-Santos. (Oct. 2016). *Arris Password of the Day Generator*. [Online]. Available: https://github.com/borfast/arrispwgen

[24] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, "Understanding the mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, 2017, pp. 1093–1110.

[25] *SUNNY BOY 3000TL/3600TL/4000TL/5000TL Installation Manual*, SMA Solar Technol. AG, Niestetal, Germany, 2014.

[26] Google Project Zero. (Apr. 2017). *Over the Air: Exploiting Broadcom's Wi-Fi Stack (Part 1)*. [Online]. Available: https://goo.gl/9A9dWC

[27] *Guidelines for California's Solar Electric Incentive Programs (Senate Bill 1)*, California Energy Commission, Sacramento, CA, USA, 2013.

[28] A. Kodjamanis and S. Angelopoulos, "Consumer perception and attitude towards advertising on social networking sites: The case of facebook," in *Proc. Int. Conf. Commun., Media, Technol. Design*, Famagusta, Cyprus, 2013, pp. 1–6.

[29] D. Geer, R. Bace, P. Gutmann, and P. Metzger. (2009). *Cyberinsecurity: The Cost of Monopoly*. [Online]. Available: https://cryptome.org/cyberinsecurity.htm

[30] J. Leskovec, A. Singh, and J. Kleinberg, "Patterns of influence in a recommendation network," in *Advances in Knowledge Discovery and Data Mining*, W.-K. Ng, M. Kitsuregawa, J. Li, and K. Chang, Eds. Berlin, Germany: Springer, 2006, pp. 380–389.

[31] DBA Energy Solutions, Oakland, CA, USA. (2018). *Distributed Generation Incentive Program Data*. [Online]. Available: https://www.californiadgstats.ca.gov/downloads/#_nem_cids

[32] DBA Energy Solutions, Oakland, CA, USA. (2018). *Distributed Generation Interconnection Program Data*. [Online]. Available: https://www.californiadgstats.ca.gov/downloads

[33] "Oahu distributed PV grid stability study part 1," Hawai'i Natural Energy Inst., Honolulu, HI, USA, Tech. Rep. DE-EE0003507, 2016.

[34] (May 2014). *State Electricity Profiles*. [Online]. Available: https://www.eia.gov/electricity/state/archive/2012/

[35] N. W. Miller and K. Clark, "Impacts of high levels of distributed PV and load dynamics on bulk power transient stability," NREL, Golden, CO, USA, Tech. Rep. NREL/CP-5D00-66971, 2019.

[36] R. George and E. Maxwell, "High-resolution maps of solar collector performance using a climatological solar radiation model," in *Proc. 24th Nat. Passive Solar Conf.* Portland, ME, USA: NREL, Jul. 1999.

[37] *A Wide-Area Perspective on the August 21, 2017 Total Solar Eclipse*, NERC, Atlanta, GA, USA, 2017.

[38] (1989). *Grand Coulee Dam—Hydroelectric Project Information*. [Online]. Available: http://www.cbr.washington.edu/hydro/grandcoulee

[39] California Energy Commission. (Oct. 2015). *RPS Program Overview*. [Online]. Available: http://www.cpuc.ca.gov/RPS_Overview/

[40] *Analysis of System Protection Misoperations*, Electr. Power Res. Inst., Palo Alto, CA, USA, 2015.

[41] *State of Reliability: 2019*, NERC, Atlanta, GA, USA, 2019.

[42] Department of Homeland Security. (2016). *Securing the Internet of Things*. [Online]. Available: https://www.dhs.gov/securingtheIoT

D. JONATHAN SEBASTIAN CARDENAS (Student Member, IEEE) received the B.E. and M.Sc. degrees in electrical engineering from the Instituto Politećnico Nacional, Mexico City, Mexico, in 2013 and 2015, respectively. He is currently pursuing the Ph.D. degree in computer science at Washington State University, Pullman, WA, USA. His current research interests include cybersecurity of large-scale systems and privacy issues.

ADAM HAHN received the M.S. and Ph.D. degrees from the Department of Electrical and Computer Engineering, Iowa State University, in 2006 and 2013, respectively. Previously, he worked as a Senior Information Security Engineer at MITRE Corporation. He is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, Washington State University. His research interests include cybersecurity of the smart grid and cyber-physical systems (CPS), including intrusion detection, risk modeling, vulnerability assessment, and secure system architectures.

CHEN-CHING LIU (Life Fellow, IEEE) received the Ph.D. degree from the University of California at Berkeley, CA, USA. He is currently an American Electric Power Professor and Director of the Center for Power and Energy, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA. He is also a Research Professor with Washington State University, Pullman, WA, USA, and a Visiting Professor with the University College Dublin, Dublin, Ireland. He was a recipient of the IEEE PES Outstanding Power Engineering Educator Award and the Doctor Honoris Causa from the Polytechnic University of Bucharest, Bucharest, Romania. He was the Chair of the IEEE PES Technical Committee on Power System Analysis, Computing, and Economics.