Cyber-Physical Modeling and Visualization for Microgrid Resiliency

Final Project Report

S-82G

Power Systems Engineering Research Center

Empowering Minds to Engineer
the Future Electric Energy System

Cyber-Physical Modeling and Visualization for Microgrid Resiliency

Final Project Report

Project Team

Anurag Srivastava, Project Leader
Adam Hahn
Sajan K. Sadanandan
Washington State University

Graduate Students

Venkatesh Venkataramanan
Partha Sarker
Jonathan Sebastian
Washington State University

PSERC Publication 20-01

March 2020

For information about this project, contact:

Anurag K. Srivastava
The School of Electrical Engineer and Computer Science
Washington State University
Pullman, WA
Phone: 5093352348
Email: anurag.k.srivastava@wsu.edu

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: http://www.pserc.org.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-727-2052

Notice Concerning Copyright Material

Acknowledgements

We are thankful to the National Renewable Energy Laboratory (NREL) for funding this important work. We appreciate all the technical support and advice from Brian Miller (NREL). We also acknowledge support from Glen Chason (EPRI), Tony Thomas (NRECA) and Evangelos Farantatos (EPRI) as industry advisors. We are also thankful to PSERC administration and staff for all the necessary logistic support. We would like to acknowledge support from Jayce Gaddis, an undergraduate student at WSU, in developing virtual reality (VR) setup as one of the tasks for this project. Finally, financial support from the US Department of Energy Cyber Resilient Energy Delivery Consortium (CREDC) project is very helpful to augment some of the tool development work discussed in this report.

Executive Summary

The growing prevalence of cyber-attacks on the power system has made it necessary to model the power system as a cyber-physical system. Many of the current systems used to support the electric power grid were designed without the requirement of being resilient to cyber-attacks. A future resilient grid will require that system architectures incorporate attack resilience as a fundamental design requirement. Creating resilient systems designs requires a foundational understanding of attacks and their impacts to the grid. The required understanding is different for transmission power systems, distribution grids and microgrids given their unique features. Microgrids have been getting much traction for its resourceful applicability and scalability. Guaranteeing the energy supply, especially to the critical facilities (e.g. Hospitals and fire department) during extreme outages is essential. With this enhancement, system vulnerabilities and the rising prevalence of cyber-attacks present significant dangers of cyber-physical power grids, especially for a military or critical microgrid. These threats cannot be entirely solved by security mechanisms, the concept of resiliency becomes important for critical infrastructure in cases of extreme contingencies.

The goal of this project is to support a 3D visualization framework for a cyber-physical defense microgrid that will enable the microgrid operator to have enhanced awareness of the operations and command. This research will develop a unique capability to monitor and control cyber and physical microgrid systems to enable increased resiliency for critical loads. This approach will provide a more comprehensive understanding for analyzing the interdependencies between the cyber/control networks and electrical functionality for a variety of microgrid architectures.

The project will leverage the resources and expertise of NREL and WSU with microgrid design and control to integrate the cyber and communication components. Increased consciousness of the microgrid operational status considering all the various layers will enable the operator to take smarter control actions and enable resiliency. In summation, we will propose cyber-physical resiliency metrics that enable the operator to better understand the resiliency of the system. The metrics will consider both cyber and physical system factors and will use an advanced decision-making process to compute metrics that accurately reflect the microgrid resilience in real time.

WSU's microgrid testbed provides a real-time, cyber-physical test environment to model and simulate various cyber-physical attacks and scenarios. WSU's resources include real-time simulation platforms such as RTDS and OPAL-RT, simulation tool such as GridLab-D, openDSS, communication system emulation technologies such as Mininet and various control algorithms that has been developed for microgrid resiliency and control. WSU also has established research focusing on microgrid resiliency metrics, including cyber-physical metrics. This project explored the following specific research goals:

- Cyber-physical microgrid modeling for Miramar Microgrid
- Cyber-physical resiliency analysis and visualization of use cases

This project utilizes system-level simulation studies to explore the impact of failures to specific security mechanisms while also working on to measure and enable resiliency with visualization to identify effective strategies in changing operating scenarios. In this work, cyber-security and cyber resiliency analysis for military microgrid has been presented. Cyber model and interface build on the emerging IEEE 2030.5 protocol for various DERs and microgrids. A framework for interfacing

the protocol with the open source power system analysis software OpenDSS using the REST interface is explained in detail. To examine the potential weaknesses when using the protocol, critical infrastructure such as defense military microgrid are considered. Two military-based microgrid systems - Fort Carson microgrid and Miramar microgrid systems are considered. Simulation results are presented to demonstrate various use cases, including current operational paradigm, and ways of enabling cyber-physical resiliency is explored. 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.

Also, use of different visualization tools has enhanced the capability to model micro grid in 3D. Moving forward the biggest challenge with this project will be to tour and model each desired area those represent the microgrid. This will help to build a complete model of microgrid, and operators can have a pseudo real-time experience of operating microgrid while monitoring resiliency of the microgrid for training. We will also use this platform for education and outreach.

The proposed cyber-security and cyber resiliency analysis application is a re-usable models and resources that will effectively bring out the interdependence of the cyber and physical systems of the microgrid. Specifically, microgrid operators will benefit from better understanding of these dependencies and the resulting system resiliency. The proposed microgrid resiliency metrics are also capable of testing and case-study analysis of various microgrid control algorithms and defense techniques. Publications resulted from this work is under review and one accepted.

Technical Publication:

[1] P. Sarker, V. Venkataramanan, D. Sebastian Cardenas, A. Srivastava, A. Hahn, and B. Miller, “Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5”, IEEE/ ACM CPSWeek, MSCPES workshop, Sydney, Australia, April, 2020

Student Thesis:

[2] Venkatesh Venkataramanan. “Cyber-Physical Resilience Assessment for Active Power Distribution Systems”, Ph.D. Thesis, Washington State University, July 2019.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

The power system has been evolving from a physical system to a "cyber-physical" system with components from the physical power system, associated communication infrastructure, and digital devices for measurement, control, and computation tasks. This transformation of the power system has made it necessary to model the power system as a cyber-physical system instead of just physical system.

On the other hand, microgrids have been gaining popularity for its versatile applicability and scalability. It is also involving cyber components for enhanced management of proper power supply to the loads. With this enhancement, system vulnerabilities and the growing prevalence of cyber-attacks present significant risks to cyber-physical power grids, especially for a military or critical microgrid. Considering that these risks cannot be completely eliminated, the concept of resiliency becomes important for critical infrastructure in cases of extreme contingencies.

While many efforts have focused on cybersecurity of the power grid, most have explored the security of specific control algorithms, communications, or overarching risk analysis methodologies. However, to achieve required compliance objectives, utilities are often faced with the unique problem of how to most optimally deploy various cybersecurity mechanisms in a way that achieved optimal security at minimal costs. This project will utilize system-level modelling, studies and simulations to explore the impact of failures to specific security mechanisms while also working on to measure and enable resiliency with visualization to identify effective strategies in changing operating scenarios.

An overall interest towards sustainable energy sources, and a mix of reduced technological costs and governmental policies has led to significant increases in the amount of installed solar and wind plants. These factors have fueled rapid increases in the amount of small-scale distribution-side generation that in some cases have exceeded the grid hosting capabilities, leading to utility's-imposed restrictions. These also complicate the detection of abnormalities in the power system, thus reduce operational quality of microgrids. The abnormalities in the power system can be detected by centralized multi-agent system (MAS) [1] and microgrid can be isolated from main grid during abnormalities. MAS also sheds non-critical loads to secure critical loads but does not manage DER units to increase microgrid resiliency further. IEEE 2030.5 [2] can provide convenient solution in these cases. So, IEEE 2030.5 also known as Common Smart Inverter Profile (CSIP) V2 protocol is utilized to provide an interface between the microgrid and DERs to achieve better microgrid management.

We have worked working with our industry partner NREL to identify suitable power system, communication system, and attack simulation tools, and the right interface between them. Based on our discussions with our industry partner we have identified OpenDSS, an open source distribution system simulator by EPRI for our power system simulation. We have used Mininet, a communication system emulator also capable of implementing Software Defined Networking (SDN) for our communication system model. We have explored various options for interfacing these two simulators together, including the COM server in OpenDSS. OpenDSS package ships

with a Dynamic Linked Library (DLL) that allowing the user to interface with the solver via COM Server. This allowed to directly control the solver using third party application such a MATLAB, Python, and such. However, this interface is limited only to Windows, while most communication network emulators work based off a Linux kernel.

