Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5

Preprint

Partha S. Sarker,[1] V. Venkataramanan,[2]
D. Sebastian Cardenas,[1] A. Srivastava,[1] A. Hahn,[1]
and B. Miller[3]

1 Washington State University
2 Massachusetts Institute of Technology
3 National Renewable Energy Laboratory

Presented at MSCPES 2020 (8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems)
April 21, 2020

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-76064
October 2022

Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5

Preprint

Partha S. Sarker,[1] V. Venkataramanan,[2]
D. Sebastian Cardenas,[1] A. Srivastava,[1] A. Hahn,[1]
and B. Miller[3]

1 Washington State University
2 Massachusetts Institute of Technology
3 National Renewable Energy Laboratory

Suggested Citation
Sarker, Partha S., V. Venkataramanan, D. Sebastian Cardenas, A. Srivastava, A. Hahn, and B. Miller. 2022. *Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5D00-76064. https://www.nrel.gov/docs/fy23osti/76064.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-76064
October 2022

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported by the Laboratory Directed Research and Development (LDRD) Program at NREL. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via www.OSTI.gov.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5

Partha S. Sarker, *Student Member, IEEE,* V. Venkataramanan, *Member, IEEE*,
D. Sebastian Cardenas, *Student Member, IEEE,* A. Srivastava *Senior Member, IEEE,*
A. Hahn, *Member, IEEE,* and B. Miller, *Member, IEEE*

***Abstract*—The development of more resilient grids is an ongoing effort that has attracted multiple participants. Within this context, Distributed Energy Resources, along with transactive energy mechanisms are being considered as the key driving technologies. Yet their under-laying communication capabilities might introduce additional cybersecurity risks that must be analysed. This paper proposes a cyber-physical microgrid testbed using OpenDSS, Mininet and IEEE 2030.5 that can be used to study the grid's cyber-resilience under various scenarios. For critical microgrid installations, it is essential that the critical loads are served in spite of multiple contingencies. A resiliency analysis is proposed for a military microgrid to study its performance with these contingencies and the results are analyzed.**

***Index Terms*—Cyber-attacks, industrial control, cyber-physical systems, microgrid automation, defense microgrid, cyber-vulnerabilities, SCADA, CVSS, resiliency.**

I. Introduction

Information technology (IT) security problem is constantly evolving, and securing assets using a single technology is not a feasible or recommended. It is also not possible to guarantee cyber security under all operating conditions, as new vulnerabilities and exposures are found everyday. This weakness in terms of cyber security becomes a bigger issue when critical infrastructure is considered, such as military/defense installations, emergency support services and more. Moreover, most of the works related to the IT security problem ignore the underlying physical system constraints. For example, in [1] the authors talk about the device vulnerabilities deployed within microgrids. However, it only focuses on improving device-level security and ignores the effects on the microgrid's capability of serving critical loads in presence of an attack. As we acknowledge that complete security can rarely be achieved, continuous operation of critical infrastructure in degraded condition under multiple contingencies becomes important. Resiliency analysis can play a vital role to address these problems [2].

Self-forming microgrids are often seen as the next logical step towards achieving resiliency at the distribution level. Such a revolutionary approach is in part possible due to the wide, and quick adoption of Distributed Energy Resources (DERs) that has occurred in recent years. Such systems, are currently re-defining the way that energy is generated and delivered. With some systems, experiencing events in which DER's supply the entire demand [3].

Nevertheless, DER-based generation introduces undesirable behaviours, such as unintentional islanding and reverse power flows. To reduce these issues, standardization bodies have updated interconnection requirements as well as operational guidelines. In particular, the Smart Inverter Working Group (SIWG) developed the *grid support functions* which allow DER's to modify their parameters according to locally observed conditions. These functions were integrated into Common Smart Inverter Standard (CSIP) [4] and utilize IEEE 2030.5 as its communication protocol. CSIP can support time and location driven rules (a.k.a. *programs*) that can be remotely pushed to end devices based on the utilitys needs [5]. Microgrids can leverage the IEEE 2030.5 capabilities to optimize DG dispatch by pre-scheduling programs that are condition-aware and site-specific. This provides superiority over other protocols like ZigBee commonly utilized in literature [6], [7]. Furthermore, IEEE 2030.5 allows the devices to transmit data using a variety of physical mediums, including public networks such as the Internet, while protecting the contents from unauthorized eavesdropping by requiring the use of Transport Layer Security (TLS).

