Assessing DER Network Cybersecurity Defences in a Power-Communication Co-Simulation Environment

Jay Johnson*, Ifeoma Onunkwo, Patricia Cordeiro, Brian J Wright, Nicholas Jacobs, Christine Lai

Sandia National Laboratories, Albuquerque, NM, USA
*jjohns2@sandia.gov

Abstract: Increasing penetrations of interoperable distributed energy resources (DER) in the electric power system are expanding the power system attack surface. Maloperation or malicious control of DER equipment can now cause substantial disturbances to grid operations. Fortunately, many options exist to defend and limit adversary impact on these newly-created DER communication networks, which typically traverse the public internet. However, implementing these security features will increase communication latency, thereby adversely impacting real-time DER grid support service effectiveness. In this work, a collection of software tools called SCEPTRE were used to create a co-simulation environment where SunSpec-compliant PV inverters were deployed as virtual machines and interconnected to simulated communication network equipment. Network segmentation, encryption, and moving target defence security features were deployed on the control network to evaluate their influence on cybersecurity metrics and power system performance. The results indicated that adding these security features did not impact DER-based grid control systems but improved the cybersecurity posture of the network when implemented appropriately.

Index Terms: Distributed energy resources, cybersecurity, network security, co-simulation, red teaming, moving target defence

1. Introduction

There is ample evidence from the last decade that many power system networks in the US [1-6] and abroad [7] are the target of active cybersecurity reconnaissance and attacks. The most widely discussed attacks are those that caused widespread blackouts in Ukraine in 2015 and 2016 [8-9], but there have been several other disconcerting trends including: the increase in operation technology (OT)-focused malware, e.g., Crash Override and Black Energy [10-11], deep reconnaissance into power system networks [12-14], and growing willingness to deploy powerful cyber weapons that are affecting critical infrastructure [8-9, 15]. Attackers often use myriad techniques to gain footholds in information technology (IT) networks and then pivot to other computers, servers, and networks to exfiltrate sensitive information, monitor operations, or plan for sophisticated attacks [16].

At the same time, penetrations of Distributed Energy Resources (DER)—e.g., Photovoltaics (PV) and Energy Storage Systems (ESS)—in the electric power system continue to grow rapidly on distribution and subtransmission systems [17-18]. Over the last decade, an increasing number of inverter vendors and aggregators have provided monitoring portals for their customers. Like many other Internet of Things (IoT) devices, modern DER provide this monitoring or control functionality via proprietary communication protocols. However, these IoT devices now control a substantial portion of the total power production in certain jurisdictions, like Hawaii and California [19-20].

In 2018, a revision to the US interconnection and interoperability standard, IEEE Std. 1547, required DER equipment to have either an IEEE 2030.5, IEEE 1815 (DNP3), or SunSpec Modbus communication interface [21]. New California Public Utility Commission (CPUC) Electric Rule 21 regulations that went into effect in early 2019 define IEEE 2030.5 [22] as the default application protocol for Investor Owned Utilities (IOUs) communications to DER [23-24]. The adoption of standardized communication protocols is a critical step toward interoperability between power system operators and DER equipment, but a comprehensive national approach to DER cybersecurity is absent.

There are many security requirements for operators of critical infrastructure in the US. Power system operators are required to adhere to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards which cover—among other things—training, security and information management, perimeter defences, and incident reporting [25]. NERC requirements are reserved for bulk power equipment operating at or above 100 kV, so DER equipment and associated networks are exempt from these requirements. The solar industry and national government understand this gap in power system security and are working to address the requirements by reviewing and updating security requirements in the DER communication protocols [26-27], standing up DER cybersecurity working groups [28], and seeking new security standards for DER devices and networks [29].

There is extensive research that may improve the national DER cybersecurity posture [30]. Generally, utilities principally rely on perimeter defences (e.g., firewall rules) to defend their IT and OT systems and there is little emphasis placed on the holistic network design. In this work, three additional network defence techniques were analysed with respect to power system performance and security trade-offs; network segmentation, encryption, and moving target defence (MTD) were deployed in a virtualized environment to (A) calculate the additional communication latencies associated with these features, (B) determine the impact these would have for distribution- and transmission-level grid

services (e.g., voltage regulation, frequency reserves, protection, etc.), and (C) evaluate any security improvements in the broad areas of confidentiality, integrity, and availability by conducting adversary-based (red team) assessments. This work produced power system performance and cybersecurity metrics to advise the solar and power system industry on best cybersecurity practices for DER networks. The primary contributions of this work are (A) designing and operating the first photovoltaic communications network in a cyber-physical co-simulation environment with real network packets passed between virtualized DER equipment and a DER management system (DERMS), (B) evaluating network latency for several DER network defence strategies, and (C) quantifying cybersecurity metrics for defensive strategies with live human-in-the-loop red team assessments.

In the remainder of the manuscript, Section 2 introduces the co-simulation environment and associated emulation components. Section 3 discusses the additional latency in DER communication networks when applying networking defence technologies. Section 4 covers the red team assessment methodology, limitations, and results for each DER network design. Section 5 provides conclusions on the cyber-physical studies and recommendations for future research.

2. Co-Simulation Environment

SCEPTRE (capitalized, but not an acronym) is a live, virtualized power system and control network co-simulation platform developed at Sandia National Laboratories (Sandia) capable of investigating the trade-offs between power system performance and cyber resilience [31]. SCEPTRE provides a comprehensive industrial control system (ICS) and/or supervisory control and data acquisition (SCADA) modelling and simulation hardware-in-the-loop (HIL) capability that captures the cyber-physical impacts of controls system operations and targeted cyber events. Changes in the network are reflected in the power simulation, and changes in the power simulation are reflected in the communication system, thereby allowing researchers to analyse the complex interactions in a cyber-physical environment. A simplified representation of the co-simulation environment is shown in Fig. 1.

2.1. Virtual Machines

The virtual components in a SCEPTRE model are created and run as virtual machines (VMs) using Minimega, an Emulytics™ (Emulation + Analytics) tool, that was developed at Sandia for orchestrating distributed VMs and producing host and network emulations. SCEPTRE leverages Minimega's hypervisor capabilities to deploy VMs on compute nodes [32]. A virtual representation of PV inverters was created as SunSpec Modbus Remote Terminal Units (RTUs) using SunSpec Models 1, 101, 123, and 126—