1.2 Overview of the Project

Keeping the power on especially to the critical facilities (e.g. hospitals and fire department) during extreme outages is essential. This project has aimed to develop a 3D visualization framework for a cyber-physical microgrid that will enable the microgrid operator to have enhanced awareness of the operations and control. This research has developed a unique capability to monitor and control cyber and physical microgrid systems to enable increased resiliency for critical loads. This approach has provided a more comprehensive understanding for analyzing the interdependencies between the cyber/control networks and electrical functionality for a variety of microgrid architectures.

This project was started to demonstrate different components of a microgrid and how they tie into smart grid key topics such as resiliency and other protective measures as well as how they respond to faults. Some of the components to be modeled were control rooms, substations, and generators. One of the key challenges for this is the amount of time it takes to model an area in 3D such that it looks realistic and that it can be scripted to show the reaction to different faults.

The project has leveraged the resources and expertise of NREL and WSU with microgrid design and control to integrate the cyber and communication elements. Increased awareness of the microgrid operational status considering all the various layers will enable the operator to take smarter control actions and enable resiliency. In addition, our proposed cyber-physical resiliency metrics will enable the operator to better understand the resiliency of the system. The metrics has considered both cyber and physical system factors and use advanced decision-making process to compute metrics that accurately reflect the microgrid resilience in real time.

2. Cyber-Physical Modeling with IEEE 2030.5 and OpenDSS

DER technical capabilities are under persistent development, constantly introducing new grid-support functions that rely on communications to promote healthy grid state despite their inherent drawbacks. In the case of power inverters, the drawbacks are due to their intermittent nature, small capacity and less-than ideal location. These drawbacks can be mitigated by limiting their output capacity or by adjusting their PQ responses according to voltage and frequency signals. However, since the balance between DER power being produced and load can vary quickly, new configuration parameters (DER programs) must be pushed to end-devices relatively quickly. CSIP V2 is able to perform this by using a lightweight REST service (a text-based, stateless communication protocol). The protocol runs at the application layer and uses HTTPS as its transport mechanism, inheriting all the security mechanisms provided by TLS 1.2. Furthermore, the client authentication mechanisms available in TLS are used to deliver and isolate messages between multiple DER units without end-device intervention, creating a virtual point-to-point connection between the server and the end-device, the following subsections describe each of the CSIP components.

2.1 DER Programs

DER programs allow the device to query for program changes in a single URL request. The query can be customized to account for device location, which itself allows the device to be classified into up to 8 categories (see figure 1). Each of these categories contains a set of independently configured program types that can be inherited. These field devices include smart grid components such as smart meters and demand response devices as well as Distributed Energy Resources (DERs) units. The standard abstracts the interfaces used to communicate and assumes that a TCP/IP connectivity is already in place. It uses a combination of HTTPS and REST services to provide a secure message interchange between a central controller (utility) and client devices. The standard uses a structured data dictionary that is based on the CIM model to facilitate message exchange. It supports multiple servers (utility, aggregator) and multiple types of end devices via specific function sets. Each function set supports multiple sub-functions such as metering, demand response, generation scheduling and file transfer functions. For the DER domain, the main goal is to enable higher penetration of distribution side DER resources while maintaining adequate control over the electrical variables. This control is achieved by using a granular control over a specific set of DER devices. The standard has a wide range of granularity options, ranging from system-wide setting to individual DER devices.

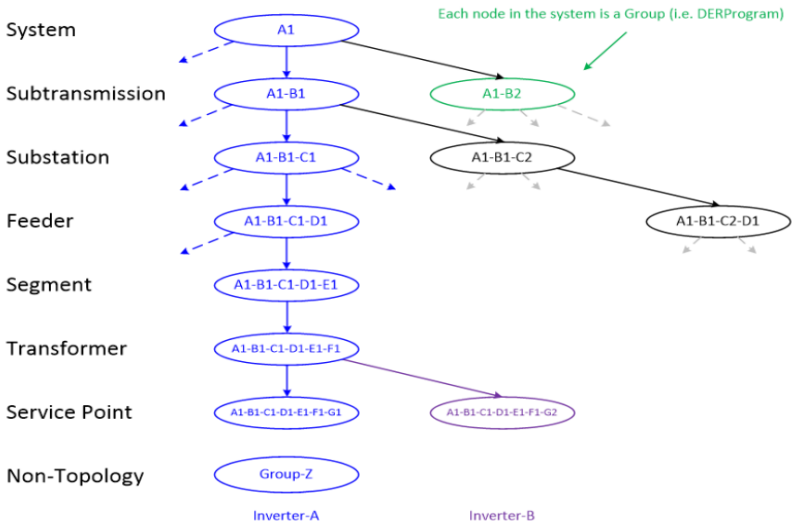

Figure 1. Hierarchical DERprogram layout as seen by two DER devices.

2.2 REST Architecture

A RESTful (or REST) service allows client devices to interact with an application server by using a uniform and stateless access mechanism. This lowers the computational requirements of client devices while providing a standardized request-response system that can be easily validated by both ends. The IEEE 2030.5 RESTful API is based on an XML format and can be configured to support client-dependent querying systems or server-side subscription systems. In a client-dependent query system, the device is responsible for constantly querying the server for updated commands or configurations. These systems are computationally inefficient but are more adequate when the client devices do not have backward reachability from the server. In a subscriber system the server can "push" the required updates directly to the client without further operations.

An overview of the IEEE 2030.5 REST architecture is given in Figure 2. For this particular work, only the DER components are shown. The REST service is designed to have a tree-like architecture that end-devices can navigate. This will enable future upgradeability by pushing new configuration nodes as needed.

2.3 Function Sets

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

a) DER Control Events: 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 specific timing requirements, for timeouts, refresh rates and fallback mechanisms.

Each of the control functions can be adjusted with different granularity levels. The granularity is achieved by having a hierarchy-based grouping, where default settings are inherited from upper levels (see Figure 2). Also the units can be managed by either the utility or a third party aggregator.

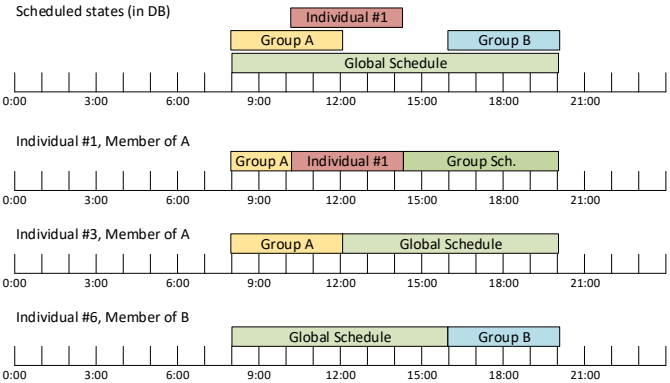

Figure 2. Time-and-location based granularity available on the IEEE 2030.5 standard.

2.4 OpenDSS

The OpenDSS platform allows to simulate the behavior of distribution systems. It includes the necessary modules required to study the effects of DER integration on unbalanced systems. The OpenDSS platform exposes a COM interface that can be used to iteratively solve time-dependent solutions. The COM interface supports Python as its controller engine. Python versatility allows to add other components that can be employed to create a DER test bed.

3. Implementation and Interface Architecture

3.1 REST Server

A REST server that replicates the IEEE 2030.5 architecture was developed as a web service. The service is connected to a database (DB) engine that contains the default control settings, as well as the dedicated datasets to allow settings inheritance and support basic client status logging. These default settings are manually added according to the circuit being loaded in OpenDSS. An overview of the DB architecture is shown in Figure 3.