Despite the built-in security mechanisms of IEEE 2030.5, implementation errors can lead to potential vulnerabilities which can be exploited to disrupt the operation [8]. Resiliency studies can help to quantify and reduce these risks. Key contributions of the presented work include:

- Testbed for exploring the IEEE 2030.5 standard for microgrid and DERs interface for cybersecurity and resilience analysis
- Propose cyber-physical resiliency framework for critical microgrids
- Analyze cyber-physical resiliency for a military microgrid multiple contingencies

Partha S. Sarker, D. Sebastian Cardanes, A. Srivastava and A. Hahn are with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163 USA. (E-mail: anurag.k.srivastava@wsu.edu)

V. Venkataramanan is currently a post-doctoral research associate with MIT, and B. Miller is with the National Renewable Energy Lab (NREL) (E-mail: Brian.Miller@nrel.gov). We would like to thank Dr. K. S. Sajan for his technical support. We acknowledge financial support from NREL through the Power Systems Engineering Research Center (PSERC) to conduct this work. This material is partially supported by the Department of Energy under Award Number DE-OE0000780.

II. CYBER-PHYSICAL MODELING OF IEEE 2030.5

Utilities continue to face new challenges. Among the key challenges is the ability to manage behind-the-meter DER installations. To assist with this task, IEEE 2030.5 was expanded to support grid-aware, rule-based DER scheduling-programs. These programs can be used to establish ride-through settings, define islanding schemes, or schedule power production among other features. CSIP is able to perform these tasks by using a stateless text-based protocol (*REpresentational State Transfer*, REST) [5]. The protocol operates at the application-level, on top of the Secure Hypertext Transfer Protocol (HTTPS), this implies that it can be deployed over wide-area networks such as the Internet.

CSIP is an application-level protocol that runs on top of the Hypertext Transfer Protocol Secure (HTTPS). It therefore, inherits all the underlaying network security mechanisms provided by VPNs and/or Firewalls. Furthermore, CSIP mandates the use of Transport Layer Security (TLS 1.2), a security suite which provides authentication mechanism for all participants while maintaining secrecy [9]. The REST Application Programming Interface (API) can additionally isolate messages between multiple DER units without end-device intervention, creating simplified, virtual point-to-point connection between the server and the end-device, this isolation can reduce both the end-device computational requirements and the amount of data being received.

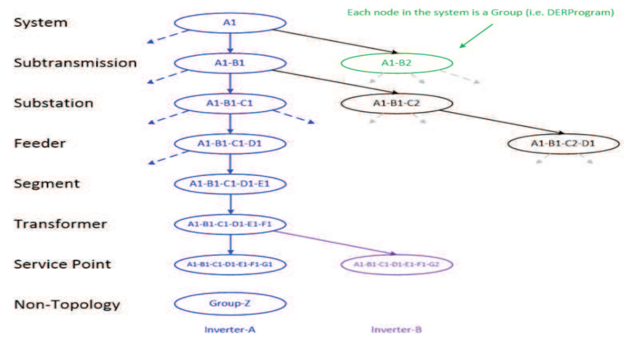

Fig. 1. Hierarchical IEEE 2030.5 architecture [4].