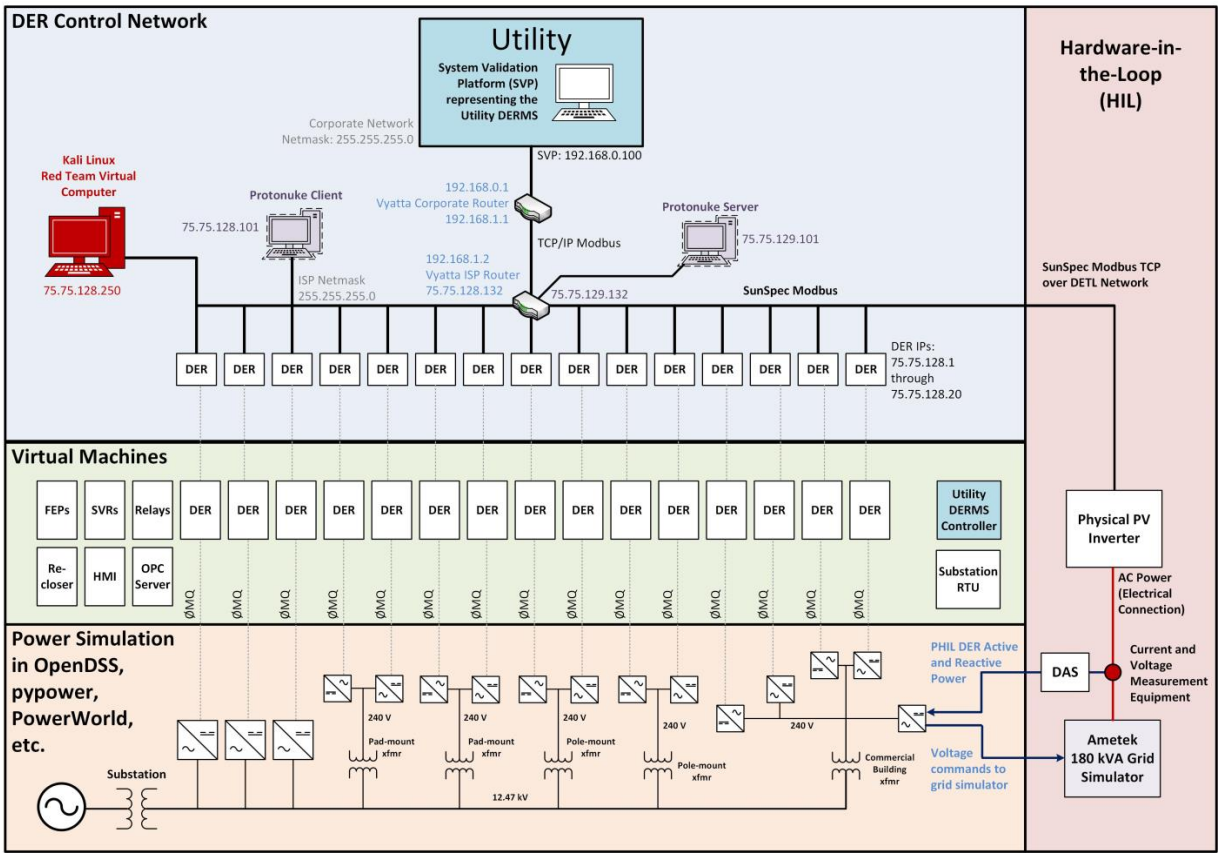

Figure 1: SCEPTRE co-simulation environment with a representative flat, unencrypted network topology and DER HIL.

containing *Common*, *Inverter (Single Phase)*, *Immediate Controls*, and *Static Volt-VAR* data (see [33]). These virtual RTUs interface with photovoltaic systems represented in the power simulation using ZeroMQ as discussed in Section 2.3.

Along with the PV inverters, networking equipment was also created using emulated switches and routers. A utility Advanced Distribution Management System (ADMS) system was created using a Windows 7 VM running a SunSpec System Validation Platform (SVP) [34] executable to provide control and monitoring of the DER systems inside the environment.

2.2. Network Environments

The communication architectures were created in SCEPTRE to include components of a utility-to-DER network. Within the utility subnet, an ADMS—implemented using the SunSpec SVP—conducted the Volt-VAR shift control algorithm from [35-36] by sending SunSpec Modbus packets through the emulated network. Measurements from the power system were pulled by the 20 DER RTUs and Volt-VAR control settings were issued—as required—once per second. For these experiments, the following environments were created:

1. A flat network with and without SSH encryption.
2. A network segmented into three random enclaves with and without SSH encryption between the ADMS and the enclaves. A HIL inverter was added to the network without SSH encryption.
3. A moving target defence network without encryption.

These architectures were adapted from the work done in [37] for cybersecurity network architectures in microgrids, but in this case reflect a DER ADMS control system. An example of flat unencrypted topology is shown in Fig. 1. Appendix A includes the flat encrypted and segmented encrypted topologies. The other topologies are presented in [38].

Internet traffic was generated to simulate normal conditions where other entities are connecting to internet resources. Simulated packets were produced using Protonuke clients and servers—standalone Minimega tools for IP traffic generation—which support HTTP, HTTPS, SSH, and SMTP communications between VMs within the emulated environment.

2.3. Power Simulations

SCEPTRE interfaces with and runs several different power simulation programs (e.g. pypower, PowerWorld, OpenDSS) depending on the use case. These simulations were coupled to the simulated control network to demonstrate the performance of DER grid-support control functions under different cybersecurity architectures, protocols, and additional security features. For these experiments, the distribution model presented in [35] was used but each of the 750 kW PV sites were assumed to be constructed with 10 75 kW PV inverters. When the DER settings were updated in the RTUs, an internal backend ZeroMQ (or ØMQ) [39] network transferred the new settings to the DER devices in the OpenDSS distribution circuit simulation. Similarly, the status of the power system at the location of the DER were transferred to the RTUs using ØMQ when there was a power simulation update.

3. Communication Latency

When cybersecurity features are added to control networks, there is an increase in communication latency from processing data, additional router/switch hops, firewall rules, exchanging keys, binding certificates, performing encryption, or reconfiguring the system. These operations have the risk of adversely affecting real-time grid operations if the delays are significant. Several experiments were conducted to determine the communication latency associated with adding security features to DER networks.

3.1. DER Latency Impact on Power System Operations

As noted in DOE's 2017 report on the *Modern Distribution Grid: Volume III*, the communication timing requirements for DER are on the order of seconds, with typical bandwidth and latency requirements of 10 kbps and 5 seconds, respectively [40]. These communications requirements represent generalized limits on tolerable latencies between the utility and smart inverters. Prior work on transmission-level and distribution-level DER control algorithms provided a more detailed view of the relationship between communication latency and performance. It was found the hierarchical Volt-VAR shift algorithm was effective with latencies up to 20 seconds [41] for distribution circuits, whereas the transmission services were severely impacted with lower latencies. Synthetic inertia experienced a loss of machine synchronism defined by rotor angle separation with latencies between 200-400 ms (depending on the gain) [42]; communications-enabled fast acting imbalance reserve was ineffective if the delay is longer than the time to the frequency nadir (e.g., ~1-10 seconds depending on system inertia) [43]; and communications-enabled DER droop control experienced oscillations with latencies of 110-400 ms (depending on the gain) [44]. These findings all indicate the control algorithm will lose effectiveness with increasing latency, leading to a range of potential problems. Therefore, the selection of cybersecurity defences must not substantially extend communication times.