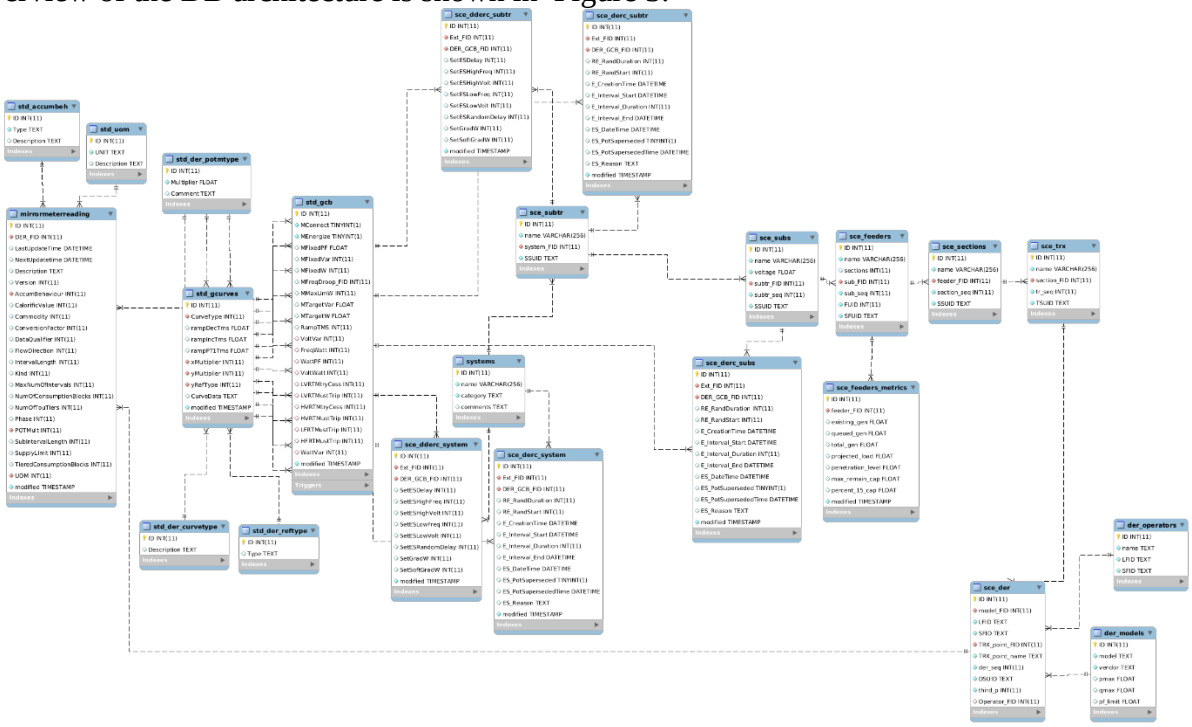

Figure 3. Database relationships.

3.2 REST Clients

A set of virtual DER devices where developed to mimic the data traffic occurring during a REST operation. These virtual clients are attached to the Python controller described in the OpenDSS section. Thus are able to receive commands from the REST service and to simulate the effect of these commands on the OpenDSS platform.

3.3 Graphical User Interface

A graphical user interface was added on top of the OpenDSS platform to aid in the visualization of the grid state, as well as tool to dynamically modify the DER parameters. An overview of such interface is shown in Figure 4.

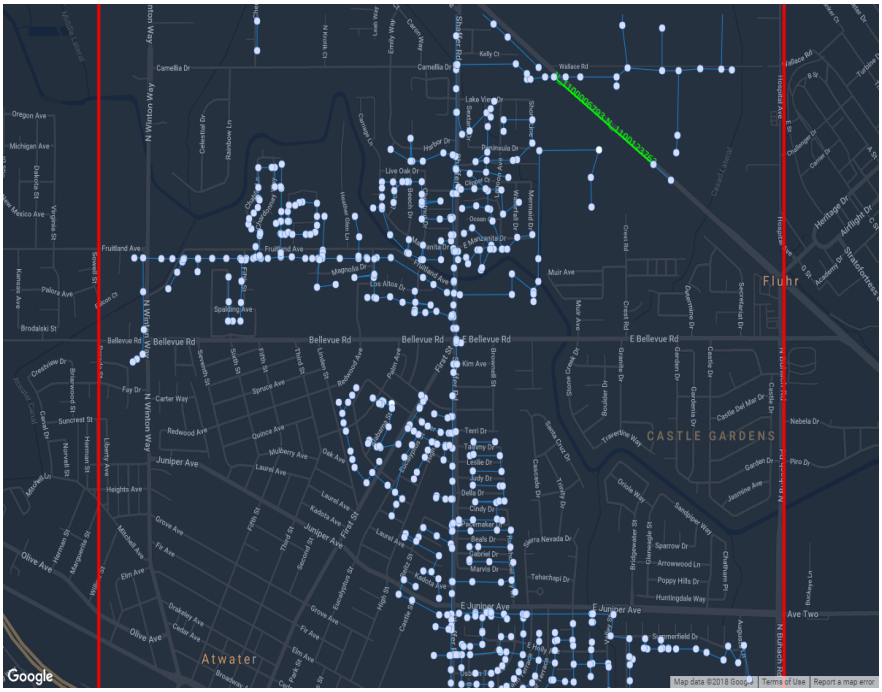

Figure 4. Graphical view of an example system.

3.4 System Integration

In Figure 5, an overview of the assembled system is presented. As it can be observed multiple virtual DER devices can be simultaneously connected. These devices stablish a direct connection to the REST server, these links can be individually inspected or intercepted to further analyze their cyber-security properties.

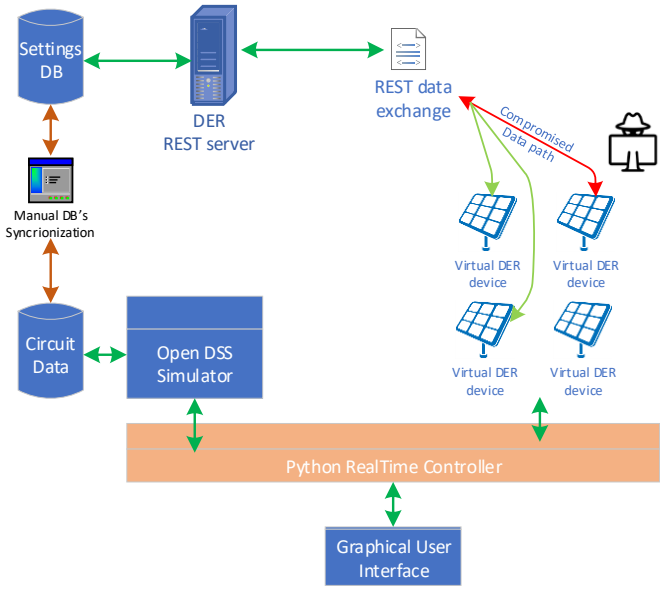

Figure 5. Block Diagram of Interconnected Simulators.

3.5 Command injection

The IEEE 2030.5 standard relies on the server being able to forward the adequate schedule programs to each end-user DER unit. In order to perform this task the system operator shall schedule the output power according to their grid studies. In the simulator, this task is accomplished by inserting events to the database before the simulation begins, each event is timestamped according to a predefined date on which the simulation will run (see Figure 6).
During the simulation phase the DER unit queries the DB and receives a response based on a virtual time stamp. The response is transmitted in an IEEE 2030.5 format, a sample of this response is presented in Figure 7.

#	tnow	pid	Ext_FID	DER_GCB_FID	RE_RandDuration	RE_RandStart	E_CreationTimeT	E_Interval_StartT	E_Interval_Duration	E_Interval_EndT	ES_ICS	ES_DateTime	ES_PotSuperseded	ES_PotSupersededTime
1	1562942793	9	2	3	NULL	NULL	NULL	1563202800	43199	1563245999	1	NULL	NULL	NULL
2	1562942793	10	2	4	NULL	NULL	NULL	1563246000	43199	1563289199	1	NULL	NULL	NULL
3	1562942793	11	2	5	NULL	NULL	NULL	1563289200	43199	1563332399	1	NULL	NULL	NULL
4	1562942793	12	2	3	NULL	NULL	NULL	1563332400	43199	1563375599	1	NULL	NULL	NULL
5	1562942793	13	2	4	NULL	NULL	NULL	1563375600	43199	1563418799	1	NULL	NULL	NULL
6	1562942793	14	2	5	NULL	NULL	NULL	1563418800	43199	1563461999	1	NULL	NULL	NULL
7	1562942793	15	2	3	NULL	NULL	NULL	NULL	NULL	NULL	-1	NULL	NULL	NULL
8	1562942793	16	2	4	NULL	NULL	NULL	NULL	43199	NULL	-1	NULL	NULL	NULL

Figure 6. DB Insertions manually generated in the back-end

```
<?xml version="1.0" encoding="UTF-8"?>
<interval>
<start>1563418800</start>
<duration>43199</duration>
</interval>
<EventStatus>
<currentStatus>0</currentStatus>
<dateTime>1562927657</dateTime>
<potentiallySuperseded />
<potentiallyupersededTime />
<reason />
</EventStatus>
```

Figure 7. A simplified digest of the program data sent to the DER device

3.6 Security of REST services

As mentioned earlier, 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 open networks. However, this requires tight integration between the DER devices and ensuring that the chain of trust is maintained and verified at all levels. However, implementations errors could result in potential vulnerabilities. This include Man In the Middle (MiM) attacks, SSL/TLS downgrade attacks, and information disclosure. Also Denial of Service attacks can occur at the aggregator or utility servers.

3.7 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 in python to replicate events such as network congestion, link malfunctions and lost packages. These events can be further defined in terms of preplanned events or randomly.

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 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. Mininet supports multiple SDN switch controllers that can be tailored to each application, in this project the simulator uses a Network Address Translation (NAT) layout (see Figure 8).