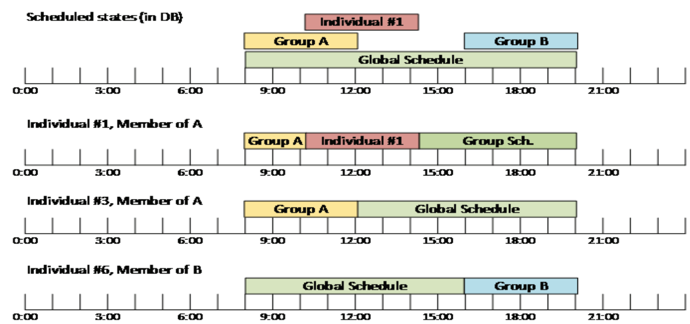

Fig. 2. Rule arbitration process in a 2D timeline [4]

A. REST Architecture

The CSIP API uses an XML container as its data envelope. It provides a standardized and stateless access mechanism that can parsed with little-or-no computational overhead. Furthermore, clients are expected to transverse a tree-like REST architecture while ignoring unsupported leaf-items. This approach will enable future upgradeability by inserting new configuration nodes as needed. In addition, the protocol can be configured in client-querying mode or server-side subscription systems that can help with scaling issues [10].

B. DER Programs/ Solutions

The REST API allows the server to distribute unique programs to each field device by filtering its response according to each client's location and current grid state. In a typical case, the utility or grid operator will first perform a variety of studies to identify problems and solutions, then it will generate a set of device-level programs that will be distributed by the server when the scenario presents itself. Since the solutions to address specific scenarios may require system-level or device-level actions, the protocol allows to store the programs (solutions) in a hierarchical manner (see Fig. 1).

The hierarchical model is based on the Common Information Model (CIM), which is an object-oriented paradigm that is commonly used to represent the electrical connectivity [11]. The CIM stores configuration settings, as well as programs inside predefined data structures that are device-specific. The stored programs are referred as *function sets* and perform device-specific tasks such as metering, demand response, generation scheduling and file transferring functions. An assemble of functions which dictate the behaviour of individual units are referred as *device programs*.

C. Function Sets

The IEEE 2030.5 standard is designed to integrate multiple technologies and thus supports device-specific functions that can be accessed by transversing the REST tree. For PV-based DER devices the core functions are defined by CSIP. The basic set of available functions include:

a) DERControlEvents This function allows the responsible party to adjust the inverter response to grid events such as voltage and frequency ride through and other frequency, volt-dependent curves (grid support functions).

b) Status This function allows the responsible party to get the operational status, device ratings and alarm states.

c) Subscription mechanisms These dictates if the device is to query or to use a subscription-based access mode. It includes the timing characteristics such as, connection timeouts, refresh rates and fallback time-outs.

D. Scheduling logic

As mentioned earlier, CSIP allows time-based and location-aware scheduling capabilities. In order to determine *rule precedence* a time-based 2-D timeline is followed, with precedence given to downstream elements (e.g. transformers) vs those upstream (system-level). An example of this rule-clearing mechanisms is given in Fig. 2.

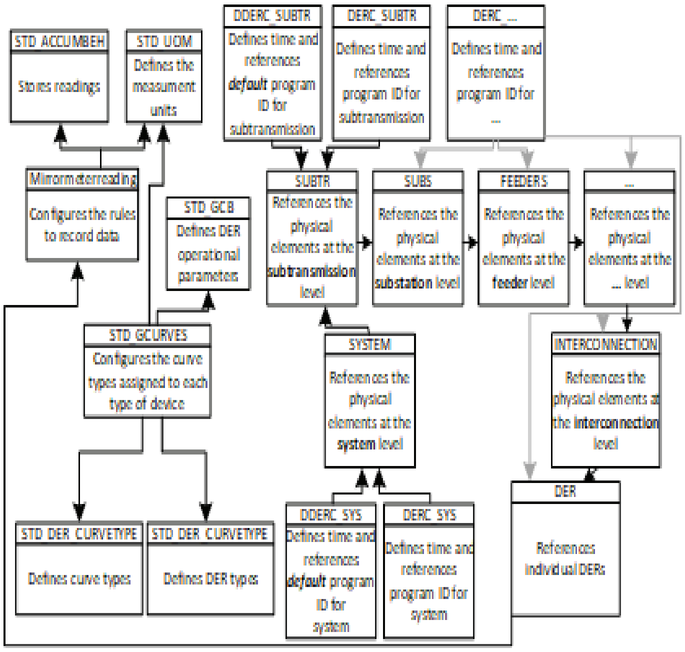

Fig. 3. Database Overview

III. Testbed Implementation and Interface

In order to evaluate the physical effects of a cyber attack on the IEEE 2030.5 protocol a co-simulation platform is required. For this work, OpenDSS was selected due to unique features and available support for PV/Inverter modeling in distribution networks. While Python and PHP were selected for the cyber-layer due to their existent libraries and ample user bases. Fig. 4 shows an overview of the developed architecture, with the next subsections explaining each sub-component.