3.2. Communication Latency Studies

Communication latency is a combination of the encryption time, number of network hops, communication media, and device read/write times. While small improvements in communication time can be made with optimization of encryption algorithms, new router technologies, and faster memory read/write times, these are likely to be minor; DER generate low-priority Internet communications with cost-competitive communication interface boards. Like many other IoT technologies, there is little incentive for DER vendors to invest in performance improvements. In this section, DER latency is dissected to show the addition of security features only increases the latency by a few percent. Therefore, the addition of security features must not substantially impact grid services and,

wherever possible, should be added to DER communication networks to improve the cybersecurity posture of the power system. The following sections investigate latency from non-security factors (geographical separation, physical media, device read/write times) and for security features (encryption, segmentation, and MTD).

3.2.3 Geographical Separation and Physical Media

Phasor measurement unit (PMU) messages between Albuquerque, NM and several geographically distributed locations within the continental United States were used to understand latency impacts of distance and communication media. PMU transit times to Albuquerque were calculated using the GPS timestamp and GPS time at the receiver. The results for communication transit times from sites in Las Cruces, NM (310 km), Pullman, WA (1570 km), and Lubbock, TX (460 km) are shown in Table 1. The connection to Texas was over a dedicated fibre line with minimal network hops, which minimized average communication time. While fibre and copper communications are both extremely fast, fibre has less signal loss, allowing for much longer runs and fewer hops [49]. Conversely, the network routes from PMUs in NM and WA had more routers and switches in the path which slowed transfer times. In general, these results show the architecture (switch and router hops) and communication medium (copper vs. fibre) impact data-in-flight times more than geographic separation [48].

3.2.4 Device Read/Write Times

1000 Modbus read and write times were collected for two commercially available residential-scale DER devices and one controller HIL (CHIL) device [50] at the Distributed Energy Technologies Laboratory (DETL) at Sandia National Laboratories. The SunSpec SVP was used to calculate mean, μ, and standard deviation, σ, for read and write operations. The results are shown in Table 2. Inverter 1 had a large standard deviation for both read and write times. It is not clear if there were internal communication checks or other inverter processes that slowed the responses. Like Inverter 1, Inverter 2—the CHIL device—had a direct Modbus/TCP connection over 1 network hop but responded much faster to both read and write requests. The connection to Inverter 3 included an Ethernet-to-Serial converter in the path to translate Modbus/TCP to serial Modbus. This added an additional delay due to the conversion processing—possibly accounting for some of the larger average communication times for reads and writes. It is believed the variations observed in these results are because the inverters used different protocol stacks, processor hardware, and scheduling techniques for I/O tasks.

3.2.1 Encryption Latency

Per the IEEE 2030.5 and IEEE 1815 requirements, public-key infrastructure (PKI) will be used to encrypt data between the utility and aggregators or DER devices. To authenticate entities, digital certificates—defined by the X.509 standard and registered to a Certificate Authority (CA)—are bound to the asymmetric key of the entities. Authenticated endpoints undergo key exchange to settle on a mutual symmetric key for bulk encryption.

The time to perform the encryption in the devices is highly dependent on the hardware. It is important to note both the value and limitations of the latency results obtained from an emulated system [45], because the absolute latency values are not representative of hardware implemented in the field. However, the relative impacts from applying additional security mechanisms are illustrative and help to provide scale. That is, the speed of the calculations is dependent on the resources available, including processor speed and available memory, which changes depending on the hardware used. IEEE 2030.5 specifies a cipher suite which uses Transport Layer Security (TLS) 1.2, Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) key exchange, Elliptic-Curve Digital Signature Algorithm (ECDSA) signature authentication, and AES-128 bulk encryption. Specifically, the AES-128 CCM8 algorithm operates with 128-bit keys and data blocks in Counter mode with Cipher Block Chaining Message Authentication Code (CBC-MAC)—providing simultaneous encryption and authentication known as Authenticated Encryption with Associated Data (AEAD) and producing an authentication tag of 8 bytes. [46].

In the co-simulation environment, the authentication and key exchange process was handled by SSH BITW devices. Due to the limitations of the co-simulation environment, tests were conducted using RSA for message signing/authentication and AES with CTR/GCM modes for symmetric encryption. Extensive cryptographic benchmarking has been conducted with Crypto++, including throughput and key setup times [47]. The symmetric encryption ciphers employed by SunSpec RTUs are listed Table 3 along with the mean round trip times (RTTs) experimentally observed in SCEPTRE for each cryptographic algorithm with TLS transport security. Cipher-specific RTT results are shown in Figure 2. The encryption process increases the RTT by 1.67-2.05 ms over the unencrypted transfer. While this represents up to an 85% increase in latency, is it only a small increase in the total time to communicate with DER devices. As shown in Table 3 and Fig. 2, increasing AES key lengths decreases the mebibyte/sec throughput because there are more cryptographic processing rounds. AES/GCM and ChaCha20-Poly1305 are authenticated encryption mode ciphers, so the algorithms perform more work than CTR mode; but GCM is efficient and parallelizable so it has similar RTTs to the CTR modes. ChaCha20-Poly1305 is an efficient stream cipher that produces the quickest RTT but has the lowest bandwidth in the cited benchmarks.

3.2.2 Network Topology

A SCEPTRE experiment was created to calculate the increased latency associated with adding network segmentation. The main difference in the topologies was the addition of an extra hop required to break the DER control network into multiple segments. A round trip time (RTT) for the segmented DER network and the flat topology were calculated by pinging the DER from the utility Windows VM. The results for more than 10,000 individual measurements showed the average RRT for the flat network to be 1.56 ms, but the segmented network was 1.82 ms on average [48].

TABLE I
PMU COMMUNICATION TIMES

PMU Data Exchange	Mean (ms)	Std. Dev. (ms)
NM-to-ABQ	78.912	8.906
WA-to-ABQ	67.155	1.585
TX-to-ABQ	36.208	3.237

TABLE II
DER MODBUS READ AND WRITE TIMES

DER	Read μ (ms)	Read σ (ms)	Write μ (ms)	Write σ (ms)
Inverter 1	163.076	26.144	168.380	133.698
Inverter 2	3.032	0.980	1.938	0.911
Inverter 3	165.862	1.056	33.730	0.6583

TABLE III
SYMMETRIC ENCRYPTION CIPHER RTT

Symmetric Cipher & Cipher Mode	Crypto++ MiB/s	Mean SCEPTRE RTT (ms)
AES128-CTR	4525	4.0526
AES192-CTR	3845	4.0662
AES256-CTR	3340	4.3728
AES128-GCM	2789	4.1056
AES256-GCM	Unavailable	4.4290
ChaCha20-Poly1305	499	4.0496
No Encryption	N/A	2.3834

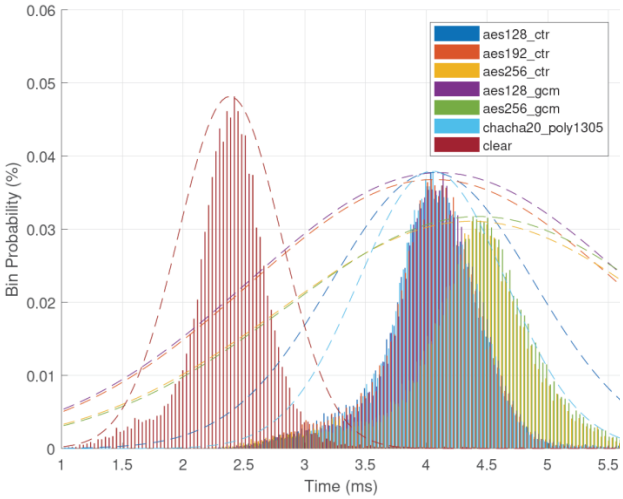

Figure 2: Histogram of round-trip communication time for Modbus with transport security using various symmetric ciphers and cipher modes.