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.

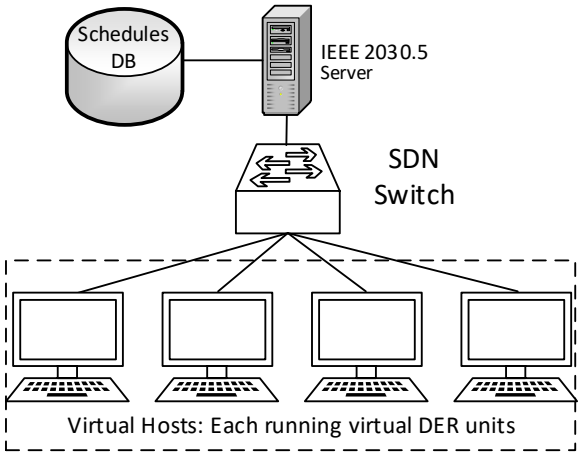

Figure 8. NAT-Based mininet architecture.

Mininet can also create monitoring interfaces that can be used to obtain network captures. For example, Figure 9 shows the typical dataflows between the server (10.0.2.15) and a given host (10.0.0.1). Notice that these addresses are in different IP segments and thus must travel though the SDN NAT-configured switch. In Figure 10, an example of a lost package capture is given.

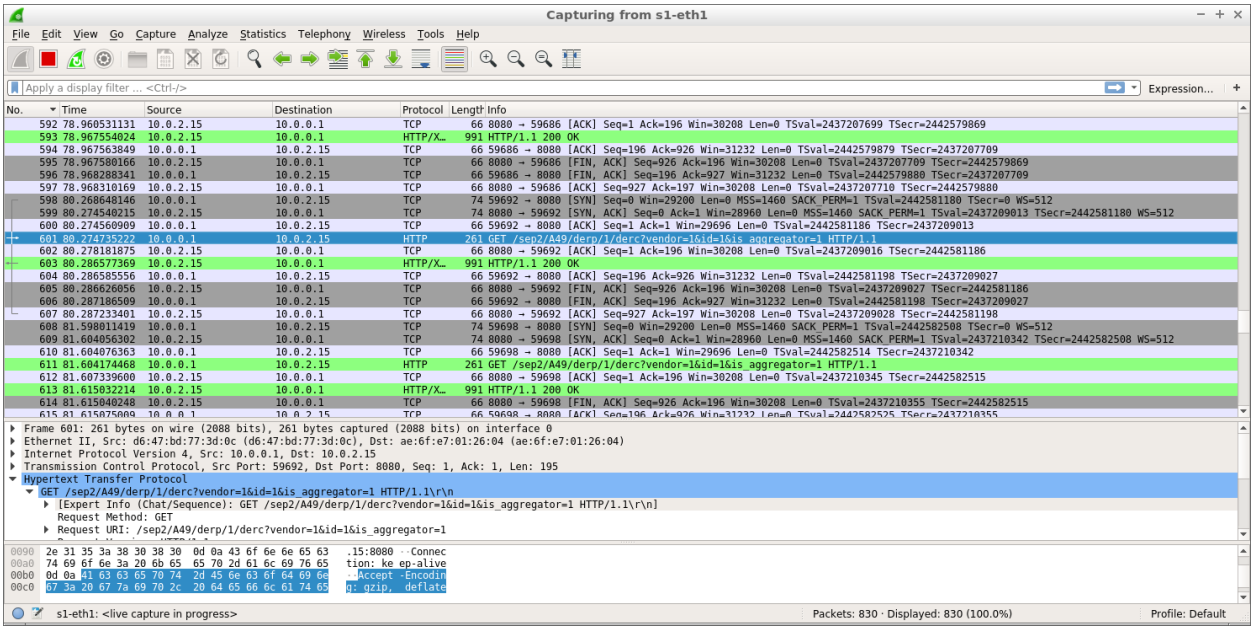

Figure 9. Sample Wireshark capture.

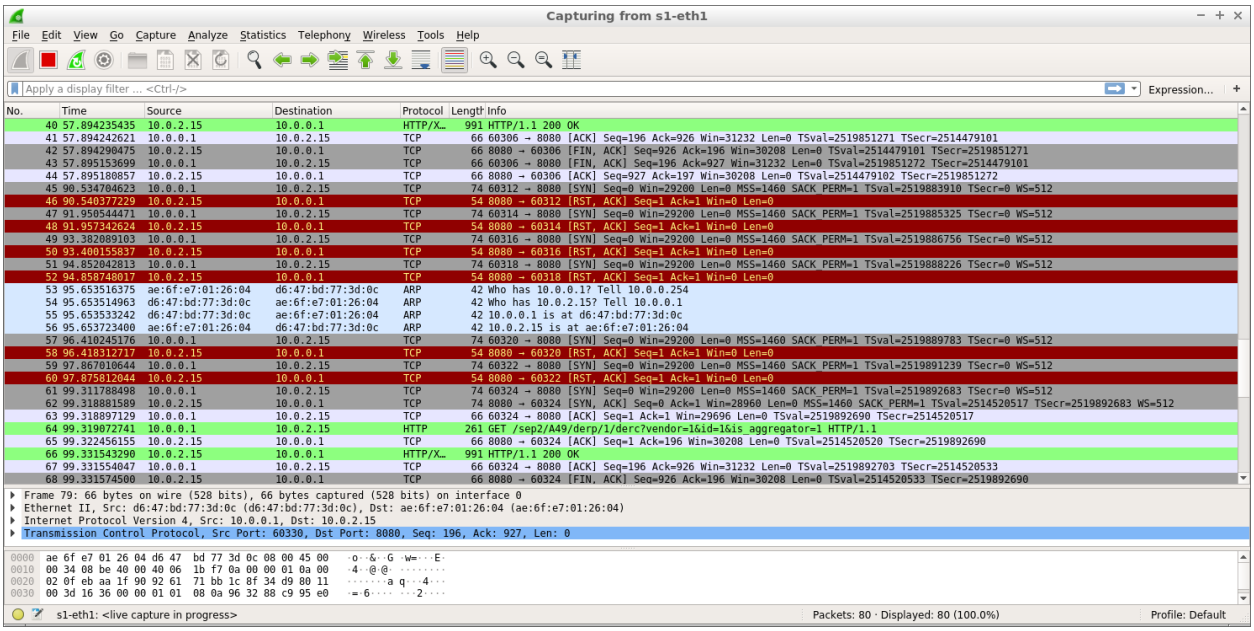

Figure 10. Wireshark capture showing lost packets.

4. Resiliency Metric for Cybersecurity Awareness

Cyber-Physical Resiliency (CyPhyR) [3] tool works by analyzing and computing cyber-physical resiliency based on the data from cyber and physical components of power system systems.

Physical resiliency considers following factors of a microgrid to find the feasible path:

1) Edge count: the ratio of total number of connected edges for each path in a possible configuration to the number of critical loads is represented by edge count.
2) Overlapping Edges: total number of common closed edges in each path for the reconfigured system.
3) Switching operations: total number of switching operations required to create the reconfigured network.
4) Repetition of sources: number of available sources that are capable of supplying the load at any given time is considered here.
5) Centrality of nodes: this factor is used to determine the criticality of each node of the microgrid.
6) Probability of availability: probability of supplying the critical load from different sources. For this system, the grid is assigned a probability of 0.9, while the DG is assigned a probability of 0.95.
7) Reactive power availability: available reactive power in the system, from VAR devices such as capacitors and remaining available capacity from DER converters.

Lastly a graph based algorithm is used to consider the power flow constraints for finalizing the feasible paths for a given microgrid. The steps for calculating physical resiliency value are shown in Figure 11.

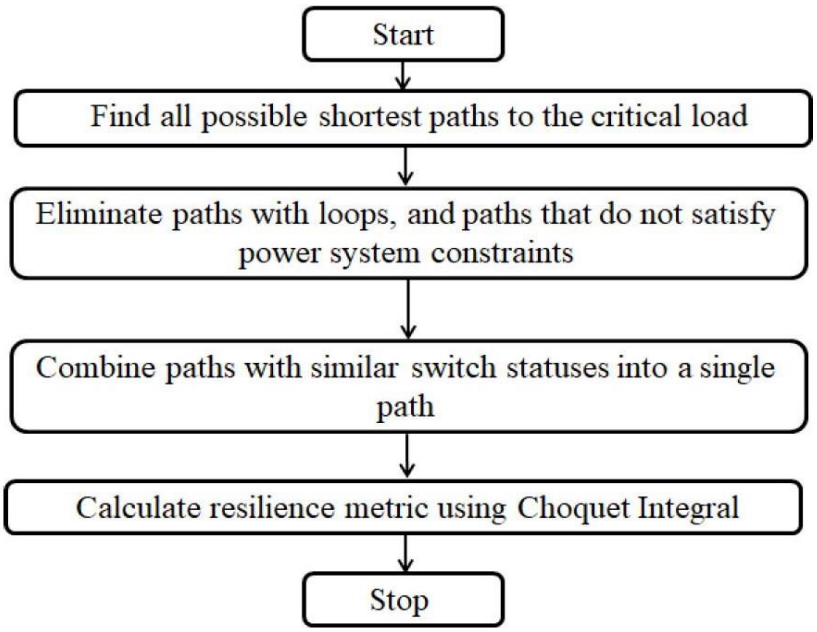

Figure 11. Steps for Computing Physical Resiliency.