A. Physical layer simulation: OpenDSS

OpenDSS is a power system simulation platform geared towards distribution systems. It includes the necessary modules required to study the effects of DER integration on unbalanced systems. The OpenDSS platform supports a communication interface (COM) that can be used to simulate time-dependent solutions.

B. REST Server

A REST server that replicates the IEEE 2030.5 functionality was developed in PHP. The service is connected to a database (DB) engine which stores the configurations, filtering functions, as well as the triggers that replicate a fully-functional CSIP environment. An overview of the DB architecture is shown in Fig. 3.

C. REST Clients

A set of virtual DER devices were developed to replicate the data traffic occurring during a REST operation. These virtual clients are hosted inside a network simulator (mininet) and connect to the Python COM server. With this layout it is possible to receive commands from the REST service and to simulate their effect on the OpenDSS platform via the Python COM server.

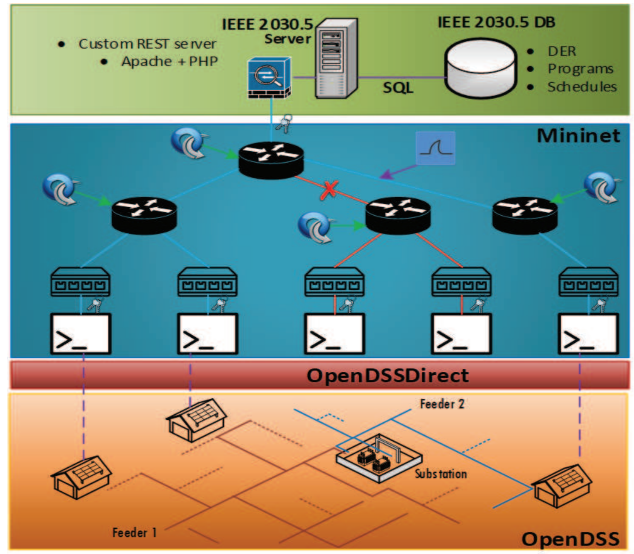

Fig. 4. Block Diagram of Testbed of Interconnected Simulators

D. System Integration

In Fig. 4, an overview of the assembled system is presented. As it can be observed multiple virtual DER devices can be simultaneously connected. These devices establish a direct connection to the REST server over a Mininet environment. Therefore, these links can be individually inspected or intercepted to further analyze their cyber-security properties.

E. Mininet Integration

Mininet is a set of tools designed to simulate realistic virtual networks under a single physical system. Under the Mininet environment, a pool of virtual hosts are connected by using software defined (SDN) switches that can route traffic by using software-defined rules. The rules can be written in high-level languages to replicate events such as network congestion, link malfunctions and lost packages.

In the Mininet environment each virtual host is a network-isolated environment where low-level communication calls are re-routed to the Mininet handlers, this allows the hosts to access all the host system resources (i.e. filesystem, IO devices) in a transparent manner while network communications are silently re-routed. Each of the virtual host network adapters is then connected via SDN to the appropriate switches, where the network simulation process can be executed. In this work the simulator uses a Network Address Translation (NAT) layout. The NAT switch routes the traffic between several virtual hosts and a local IEEE 2030.5 server. The switch replicates the connectivity characteristics of multiple DER devices connected across wide area networks (aka the Internet). Thanks to this approach, different routing mechanisms as well as disrupting events can be simulated to evaluate the DER response in case of less-than-ideal network conditions.