3.2.5 Moving Target Defence

Moving Target Defence (MTD) is a class of technologies that dynamically modify a system environment to create uncertainty for adversaries by overlaying another control network on the publicly addressable one. MTD leverages software defined networking (SDN) to randomize network parameters (IP addresses and ports) and communication paths. It is possible to randomize IP addresses and port numbers at fixed intervals or in response to detected network activity—i.e., dynamic defence. Randomizing IP addresses at a configurable frequency supports evading adversarial discovery. This is meant to thwart the ability of an adversary to conduct reconnaissance and establish communications between devices on the network [51]; MDT has been proven to be effective at increasing the resilience of grid wide area networks against certain types of attacks [52].

An example of this technology is shown in Figure 3. On the left is a utility subnet consisting of an ADMS, Geographical Information System (GIS), and DERMS. On the right, is a collection of DER in a campus or utility/commercial site on a single switch. There is an "IP Generator" computer in the bottom that sends the new IP addresses to the switches in front of actual DER or computation devices. The MTD changes the IP addresses of these switches but the utility-owned and DER nodes retain static IP addresses. Actual implementation would likely require multiple MTD subsystems that independently reconfigure the IP addresses of the utility subnet and DER devices. Since this technology requires a sperate network to be overlaid on the publicly-addressable one, it is likely that DER would require a cellular modem or other out-of-band communication technology to be included in the MTD/SDN overlay.

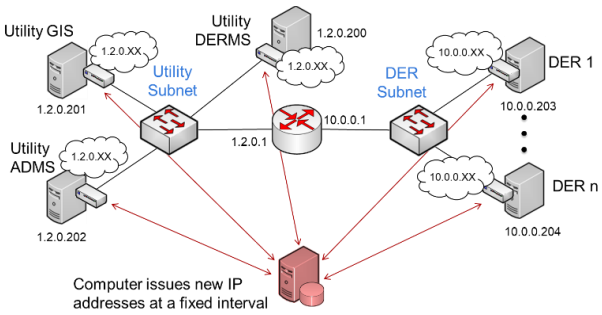

Figure 3: Implementation of Moving Target Defence on a DER communication network.

In prior work, the communication latencies for various MTD modes were determined for different randomization time periods; it was found that MTD increased the average latency by less than 1 ms but caused slightly higher dropout rates (approx. 1 dropout per 33.3 seconds with IP randomization every 3 seconds) [51]. Other approaches to MTD, like path randomization, may increase latency more. A 11.73 ms increase in RTTs for path randomization was reported by Chavez [53].

3.3. Latency Observations

Based on the results for network segmentation, encryption, MTD, geographical separation, and DER read/write times, some observations can be made about the impact to the control system when adding security features. In general, large geographic distances have the possibility of adding 50-100 ms of latency for utility-to-DER communications due to the additional networking equipment (routers and switches) between endpoints. DER read and

write times vary widely; they can be 1 second or larger in some situations. In contrast, network segmentation adds less than 1 ms, encryption adds on the order of 3-5 ms of additional latency, and MTD adds 1 ms. Therefore, for the proposed cybersecurity features, it is not believed they will impact the grid-support service performance since they only contribute a minor percentage of the total latency between the utility and DER.

4. Red Team Assessments

Red teaming is defined as an authorized, adversary-based assessment conducted to strengthen defences through awareness of the potential device or system vulnerabilities. The assessment combined practices from multiple sources: Sandia's Information Design Assurance Red Team (IDART), NIST's Guide to Industrial Control Systems (ICS) Security Guidelines, best cyber security practices, and collective expertise regarding the DER devices and network. These guides informed the methodology that was used for the assessment of the network environments. The rules of engagement were limited to the SCEPTRE experiment network and the HIL device. For each of the environments, the red team assessment focused on identifying and compromising the PV inverters by turning them off, as well as disrupting network communications and modifying grid-supported functions (e.g. Freq-Watt, Volt-VAR, Power-Factor).

The two scenarios investigated on the segmented networks for this assessment were:

1. Public Network Attacker (Outsider) access: This is an intruder who does not have access to the DER device but does have access to one of the ISP routers. This also implies that the intruder is on the perimeter network.
2. Local Attacker (Insider) access: The intruder is on the DER home area network (HAN) with a foothold on any of the network enclaves or subnets.

The adversary is a computer running either a Kali Linux 64-Bit OS or a Window 32-Bit OS with third-party tools. The Kali Linux VM is shown in Figure 1. The network mapper Nmap and OpenVAS vulnerability scanning tools were used to map the network, provided IP identification, detect open ports, host fingerprinting, and discover vulnerabilities on the devices in the network. Packet sniffers—Tcpdump and Wireshark—were used to capture packets and interpret the traffic. SunSpec dashboard application and Simply Modbus monitoring software were used to craft specific protocol traffic to the target devices and replayed using netcat or Python scripts. To eavesdrop on traffic, the network security tool Ettercap was used. Scripts to modify and drop traffic was written using its filter compiler, etterfilter. Hping3 and Flood_router6 were used to deny services/resources to legitimate users.

The SCEPTRE experimental environment testbed contained real and simulated components that are representative of a DER communication system. The simulated inverters were Linux-based, unhardened, and network-connected, much like many commercial DER devices on the market. The simulated routers ran valid routing/firewalling services, but not on actual hardware.

The Emulytics challenges for the red team included a reduction in attack surfaces, no human elements, limitations in hardware, software, and firmware diversity, and limited emulated system complexity to subvert. The biggest challenge was found to be the interactions between the backend processes–SCEPTRE, Phēnix, Minimega, and OpenDSS—because they are a disparate set of tools not originally designed to seamlessly interface together in real time. It was common that the environment needed to be re-initialized to complete all the assessments.

The flat topology was designed to represent a network where the utility communicated to the inverters in a LAN network. The segmented topologies included the same utility to inverter interactions but have added security features controlled by a system owner inside their network. The moving target defence network employed dynamic configuration to obfuscate network and routing parameters. The network topologies for these experiments, though simplified and contrived, are still representative of some real world DER control networks.