The user can modify these factors, and the weights assigned to them in computing the 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. CI combines all the above factors considered and assign weights for all these criteria and come up with a single value for resiliency of a particular configuration.

The Common Vulnerability Scoring System (CVSS) is utilized in this tool to consider the cyber components of the microgrid in resiliency calculation. Cyber-physical resiliency score is calculated using Eqn. (1.1) to study the maximum impact each device can cause rather than the impact of a specific cyber vulnerability.

$$Cyber\ physical\ resiliency = CV\ SS\ \times\ CB(d) \times EnvironmentalImpact \times\ Controllability \tag{4. 1}$$

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 betweenness centrality is used to calculate the criticality of the node and edge in the network as shown in below equation.

$$C_B(d) = \sum_{\{j \neq d \neq k\}} \frac{\sigma_{jk}(d)}{\sigma_{jk}} \tag{4.2}$$

In the equation, $\sigma_{jk}(d)$ is the number of paths that pass through node d, and σ_{jk} is the total number of shortest paths from node j to k. For nodes, C_B is used, while for the switches E_B, the edge centrality is used. The edge centrality is used to represent the controllability that is lost when a particular switch is compromised. E_B is given by a similar formula as C_B, which is

$$E_B(e) = \sum_{\{j \neq d \neq k\}} \frac{\sigma_{jk}(e)}{\sigma_{jk}} \tag{4.3}$$

In the equation, $\sigma_{jk}(e)$ 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.

The environmental impact score is the change in the resiliency value from the base configuration to the new configuration as physical resiliency will be calculated for each configuration using the above mentioned steps in Figure 12.

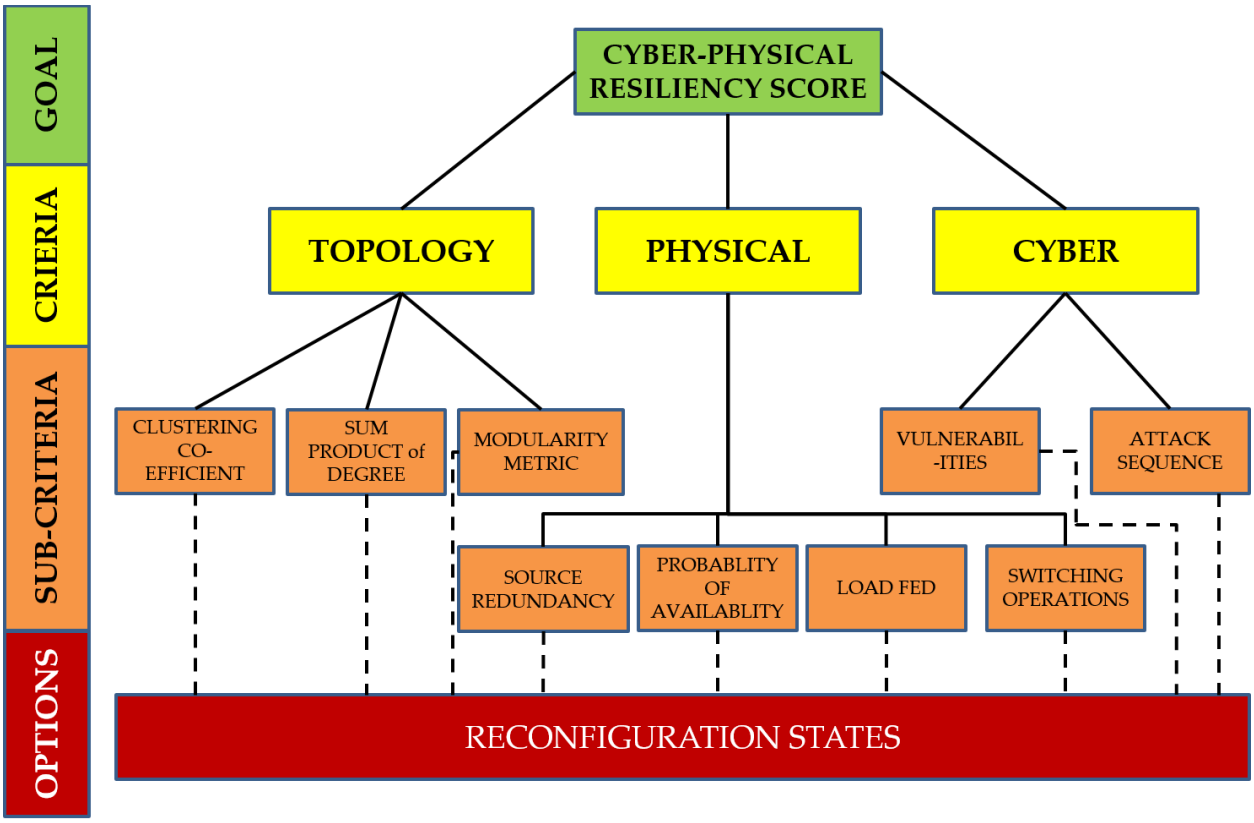

Figure 12. Cyber-Physical Resiliency Calculation.

5. Test Systems

Any microgrid that serves critical loads can be used to study the effectiveness of the proposed modeling and resiliency analysis. In this work we have chosen to test it under army-operated microgrids because of their following characteristics:

1) Size,
2) Presence of critical loads and priority loads,
3) Allurement potential, Cyber-attacks to critical assets are high-stake endeavors.

The SPIDERS (Smart Power Infrastructure Demonstration for Energy Reliability and Security) phase 2 report states that the objectives of critical infrastructure microgrids are to:

1) Protect defense critical infrastructure from loss of power because of physical disruptions or cyber-attack to the bulk electric grid,
2) Sustain critical operations during prolonged utility power outages,
3) Integrate renewable energy sources, energy storage, and other distributed generation to power defense critical infrastructure in times of emergency,
4) Manage DoD installation electrical power and consumption efficiently to reduce petroleum demand, carbon "footprint", and cost.

5.1 Microgrid System and Sensors Modeling

The microgrid used in this work is based on the model of an Army microgrid [4] [5]. Fort Carson microgrid in Colorado is part of the SPIDERS phase 2 project. This microgrid is already established, and a few details about the size of the microgrid has been made public. A conceptual overview of the microgrid's architecture is also available in public domain [5], which has been used to design the microgrid for this work.

This picture shows the basic layout of the Fort Carson microgrid. The picture also mentions some of the details about the microgrid which has been listed below:

1) The energy storage and the renewable source (PV) has been combined into a single unit, to make the system more reliable and to compensate for the variability of the PV.
2) A non-critical load has been added to the system to demonstrate the effect of reconfiguration.
3) The backup generation which are associated to each individual load has been connected to the main system so that the loads can be shared even when the microgrid is in islanded mode.
4) The priority load does not have its own auxiliary generator but is tapped off from the main feeder. The critical load has an auxiliary diesel generator that is normally in reserve (connected through a normally open breaker) but can be connected through the reconfiguration algorithm.
5) The electric vehicles have not been modeled. This is because the electric vehicles are rated much smaller than the other generation/load present in the system.

The microgrid model is shown in Figure 13. In the microgrid model, the critical load is placed at the far left, and it has an auxiliary generator connected to it. There is also the PV panel right above it, but at a farther distance as seen in Figure 13. The priority load comes right next to it but is not connected to its own auxiliary generator as explained above. This part of the microgrid is followed by a sectionalizing switch which can be used to further isolate the sensitive loads from the rest of the microgrid. The non-critical load comes last and is being fed by the grid.