IV. Cyber-Physical Resiliency Metric

Cybersecurity awareness is based on the resiliency metric which is formulated by further developing our previous work on Cyber-Physical Resiliency (CyPhyR) [12]. Besides graph theoretic properties of a power system network, physical attributes are also considered along with data from cyber components while formulating the metrics.

Various feasible configurations of the microgrid are derived based on a shortest path algorithm, and their feasibility is verified using power flow constraints. For all the feasible configurations, the following factors are considered to contribute to the physical resiliency of a microgrid.

Topological Factors:

1) Algebraic Connectivity: network robustness which increases as the algebraic connectivity of the network increases.
2) S-Metric: measures how interconnected the nodes are in the network.
3) Link Density: portion of the potential connections in a network that are actual connections.

Physical Factors:

1) Source Redundancy: the total number of energy source available in the operating configuration.
2) Probability of Availability: probability of supplying the critical load from different sources.
3) Load Fed: the total number of load is being fed during operation.
4) Switching Operations: total number of switching operations required to create the reconfigured network.

The user can modify these factors, and the weights assigned to them in computing the physical resiliency according to the requirements. The quantification of resiliency is done based on Choquet Integral (CI) as it can be formulated as multi-criteria decision making (MCDM) problem [12]. CI combines all the above factors considered and assign weights for all these criteria and come up with a single value for physical resiliency of a particular configuration.

From the cyber network side, Common Vulnerability Scoring System (CVSS) of the cyber components of the microgrid and their impact on the on system due to their position in the network and exploitability are considered in resiliency calculation. For each device maximum values for impact and exploitability is considered, and then using its position in the microgrid network its impact potential is calculated. Central point dominance otherwise called betweeness centrality is used to calculate the criticality of the node and edge in the network and here for a particular switch, edge centrality E_B is calculated by,

$$E_B(e) = \sum_{j \neq d \neq k} \frac{\sigma_{jk}(e)}{\sigma_{jk}} \quad (1)$$

where, $\sigma_{jk}(e)$ is the number of paths that pass through edge e, and σ_{jk} is the total number of shortest paths from node j to k.

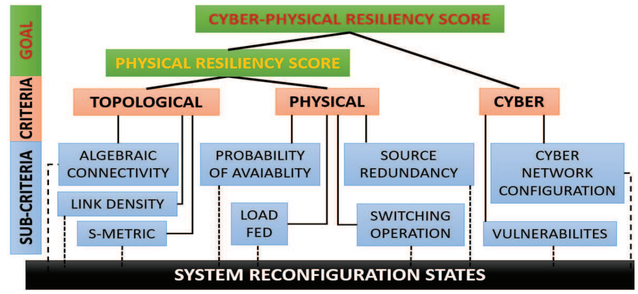

Fig. 5. Cyber-Physical Resiliency Calculation

To relate the impact of cyber components to the physical system, environmental impact score is introduced. This is the change in the physical resiliency value from the base configuration to the new configuration due to attack on cyber components. Lastly, controllablilty score is defined based on the number of affected nodes for availability and integrity based attacks, and determines what portion of the system is available for reconfiguration.

Finally, using above described scores cyber-physical resiliency score is calculated using Eqn. 2 to study impact each device can cause.

$$\begin{aligned} Cyber{-}physical\ resiliency = CVSS \times E_B(e) \times \\ Environmental Impact \times Controllability \end{aligned} \quad (2)$$

As the factors affecting resiliency are in different scales and units, each parameter is individually normalized by using a theoretical maximum for each value as the standard. Hence the maximum cyber-physical resiliency score would theoretically be the maximum possible score that can be achieved by the system. Similar lower bound for the score can also be calculated. An overview of the cyber-physical resiliency score formulations is shown in Fig. 5.

V. Test System and Results

In this section the aforementioned resiliency metric and IEEE 2030.5 simulation tool are used to evaluate a sample system. The results indicate that there exists room for improvement.

A. Test System description

The Miramar microgrid, a defense installation in Miramar, California is shown in Fig. 6. The system parameters are,

1) 6.4 MW power plant with 1.5 MW battery,
2) 3.2 MW landfill gas power plant,
3) Hundreds of buildings with critical loads, individual backup generators and solar PV which we assumed to be of 1.5MW of total capacity for this study,
4) Motor operated switches to disconnect non-critical feeder sections,
5) Control facility and Ethernet fiber network,
6) Bidirectional electric vehicles.