4.1. Assessment Approach

The following red team assessments were conducted on each DER control reference architecture:

1. Network Reconnaissance: this phase involved the intruder actively gathering information about the vulnerabilities of the target system. This yielded network information, including IP addresses, MAC addresses, open ports, slave IDs, vulnerable services, and operating systems.
2. Fabrication: this network attack inserted or maliciously replayed fake messages on the network to investigate the confidentiality and integrity of data transfer between the utility and the RTUs.
3. Interruption: this network attack generated a deluge data transmission to render the system unavailable to legitimate users. This test investigated the availability of the RTUs and utility to operate under a DoS attack.
4. Interception: under this attack, data transmissions were eavesdropped, maliciously dropped, delayed or altered while in transit from the utility to the RTUs and vice versa. This test investigated the confidentiality and integrity of data transfers under a man-in-the-middle (MITM) attack.

4.2. Experimental Results

Red team assessment observations and challenges from each SCEPTRE environment are summarized below. Further details of the exposed vulnerabilities are provided in [38].

4.2.1 Flat network without encryption:

Observations*:* Reconnaissance enabled mapping of the network. The routers and inverters were susceptible to DoS attacks. MITM attacks between each inverter and the corporate utility router were possible. Fabricated data was easily replayed to modify grid-support functions on the inverters.

Challenges: None. This environment was the baseline for the assessments.

4.2.2 Flat encrypted network

Observations: Reconnaissance enabled mapping of the network and showed encryption was added via a bump-in-the-wire (BITW) technique. Improper cryptographic implementation enabled replayed register changes to the inverter. DoS and MITM attacks were also successful.

Challenges: On a BITW encryption setup, an attacker intercepting traffic between the BITW endpoints will only see encrypted traffic across any potential attacker-controlled parts of the network, but this challenge was not encountered due to misconfiguration of the encryption tunnel that exposed unencrypted data in some communication paths.

4.2.3 Segmented network without encryption

Observations: The red team were provided two access points, one on the ISP router's subnet (outsider access) which was bereft of inverters and the other access on one of the subnets with a subset of the inverters. Reconnaissance was successful from both access points. From the outsider access, MITM was unsuccessful because there were no addressable inverters. Attempts to pivot using the password-less SSH boxes and deploy MITM were unsuccessful due to Linux package dependencies on the air-gapped SCEPTRE network. That is, the needed tools could not be loaded on the SSH VMs without tearing down and rebuilding the Emulytics environment. MITM was only successful within one local subnet or enclave. However, DoS and replay attacks were successful from both access points.

Challenges: From an outsider position on an emulated network, it was not a target-rich environment. Pivoting into subnets with targets was difficult when hosts did not have the human element and OS vulnerabilities seen in the real world.

4.2.4 Segmented encrypted network

Observations: The red team was provided the same two access points described above. Encrypted tunnels to the utility (Corporate Network) were created to each segmented unencrypted subnet using BITW SSH gateway hosts. Reconnaissance confirmed the encryption tunnel was again misconfigured, with the inverters immediately connected to the ISP router rather than being located behind the SSH box. Placing the inverters behind SSH boxes would have ensured the encryption of data between the inverters and the gateway, thereby eliminating some attack types on the same subnet as the inverters. While MITM was still an available attack when the adversary was on the DER subnet, an outsider without the ability to pivot and deploy tools remains excluded from this attack vector. Again, DoS and replay were successful from both access points.

Challenges: No unique challenges were introduced in this topology.

4.2.5 Segmented, unencrypted network with HIL DER

Observations: Only the outsider access was granted to the adversary in this topology. The HIL device was not on the same subnet as the adversary. Reconnaissance, replay, and DoS attacks were successful. MITM attack was unsuccessful because there were no inverters in the same subnet with the adversary.

Challenges: The HIL inverter was known to have grid-support functions and communicate with UDP. However, while attached to the Emulytics environment, the HIL could not be commanded with netcat UDP packets and the red team did not discover whether this was due to the Emulytics platform translating all traffic through protocol buffers or due to other network effects. Python UDP communication still succeeded in replaying fabricated data.

4.2.6 Flat MTD without encryption

Observations: MTD provided a couple of features that initially inhibited red team traction. Vulnerable switch proprietary protocols running on default switch configurations were exploited for reconnaissance resulting in VLAN information, SDN controller IP addresses, and open ports. DoS attacks on the switch was successful but MITM was not successful.

Challenges: The MTD environment was built with SDN concepts inside an Emulytics platform. This platform is also built on rapid prototyping models of SDN, causing a fusion of certain network surfaces that would have been separated in the real world. For instance, a real MTD system would protect the applications and application plane communications with the interceding control plane, leaving the controller and control plane communications as new attack surface. Conflation of the Emulytics platform and the MTD environment may have contributed to difficulties defining what element were in scope and what new attack surfaces were available.

Finally, the common observation and challenge evident in all the topologies was the abbreviated set of DER Modbus registers in the virtual devices. This artificially limited the attack surface of the simulated inverters.

4.3. Summary

In the assessments of each of the network topologies, the team identified vulnerable areas that could be exploited—mostly due to flaws in system configurations and network implementation. To quantify the impact of the red team on the virtualized communication networks, a scoring rubric was created loosely based on prior assessment work with military microgrids [54-56].

The findings of this assessment are summarized in Table IV. For the CIA (confidentiality, integrity, availability) columns, a scale of 1 to 5 was created to categorize the risk levels. A score of 1 indicated a low risk to all the devices and a score of 5 indicated a high risk to most of the devices. Scores between 2 and 4 indicated an increasing number of compromised devices or system risk. Total scores were summed for a security risk score between 3 to 15. For this defined range, scores between 3-4 where assigned a low risk, scores between 5-9 as medium risk, and scores between 10-15 were assigned as high risk, based on the red team impact on CIA. This was completed for the *theoretical* security posture provided by the defensive components and the as-built system the red team assessed and *quantified*, as indicated in Table IV.

Unfortunately, it is difficult to calculate a power system risk using red team scores from the penetration tests [56-57] because a single vulnerability can compromise the entire DER network and drastically impact the power system. Typically, enterprise cyber teams will establish scoring rubrics to track their cybersecurity posture over time using tools like ATT&CK [58], Nessus/CVSS [59], or STRIDE [60]. In this work, scores were generated for barebones

TABLE IV
THEORETICAL AND ADVERSARY-BASED ASSESSMENT OF DER NETWORK

			Theoretical							Quantified						
			Attacks			Risk Level				Attacks			Risk Level			
Topology	Encryption	Access	DoS	Replay	MITM	C	I	A	Total Score	DoS	Replay	MITM	C	I	A	Total Score
Flat	None	Insider	✓	✓	✓	5	5	5	15	✓	✓	✓	5	5	5	15
Flat	None	Outsider	✓	✓	✓	5	5	5	15	✓	✓	✓	5	5	5	15
Flat	RFC 7539	Insider	✓			1	1	5	7	✓	✓	✓	5	5	5	15
Flat	RFC 7539	Outsider	✓			1	1	5	7	✓	✓	✓	5	5	5	15
Segmented	None	Insider	✓	o	o	3	3	4	10	✓	✓	✓	5	4	5	14
Segmented	None	Outsider	✓			2	2	3	7	✓	✓		5	2	5	12
Segmented + PHIL	None	Outsider	✓			2	2	3	7	✓	✓		5	2	5	12
Segmented	RFC 7539	Insider	✓			1	1	4	6	✓	✓	✓	5	4	5	14
Segmented	RFC 7539	Outsider	✓			1	1	3	5	✓	✓	o	5	2	5	12
Flat MTD	None	Insider	✓			1	1	5	7	✓			1	1	5	7
Seg MTD + WL	RFC 7539	Outsider				1	1	2	4							