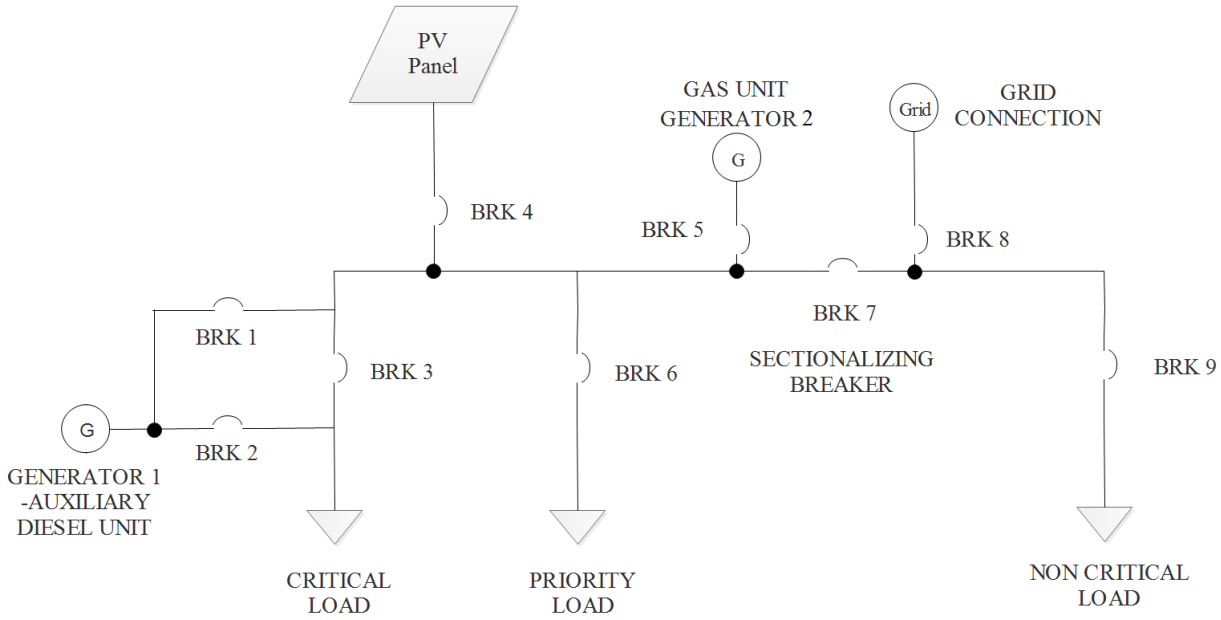

Figure 13. Fort Carson microgrid Model.

In normal operation, the grid is connected to the microgrid, and most of the loads are taken up by the grid and the PV array. The generator 2, which is considered as a gas turbine-based generator is normally open and has the first priority to be connected to the system. Generator 1 is an expensive diesel unit and does not supply any load in normal operation. However, when the critical load needs to be supplied, this generator is used.

The Miramar microgrid is a defense installation in Miramar, California. The system parameters are as follows,

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 some solar PV,
4) Motor operated switches to disconnect non-critical feeder sections,
5) Control facility and Ethernet fiber network,
6) Bidirectional electric vehicles.

The Miramar microgrid model is shown in Figure 14. The Miramar system has 8 total feeders. 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. The Miramar system has a variety of generation sources and some individual critical loads have their own backup. However, these sources might not be sufficient in case of an extended outage, in which case redundant sources and redundant reconfiguration paths become important. This is demonstrated for the Fort Carson microgrid, in the results.

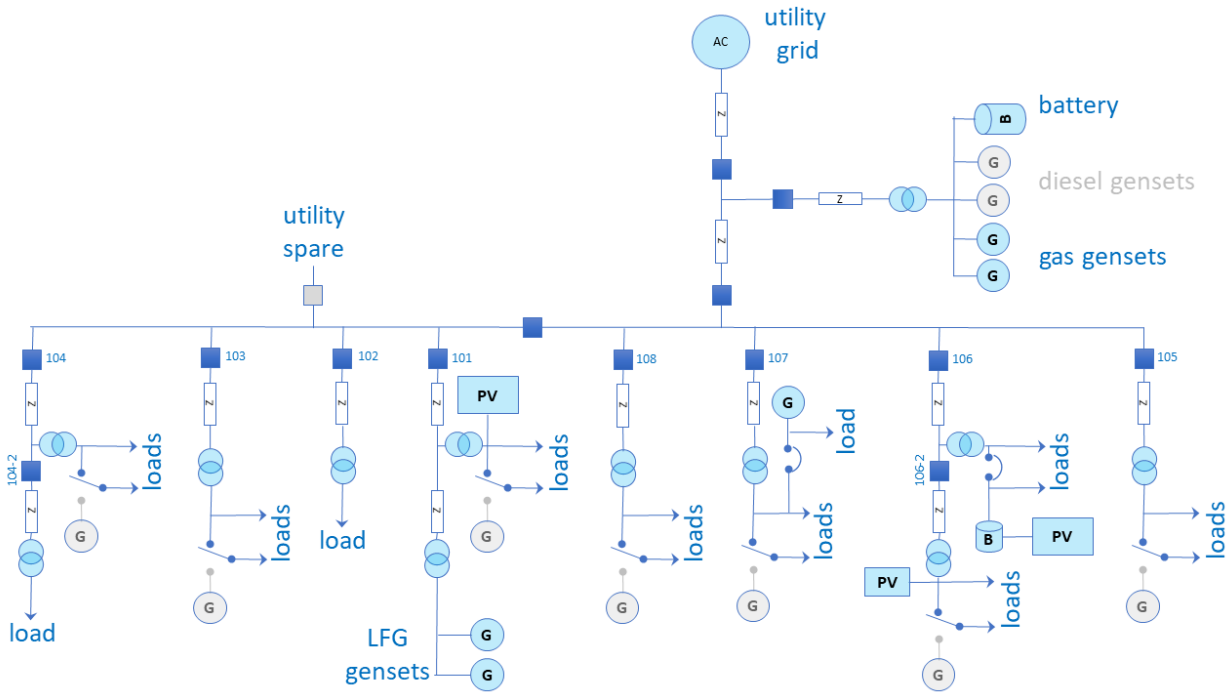

Figure 14. Miramar Microgrid Model

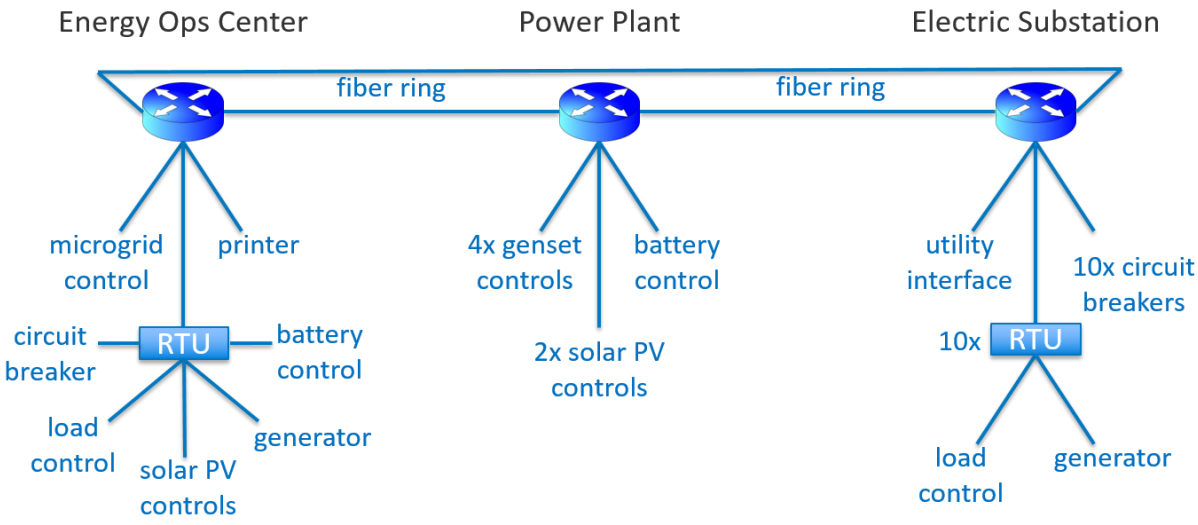

Figure 15. Communication Model for Miramar Microgrid.

The control and communication model for the Miramar microgrid model is shown in Figure 15. Typically, the utility nor the microgrid operator have a complete understanding of the network configuration and network status. 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.

6. Simulation Results

In this section we present some results from a distribution system "Alhambra 1104" [6], and study how using IEEE 2030.5 would have an impact on the system resiliency. We also present results from the Fort Carson microgrid to demonstrate the value of having alternate configurations for the microgrid, which can ensure power supply to the critical load in the presence of multiple contingencies. The study is divided into two main components, the first one, uses a grid-focused approach that studies the impacts of DER-based attacks in a distribution grid in terms of grid voltages. The second one uses a topology-based model that assesses component availability on a microgrid.