The Miramar system has 8 total feeders. Voltage level are assumed 13.8KV for the primary feeders connecting to distribution transformers and 4.2KV for the secondary feeders.

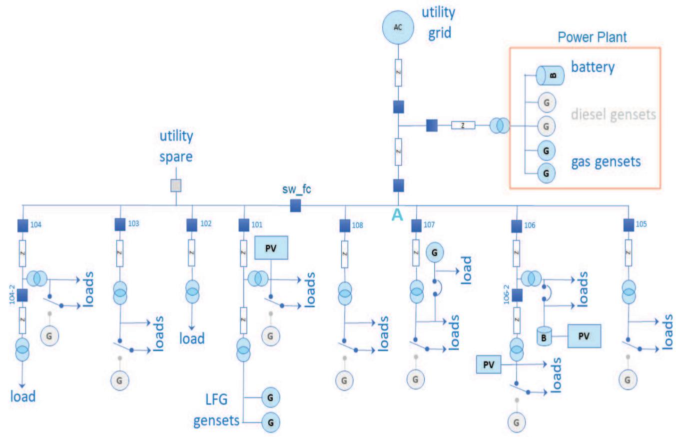

Fig. 6. Miramar Microgrid Model

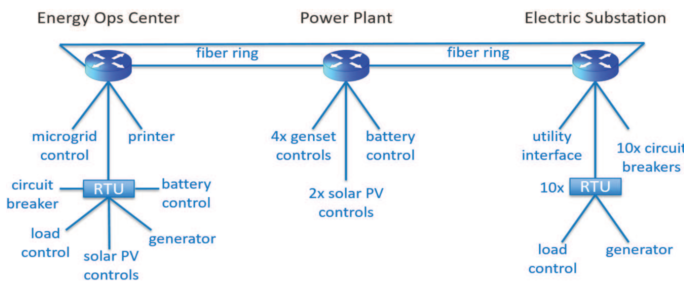

Fig. 7. Communication Model for Miramar Microgrid

It also has 2 machine operated SCADA switches, creating a total of 10 “zones” of power. The control center for the system is in a zone with a grid forming inverter which ensures it does not lose power. Though the Miramar system has a variety of generation sources and some individual critical loads have their own backup, in case of an extended outage redundant sources and redundant reconfiguration paths will become important. The control and communication model for the Miramar microgrid model is shown in Fig. 7. Typically, a communication network operator is responsible for monitoring the status of the network. In case of critical infrastructure microgrids such as defense installations, it is important that the network operator and the power system operator coordinate and exchange information to ensure that potential problems are identified quickly. For the Miramar microgrid, a fiber ring is used to connect the control center (referred to as the Energy Ops Center), the substation, and the various power generation sources, where network routers are installed. These network routers are responsible for directing the network traffic to the right destination inside their networks. There exists a logical separation between these devices, such as firewalls to prevent unauthorized network traffic.

B. Simulation Results

In this section we used the Miramar microgrid to assess potential impacts of CSIP-based attacks towards system re-

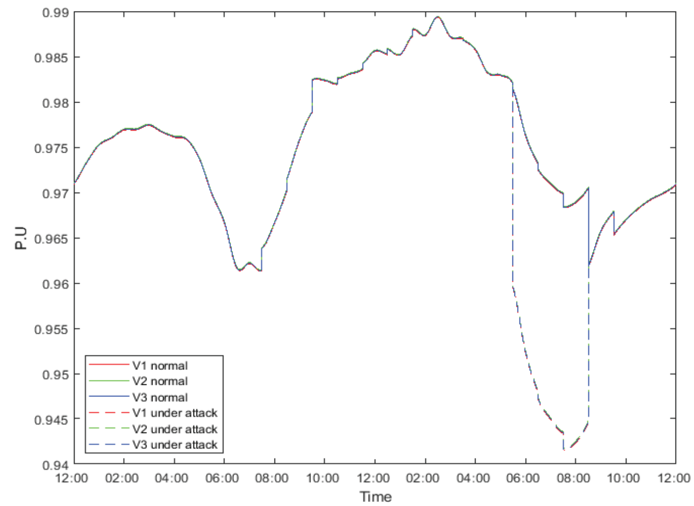

Fig. 8. Measured voltage in normal and attack scenario at point A.

siliency. We also present resiliency results for different configurations and in presence of coordinated attacks.