- ✓ indicates the attack is possible for all DER devices
- o indicates the attack could succeed for a portion of the DER devices
- WL indicates whitelisting of the MTD network
- RFC 7539 is the IETF Protocol for ChaCha20 stream cipher and Poly1305 authenticator

environments and strictly represented a gradation of security practices indicating quality of defences and number of ICS assets that were subverted [61], but not a measure of time/effort required to affect OT network or power systems operations. The scores were partially advised using the Common Vulnerability Scoring System (CVSS) methodology that ranks vulnerabilities based on ease and severity of exploitation [62]. The following rubric was used for the CIA scoring:

- Confidentiality:
  - 1: None of the DER data traversing the network was readable by the red team
  - 2: Data from 1-5 DER devices were readable by the red team
  - 3: Data from 5-10 DER devices were readable by the red team
  - 4: Data from 11-19 DER devices were readable by the red team
  - 5: All DER data traversing the network were plaintext and accessible by red team
- Integrity:
  - 1: Red team could not replicate or manipulate DER traffic
  - 2: Red team successfully conducted replay attacks on 1-19 DER devices
  - 3: Red team successfully conducted replay attacks on all 20 DER
  - 4: Red team successfully conducted MITM attacks on 1-19 DER
  - 5: Red team successfully conducted MITM attacks on all 20 DER
- Availability:
  - 1: Red team DoS attacks did not affect OT networking
  - 2: Red team DoS attacks affected 1-5 DER
  - 3: Red team DoS attacks affected 5-10 DER
  - 4: Red team DoS attacks affected 11-19 DER
  - 5: Red team DoS attacks affected communications to all DER

Comparing the theoretical vs. quantified cybersecurity risks in Table IV, clearly proper security feature implementation is essential to gain the advantages offered by these technologies. In the case of implementation errors or oversights—as were common in these assessment environments—minimal additional effort was required by the adversary to sidestep the defences and subvert the DER control network. Any implementations that did not receive scores of 1 across the board should be considered exploitable and/or at risk for disruption. Thus, all topologies the red team assessed represent some power system risk.

Based on the results of the assessments, the following recommendations are provided:

1. Denial of service attacks are difficult to prevent (as evidenced by the March 2019 attack on sPower [63-64]). Aggregators/utilities should regularly patch their networking equipment and implement firewall whitelists to mitigate these attacks.
2. Segmentation makes it difficult for the adversary to move between subnets. Flaws in system configuration and networking implementation enabled manipulation of all DER devices.
3. Implementing the right encryption tunnel between DERMS and DER drastically reduces the risk of replay and MITM attacks.
4. It is important that developers add layers of defence by reviewing and pushing secure code to applications to prevent common attacks.
5. MTD has the potential to drastically improve security for DER networks, but this is still an area of research.

5. Conclusions

This work studied the trade-offs between communication quality of service (QoS) metrics and cyber resilience for a grid services provided by a distributed energy resource (DER) control network. To effectively provide grid services (e.g., voltage regulation, frequency reserves,

protection, etc.), certain tolerances for latency, networking dropouts, and communication availability were previously determined. Using those communication requirements as a reference, the impact of network segmentation, encryption, and MTD were calculated. It was found that each of the three security features generate minimal increases in latency compared to unsecured topologies, and therefore would not adversely impact grid control operations, while substantially increasing the theoretical cybersecurity posture of the control network. And while this additional security comes with some operational overhead for maintaining the necessary infrastructure, it is believed the security benefits outweigh those costs. It is noted from the red team assessments, however, that improper implementation of the security features will only provide a false sense of security and dedicated adversaries will find ways to evade these defences.

Further work is recommended to assess the security features of other communication protocols, such as IEEE 2030.5, for better understanding of the security posture in soon-to-be-fielded DER control environments. The inclusion of aggregator services in the DER networks should also be considered for future SCEPTRE red team assessments, as these are commonly used to pass control and measurement data to/from utilities. Lastly, the full lifecycle of DER operations should also be analysed from a security perspective and include establishing firmware update procedures, patching requirements, and recommended maintenance schedules.

6. Acknowledgements

The authors would like to thank several researchers for helping stand up the SCEPTRE environment. Matthew J. Reno provided significant support in integrating OpenDSS into SCEPTRE and providing the PMU latency data; Adrian Chavez and Will Stout stood up the MTD environment; and Derek Hart and Jordan Henry provided invaluable assistance in the SCEPTRE development efforts. Keith Schwalm created the network topologies and Bryan T. Richardson constructed the DER-OpenDSS ØMQ interface, built the OpenDSS SCEPTRE provider, and debugged the HIL implementation.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

This work was completed within the “Secure, Scalable Control and Communications for Distributed PV” project funded by the US Department of Energy Solar Energy Technologies Office under Award DE-EE0001495-1593.