6.1 Effect of malicious DER controls on the Alhambra distribution system

The Alhambra feeders are located within the Alhambra substation, which is part of the PG&E Diablo Division. The substation contains two banks with a nominal load of 14.20 MW and 7.25 MW respectively, as reported by the WECC. The substation is classified as a typical "Northern California Inland" substation, with a mix of residential [40% - 60%], commercial [40% - 60%] and industrial [0-20%].

As previously discussed, IEEE 2030.5 v2 enables the utility to establish location and time-based rules to achieve global objectives that satisfy the voltage control, demand response or interconnection rules. Advance features such as time of day pricing, and management of distributed assets including electric vehicles can also be appended. As mentioned earlier, 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. However, implementations errors could result in potential vulnerabilities. This include Man in the Middle (MiM) attacks, SSL/TLS downgrade attacks, and information disclosure. Also, Denial of Service attacks can occur at the aggregator or utility servers.

In this study, we consider the case where the attacker can spoof the voltage at the end of the feeder and cause the utility to request an increase in VAR support from the DER units when it is not required. This loss of available reactive power reduces the resiliency of the microgrid. Figure 16 shows the grid support provided by the DER in the microgrid, and the voltage profile at the Point of Common Coupling (PCC). This loss of reactive power capacity has an impact on the resiliency of the microgrid, in addition to having an adverse effect on the distribution system managed by the utility, and the price for the consumer.

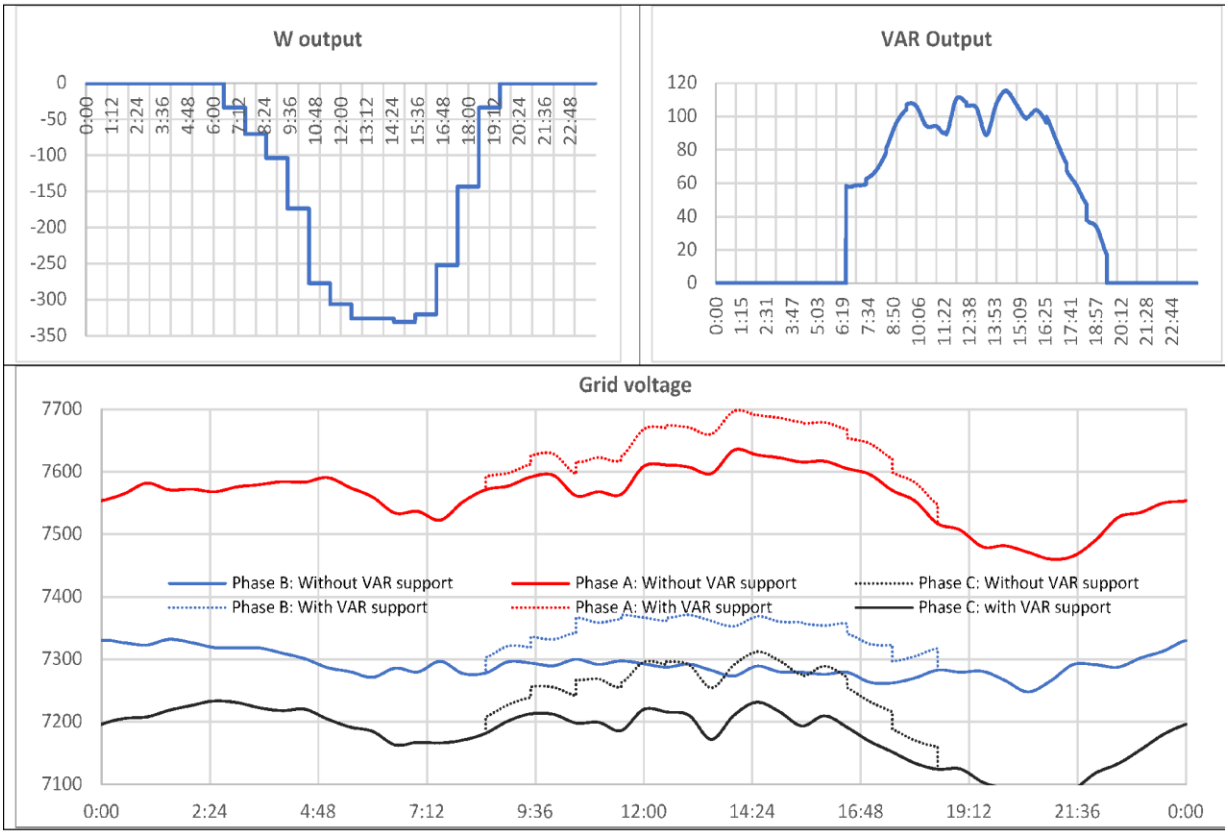

Figure 16. Voltage at PCC with VAR Support, Alhambra 1104.

6.2 Resiliency evaluation of a military microgrid

As mentioned in section 5, the Carson microgrid is a well-known military system, whereas the Miramar system is less-publicly accessible. Based on this data restriction the resilience analysis was performed on the Carson microgrid, nevertheless the proposed technique and resulting results should also be applicable to the Miramar System.

6.2.1 Effect of Coordinated Sequence Attack

In this case, we consider that a malicious attacker wants to compromise the critical infrastructure. The attacker would need to do this in two steps - interrupt the supply from the utility and compromise the DERs present in the microgrid. We compute the resiliency score for these scenarios. We consider a proxy attack in this study, and do not explore the techniques that the attacker uses to compromise physical infrastructure.

In the first step, we consider that the attacker has compromised the connection from the utility to the microgrid. In this case, the system moves into the microgrid configuration (after allowing time for reconfiguring the grid), and a majority of the load is picked. Figure 17 illustrates the configuration in this scenario, and percentage of loads picked up for each feeder. The percentage of loads picked up is dependent on the capacity of the DER units, and load priorities assigned previously by the utility and 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 units which have lower availability, and less redundancy in the system to supply the load.

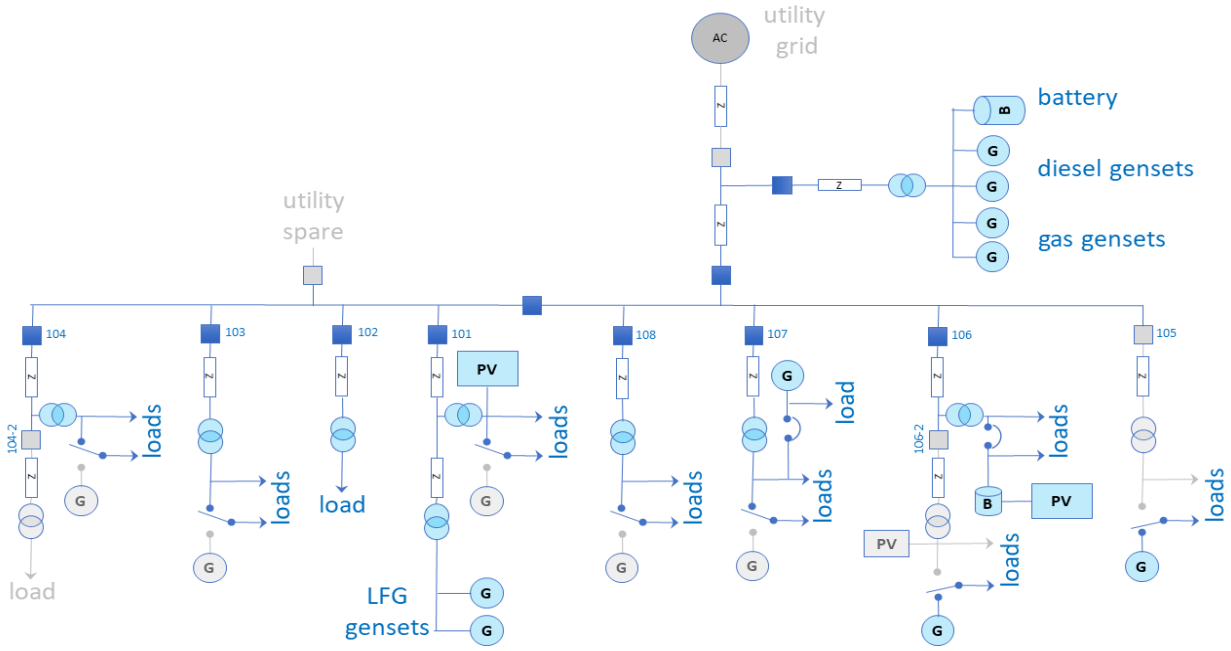

Figure 17. Miramar System in Islanded Mode.

In the next step, we consider the case where a malicious attacker disconnects the DER units from the microgrid by compromising the IEEE 2030.5 scheduling logic. In this case, the critical loads need to be picked up by the auxiliary generators connected to the load directly as shown in Figure 18.