1) Effect of malicious DER control on voltage: As previously discussed, CSIP enables the utility to describe location and time-based rules to achieve a global objective. The data exchange mechanism relies on a set of REST services running over a secure channel (TLS 1.2). If implemented correctly, it could mitigate most of the risks of communication over open networks such as the Internet. However, this requires tight integration between the DER devices and ensuring that the chain of trust is maintained and verified at all levels. Implementations errors could result in potential vulnerabilities such as Man In the Middle (MiM) attacks, SSL/TLS downgrade attacks, and potential information disclosures [13]. Also, generic Denial of Service attacks can occur at the aggregator or utility servers.

In this case, we consider the case where the attacker can spoof the voltage at the end of the feeder and cause the utility to request for decrease the VAR support from the PV inverter. Such an attack could be the result of a MiM attack or database modification attack. Fig. 8 shows the voltage profile at point A which is the common point of connection for all the feeders. This loss of reactive power capacity has an impact on the resiliency of the microgrid. The voltage of the entire microgrid falls below 0.95pu during the attack which creates adverse effect on the distribution system managed by the utility, and a potential power-quality issue for the consumer. Notice, that under this scenario, as PVs go out of operation during night time the voltage recovers without any proactive action by the utility.

2) Effect of Coordinated Sequence Attack: In this case, we consider a proxy attack that a malicious attacker wants to compromise the critical infrastructure. The attacker techniques of attack to compromise physical infrastructure is not explored in this study. The attacker would need to do this in two steps - interrupt the supply from the utility, and compromise the power plant present in the microgrid as shown in Fig. 6.

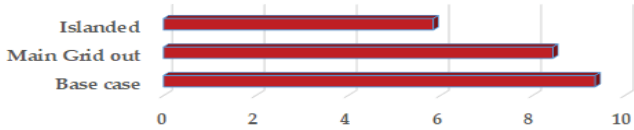

Fig. 9. Physical resiliency of Miramar microgrid for different configuration.

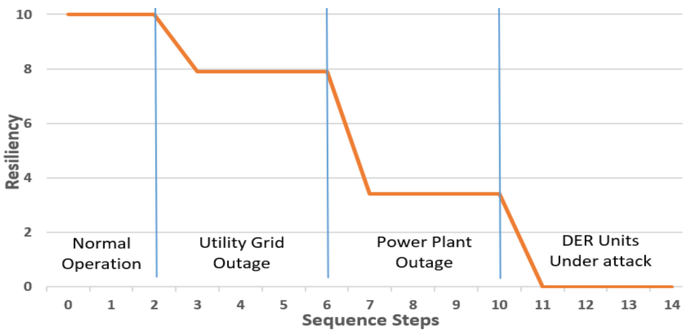

Fig. 10. Cyber-Physical resiliency during coordinated sequence attack.

Changes in physical resiliency for these steps is shown in Fig. 9 for different configuration.

Fig. 10 shows the effect on cyber physical resiliency during the sequenced attack. In the first step, we consider that the attacker has compromised the connection from the utility to the microgrid. Hence, the system moves into the microgrid configuration (after allowing time for reconfiguring the grid), and a majority of the load is picked. The percentage of loads picked up is dependent on the capacity, and load priorities assigned previously by the operators of critical infrastructure. In this case, there is an impact on resiliency due to a larger percentage of loads being picked up by the DER and power plant units which have lower availability, and results in less redundancy. In the next step, we consider the case where the attacker takes out the power plant unit. To continue operation, operator has to open tie switch sw_fc for reconfiguration to form islands and the critical loads need to be picked up by the DER units and auxiliary generators connected to individual loads. This lowers resiliency by huge value as the critical loads are being directly supplied by the DER units and auxiliary or backup generators. There is no redundancy present in the system, and no other sources of reactive power support. Now if the attacker sends malicious control signals to the DER units by exploiting the IEEE 2030.5 protocol and sets them up for inappropriate VAR support, the islands will collapse immediately as there is not enough sources in the system to stabilize the system. In this case resiliency will go to zero.