7. References

[1] Idaho National Laboratory, ‘Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Mission Support Center Analysis Report,’ (INL/EXT-16-40692), Aug 2016.
[2] Smith, R., ‘How a U.S. Utility Got Hacked,’ (The Wall Street Journal), 30 Dec 2016.
[3] Smith, R., ‘Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say,’ (The Wall Street Journal), 23 June 2018.
[4] Caine, P., ‘Russian-Backed Hackers Infiltrating US Power Grid,’ (WTTW), 7 Aug 2018.
[5] Wilber, D.Q., ‘Russian Malware Found on Vermont Electric Utility Laptop’ (Los Angeles Times, CA), 31 Jan 2017.
[6] Bradbury, D., ‘Staff Dust Off Their Typewriters After Malware Attack’ (Naked Security), 1 Aug 2018.
[7] Kirkpatrick, D., ‘British Cybersecurity Chief Warns of Russian Hacking’, (The New York Times), 14 Nov 2017.
[8] Zetter, K., ‘Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid’, (Wired), March 3, 2016.
[9] Greenberg, A., ‘How an Entire Nation Became Russia's Test Lab for Cyberwar’, (Wired), 20 June 2017.
[10] Greenberg, A., ‘Crash Override: The Malware That Took Down a Power Grid’, (Wired), 12 June 2017.
[11] Campbell, R.J., ‘Electric Grid Cybersecurity’, (Congressional Research Service), 4 Sept 2018.
[12] Riley, M., Dlouhy, J., Gruley, B., ‘Russians Are Suspects in Nuclear Site Hackings, Sources Say’, (Bloomberg), 6 July 2017.
[13] Perlroth, N. ‘Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say’, (The New York Times), 6 July 2017.
[14] Perlroth, N., Sanger, D.E., ‘Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says’, (The New York Times), 15 Mar 2018.
[15] Greenberg, A. ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, (Wired), 22 Aug 2018.
[16] E-ISAC: ‘Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case’, March 18, 2016.
[17] Solar Energy Industries Association and GTM Research: ‘U.S. Solar Market Insight Q3 2018’, 12 September 2018.
[18] U.S. Energy Information Administration: ‘U.S. Battery Storage Market Trends’, May 2018.
[19] Page, S., ‘Hawaii Will Soon Get All of Its Electricity from Renewable Sources’, (Think Progress), 7 May 2015.
[20] Penn, I., ‘California Invested Heavily in Solar Power. Now There's So Much That Other States Are Sometimes Paid to Take It’, (LA Times), 22 June 2017.
[21] IEEE Std. 1547-2018: ‘IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces’, (Institute of Electrical and Electronics Engineers, Inc.), New York, NY, 15 Feb 2018.
[22] IEEE Std. 2030.5-2013: ‘IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard’, 11 Nov 2013.
[23] SunSpec Alliance, Common Smart Inverter Profile: IEEE 2030.5 ‘Implementation Guide for Smart Inverters, Version 2’, Mar 2018.
[24] Pacific Gas and Electric Co., Electric Rule No. 21: ‘Generating Facility Interconnections’, Filed with the CPUC, 8 June 2017.
[25] ‘North American Electric Reliability Corporation, Critical Infrastructure Standards’, accessed 11-14-2018, URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[26] Cordeiro, P., Obert, J., Johnson, J., ‘Recommendations for Trust and Encryption in DER Interoperability Standards’, (Sandia Technical Report), Dec 2018.
[27] Lai C., Jacobs, N., Hossain-McKenzie, S., Carter, C., Cordeiro, P., Onunkwo, I., Johnson, j., ‘Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators’, (Sandia Technical Report, SAND2017-13113), Dec 2017.
[28] ‘SunSpec Alliance, SunSpec DER Cybersecurity Workgroup’, accessed 11-14-2018, URL: https://sunspec.org/sunspec-cybersecurity-workgroup/
[29] Saleem, D., Carter, C., ‘Certification Procedures for Data and Communication Security of Distributed Energy Resources’, (NREL Technical Report), 2018 (forthcoming).
[30] Johnson, J., ‘Roadmap for Photovoltaic Cyber Security’, (Sandia Technical Report, SAND2017-13262), Dec 2017.
[31] Jacobs, N., Johnson, J., ‘SCEPTRE: Power System and Networking Co-Simulation Environment’, (Workshop on Co-Simulation Platforms for the Power Grid, LBNL, Berkeley, CA), 21 May 2018.
[32] ‘Minimega, A distributed VM management tool’, accessed 11-14-2018, URL: minimega.org
[33] ‘SunSpec Alliance, Specifications & Information Models’, accessed 11-14-2018, URL: https://sunspec.org/about-sunspec-specifications/
[34] ‘SunSpec Alliance, SunSpec System Validation Platform (SVP)’, accessed 11-14-2018, URL: https://sunspec.org/sunspec-svp/
[35] Quiroz, J.E., Reno, M.J., Lavrova, O., Byrne, R.H., ‘Communication Requirements for Hierarchical Control of Volt-VAr Function for Steady-State Voltage’, (IEEE ISGT 2017, Arlington, VA), 23-26 April 2017.
[36] Reno, M., Quiroz, J., Lavrova, O., and Byrne, R., ‘Evaluation of Communication Requirements for Voltage Regulation Control with

Advanced Inverters', (Proceedings of the IEEE North American Power Symposium, Denver, CO), 18-20 Sept 2016.
[37] Stamp, J., Veitch, C., Henry, J., et al., 'Microgrid Cyber Security Reference Architecture (V2)', (Sandia National Laboratories Technical Report SAND2015-9711), Nov 2015.
[38] Onunkwo, I., Cordeiro, P., Wright, B., Jacobs, N., Lai, C., Johnson, J., Hutchins, T., Stout, W., Chavez, A., Richardson, B.T., Schwalm, K., 'Cybersecurity Assessments on Emulated DER Communication Networks', (SAND2019-2406), March 2019.
[39] 'ZeroMQ', accessed 11-14-2018, URL:http://zeromq.org/
[40] US DOE OE, 'Modern Distribution Grid: Decision Guide Volume III', 28 June 2017.
[41] Reno, M.J., Quiroz, J.E., Lavrova, O., Byrne, R.H., 'Evaluation of communication requirements for voltage regulation control with advanced inverters', (NAPS), Sept 2016.
[42] Concepcion, R., Wilches-Bernal, F., Byrne, R.H., 'Effects of Communication Latency and Availability on Synthetic Inertia', (2017 IEEE ISGT, Washington, DC, pp. 1-5.) April 23-26,2017
[43] Wilches-Bernal, F., Concepcion, R., Neely, J., Byrne, R., and Ellis, A., 'Communication Enabled – Fast Acting Imbalance Reserve (CE-FAIR)', (IEEE Trans. Power Systems, vol. 33, no. 1, pp. 1101-1103), Jan. 2018.
[44] Wilches-Bernal, f., et al., 'Impact of Communication Latencies and Availability on Droop-Implemented Primary Frequency Regulation' (49th NAPS, Morgantown, WV), Sept 2017.
[45] Jones, S.T., Gabert, K.G., Tarman, T.D., 'Evaluating Emulation-based Models of Distributed Computing Systems', (SAND2017-10634), Aug 2017.
[46] Lum, G., 'IEEE 2030.5 Security Overview', (DER Cybersecurity Workgroup Webinar), 24 July 2018.
[47] 'Crypto++ 6.0.0 Benchmarks. Crypto++'. Accessed 12 Dec 2018. URL: https://www.cryptopp.com/benchmarks.html
[48] Johnson, J., 'Secure, Scalable Communications for Distributed PV – Final Technical Report,' Sandia Technical Report SAND2019-0495 R, 15 Jan 2019.
[49] Babani, S., Bature, A.A., Faruk, M.I., Dankadai, N.K., 'Comparative Study Between Fiber Optic And Copper In Communication Link,' (International Journal of Technical Research and Applications), Vol. 2, No. 2, pp. 59-63, March-April 2014.
[50] Johnson, J. Ablinger, R., Bruendlinger, R., Fox, B., and Flicker, J., 'Design and Evaluation of Sunspec-Compliant Smart Grid Controller with an Automated Hardware-in-the-Loop Testbed,' (Technology and Economics of Smart Grids and Sustainable Energy,) Vol. 2, December 2017.
[51] Chavez, A.J., Hamlet, J.R., Stout, W.M.S., 'Artificial Diversity and Defense Security (ADDSec) Final Report', (SAND2018-4545), April 2018.
[52] Hossain-McKenzie, S., Lai, C., Chavez, A.R., and Vugrin, E., 'Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense', (44th IECON), Washington DC, 2018.
[53] Chavez, A.R., Stout, W.M.S., and Peisert, S., 'Techniques for the dynamic randomization of network attributes', (2015 International Carnahan Conference on Security Technology (ICCST) pp. 1-6), Taipei, 2015.
[54] Roley, R., 'Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)', (Cyber Security Metrics Workshop, Rome, NY), 12 Nov 2014.
[55] Horton, B.R., 'Cybersecurity Metrics: A Red Team Perspective', (2nd ITEA Cyber Security Workshop), 24 April 2015.
[56] Sandia National Laboratories: 'Red Team Metrics Quick Reference Sheet', (SAND2017-9681 TR), 2017.
[57] Baiardi, F., 'Avoiding the Weaknesses of a Penetration Test,' (Computer Fraud & Security), Vol. 2019, No. 4, pp 11-15, 2019.
[58] MITRE, 'ATT&CK,' Accessed 23 Dec 2019, URL: attack.mitre.org.
[59] Tenable, 'Nessus,' Accessed 23 Dec 2019, URL: tenable.com/products/nessus
[60] Shostack, A. 'Threat Modeling: Designing for Security.' Wiley, 2014.
[61] Wood, B. J. and Duggan, R. A., 'Red Teaming of advanced information assurance concepts,' (DARPA Information Survivability Conference and Exposition, Hilton Head, SC), vol. 2, pp. 112-118, 2000.
[62] FIRST.Org, Inc, 'Common Vulnerability Scoring System v3.1: User Guide,' Accessed 23 Dec 2019, URL: https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf
[63] Sobczak, B. 'First-of-a-Kind U.S. Grid Cyberattack Hit Wind, Solar,' (E&E News), 31 Oct 2019.
[64] Walton, R., 'First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say,' (Utility Dive), 4 Nov 2019.