3) Situational awareness and enabling resiliency with metrics: The resiliency score is useful for the system operator to quickly understand the resiliency of the system in real time. With this information, the system operator can respond to disruptive events quickly, or in some cases take proactive control actions to recover the resiliency by operating in a suitable degraded state. For example. with appropriate physical and network control schemes in place, the operator can choose to move to a microgrid mode if there a problem with the main grid interconnection. The operator can also disable any remote operation for the DER converters, and prevent any further attacks on these devices.

VI. Conclusions

In this work, testbed for cyber-security and cyber resiliency analysis of military microgrid has been presented. Cyber model and interface builds on the emerging IEEE 2030.5 protocol for DERs and microgrids. A framework for interfacing the protocol with the open source power system analysis software OpenDSS using the REST interface has been discussed. To examine the potential weaknesses of the protocol, critical infrastructure such as defense military microgrid is considered. Representative model of Miramar military microgrid system is used for validation. Simulation results are presented to demonstrate various use cases including operational scenarios and control for cyber-physical resiliency. A method of measuring resiliency in microgrids is presented and analyzed. By improving situational awareness to take quick and proactive control actions, and by strategically designing the microgrid including various reconfiguration options, the microgrid resiliency can be improved to minimize the impact of cyber attacks.

References

[1] S. Islam, Z. Baig, and S. Zeadally, “Physical layer security for the smart grid: Vulnerabilities, threats and countermeasures,” *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[2] V. Venkataramanan, A. Srivastava, A. Hahn, and S. Zonouz, “Enhancing microgrid resiliency against cyber vulnerabilities,” in *2018 IEEE Industry Applications Society Annual Meeting (IAS)*, Sep. 2018, pp. 1–8.

[3] CAISO, “California iso monthly stats,” Feb 2018. [Online]. Available: https://www.caiso.com/Documents/MonthlyStats-Feb2018.pdf

[4] IEEE, “Common smart inverter profile: IEEE 2030.5 implementation guide for smart inverters,” 2018. [Online]. Available: https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf

[5] IEEE, “IEEE standard for smart energy profile application protocol,” *IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013)*, pp. 1–361, Dec 2018.

[6] N. Batista, R. Melcio, J. Matias, and J. Catalo, “Photovoltaic and wind energy systems monitoring and building/home energy management using zigbee devices within a smart grid,” *Energy*, vol. 49, pp. 306 – 315, 2013.

[7] A. Ghosh and N. Chakraborty, “Design of smart grid in an university campus using zigbee mesh networks,” in *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, July 2016, pp. 1–6.

[8] O. T. Soyoye and K. C. Stefferud, “Cybersecurity risk assessment for california’s smart inverter functions,” in *2019 IEEE CyberPELS (CyberPELS)*, April 2019, pp. 1–5.

[9] IETF, “The transport layer security (TLS) protocol version 1.2,” 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246

[10] G. F. Coulouris, J. Dollimore, and T. Kindberg, *Distributed systems: concepts and design*. Addison-Wesley, 2012.

[11] IEC, “Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM) base,” International Electrotechnical Commission, Standard, Dec. 2016.

[12] V. Venkataramanan, A. Hahn, and A. Srivastava, “CyPhyR: a cyber-physical analysis tool for measuring and enabling resiliency in microgrids,” *IET Cyber-Physical Systems: Theory & Applications*, March 2019.

[13] C. Meyer and J. Schwenk, “Lessons learned from previous ssl/tls attacks - a brief chronology of attacks and weaknesses,” *IACR Cryptology ePrint Archive*, vol. 2013, p. 49, 2013.