Appendix A: Network Topologies

The construction of the networking topologies in SCEPTRE required programming different custom-built VMs running open-source software and emulators. The flat, encrypted environment, shown in Fig. 4, established an encrypted tunnel between the utility corporate network subnet (192.168.0.0/24) and the DER OT network (75.75.128.0/24) with two Vyatta routers running AutoSSH. This was intended to prevent the red team from seeing plaintext DER network traffic from their connection at the ISP router.

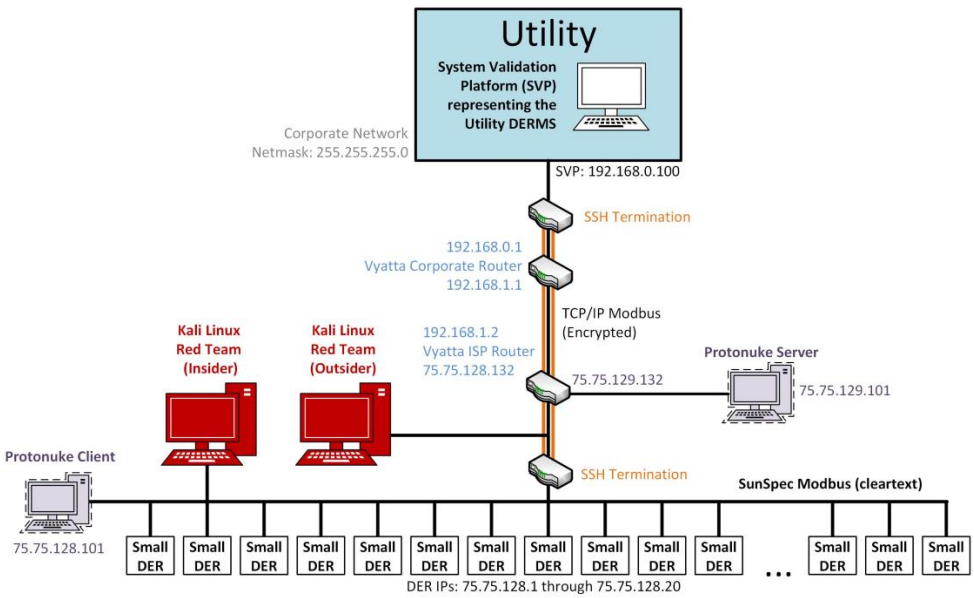

Figure 4: SCEPTRE flat encrypted network topology.

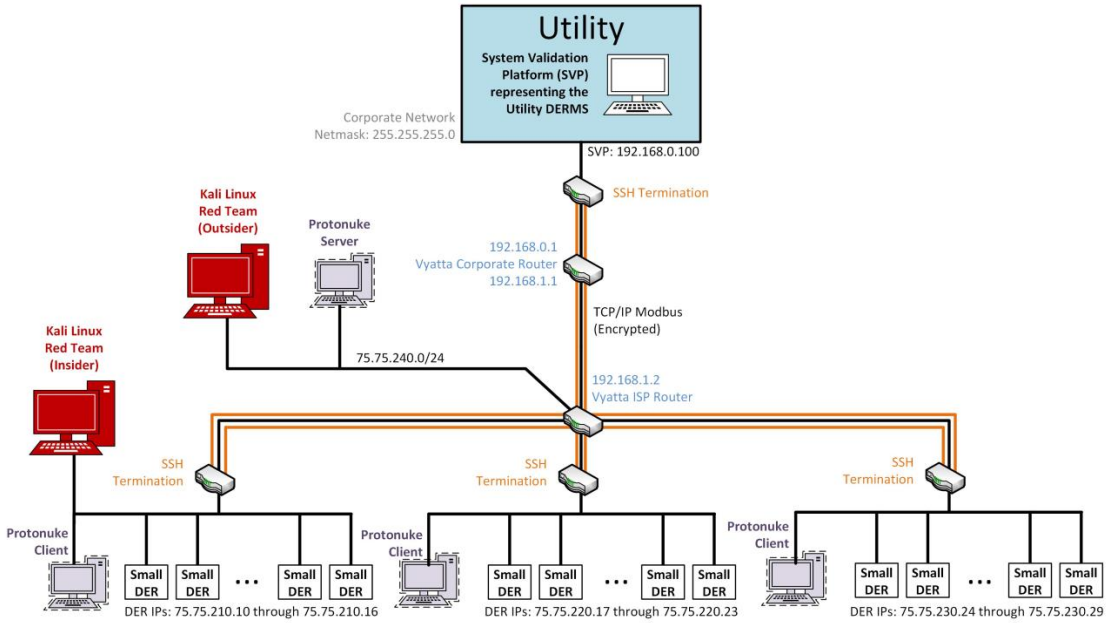

Figure 5: SCEPTRE segmented encrypted network topology.

However, the red team was still able to issue Modbus commands to the DER devices from their location on the network.

Fig. 5 shows the segmented, encrypted topology with three DER enclaves that exchange encrypted data with the utility DERMS. In this topology, no firewall rules were implemented at the segment boundaries, so the red team was once again able to issue commands directly to the DER but unable to see the utility-to-DER communications in the other segments. The addition of strict firewall rules would greatly improve the cybersecurity resilience of these topologies.