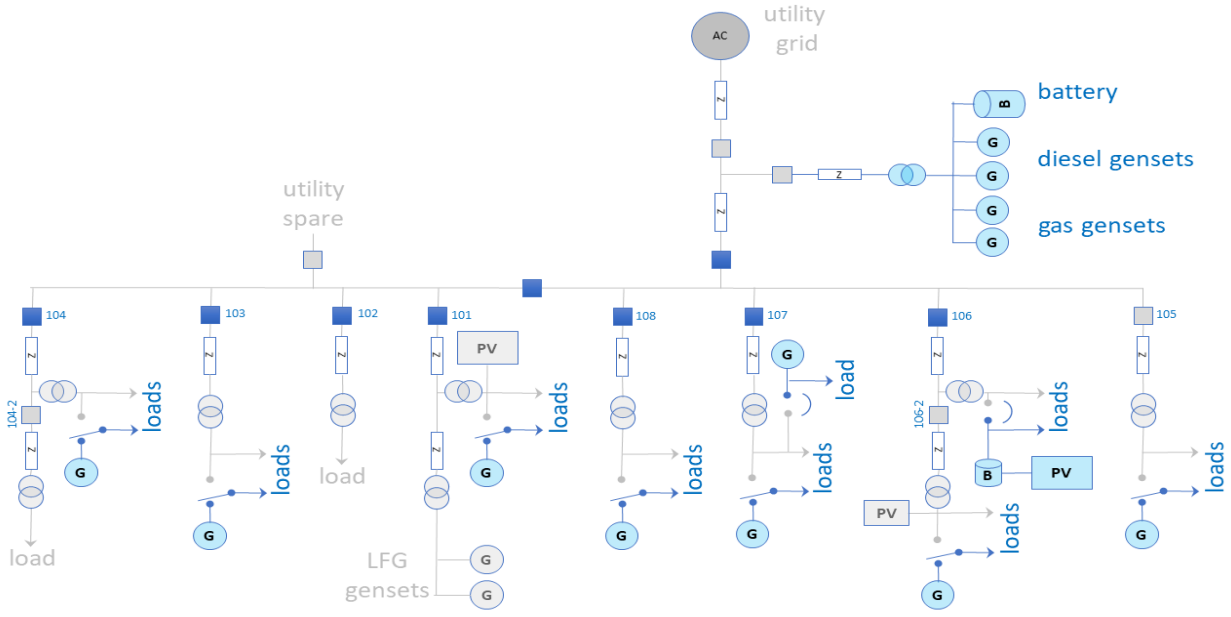

Figure 18. Miramar System in Grid Outage.

In this case, the resiliency is the lowest as the critical loads are being directly supplied by the auxiliary or backup generators. There is no redundancy present in the system, and no other sources of reactive power support. The resiliency metric is designed to go to zero if the critical load is not supplied, so any other failures in this configuration will reduce the resiliency value to zero.

6.2.2 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.

We have previously demonstrated a 2015 Ukraine attack base scenario for the Fort Carson microgrid. Here, we extend those results to calculate the feasible paths from all the generation sources to various combinations of load. These results are presented in Table 1. The table demonstrates that with strategic placing of SCADA switches, and redundancy in generation sources, cyber-physical resiliency can be enabled even in the presence of multiple contingencies.

Table 1

Load Served	Source	Path	Resiliency Metric
CL Only	Diesel Generator	12, 11	0.5239
	PV	9, 8, 10, 11	0.3719
	Gas Unit	4, 5, 6 ,8, 10, 11	0.4006
	Grid	2, 3, 5, 6, 8, 10, 11	0.3889
	Diesel and PV	12, 11 and 9, 8, 10, 11	0.7722
	Diesel and Gas	12, 11 and 4, 5, 6 ,8, 10, 11	0.7639
	Diesel and Grid	12, 11 and 2, 3, 5, 6, 8, 10, 11	0.7617
	PV and Gas	9, 8, 10, 11 and 4, 5, 6 ,8, 10, 11	0.6427
	PV and Grid	9, 8, 10, 11 and 2, 3, 5, 6, 8, 10, 11	0.6399
	Gas and Grid	4, 5, 6 ,8, 10, 11 and 2, 3, 5, 6, 8, 10, 11	0.6321
CL and PL	Grid	2, 3, 5, 6, 8, 10, 11, 7	0.3791
	Diesel and PV	12, 11, 10, 8, 6, 7 and 9, 8, 10, 11, 7	0.7521
	Diesel and Gas	12, 11, 10, 8, 6, 7 and 4, 5, 6 ,8, 10, 10, 11, 7	0.7893
	Diesel and Grid	12, 11, 10, 8, 6, 7 and 2, 3, 5, 6, 8, 10, 11, 7	0.7825
	PV and Gas	9, 8, 10, 11, 7 and 4, 5, 6 ,8, 10, 11, 7	0.6824
	PV and Grid	9, 8, 10, 11,7 and 2, 3, 5, 6, 8, 10, 11, 7	0.6794
	Gas and Grid	4, 5, 6 ,8, 10, 11, 7 and 2, 3, 5, 6, 8, 10, 11, 7	0.6837
CL, PL, and NCL	Grid	2, 3, 5, 6, 8, 10, 11, 7, 1	0.3329
	PV and Gas	9, 8, 10, 11, 6, 7, 5, 3, 1 and 4, 5, 6 ,7, 8, 10, 11, 3, 1	0.5612
	PV and Grid	9, 8, 10, 11, 6, 7, 5, 3, 1 and 2, 3, 5, 6, 8, 10, 11, 7, 1	0.5592
	Gas and Grid	4, 5, 6 ,7, 8, 10, 11, 3, 1 and 2, 3, 5, 6, 8, 10, 11, 7, 1	0.5828

7. Visualization for microgrids operation and control

Visualization is important for representing a large amount of information in a comprehensible manner. It is an important aspect of increasing situational awareness. Visualization must be developed for providing information than just producing data in a pictorial form. Some of the principles of display design include features such as legible displays, avoiding absolute judgment, using discernible elements, redundancy gain, minimizing information access cost and consistency. The main concern of the data visualization is to place it in an understandable manner which is easy to perceive the actual context.

For the visualization part, we are using a number of software and their packages. The rationale behind this is to get a perception and apprehend the information generated. Initially this was entirely handled in Unity engine with some of the more complex models being designed in CAD software or Blender. After realizing the sheer amount of time that it took to model these areas, new software that could dramatically reduce the time to model an area had to be researched. An open source software called Meshroom which a 3D reconstruction software met this requirement. With a few dozen digital images of an object it can model and texture any stationary object realistically. It makes the measurements from the photographs and adds depth or a 3rd dimension to it creating a textured mesh of any object. It allows us to run the whole photogrammetric pipeline. Now this software can be used in conjunction with Unity engine to create realistic virtual reality models in a fraction of the time that it took to create these textures and models by hand. Using this software, we generate a 3D model of our grids, control panel, and the solar system.

After getting the raw model, we structure the data to get the essential information. This is done using the blender, which is an open-source 3D creation suite. It generates the pipelining of the model and renders the simulation which enables us to get what we want without any redundant and superfluous information. Blender simulates and composes the motion tracking and also helps to add any external API if desired. It is a cross-platform which uses OpenGL to provide a consistent experience.

When the final 3D model is created using the two software, the final step is to create a real-time model which enables us to interact virtually. Unity is a cross-platform which uses C# as the scripting language to add functionality and actions to our model, to deploy them across compatible platforms which support VR/AR and consoles.
For this project, our idea is to capture raw images of the control rooms, microgrids and solar panels across the campus. Using these images, we will render and generate a 3D model of those components. Using these models, we will extract the useful information and add C# scripts to it which will add the functionality to the model.
Objective will be to have a working VR for microgrid resiliency for education and training.

8. Conclusions

This project utilizes system-level modeling and simulations to explore the impact of failures due to specific security mechanisms while also working on to measure and enable resiliency with visualization to identify effective strategies in changing operating scenarios. In this work, cyber-security and cyber resiliency analysis for military microgrid has been presented. Cyber model and interface build on the emerging IEEE 2030.5 protocol for various DERs and microgrids. A framework for interfacing the protocol with the open source power system analysis software OpenDSS using the REST interface is explained in detail. To examine the potential limitations when using the protocol, critical infrastructure such as defense military microgrid are considered. Two military-based microgrid systems - Fort Carson microgrid and Miramar microgrid systems are considered. Simulation results are presented to demonstrate various use cases, including current operational paradigm, and ways of enabling cyber-physical resiliency is explored. 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.

Additionally, virtual reality microgrid resiliency model is being developed. We will also use this platform for education and outreach.

References

[1] A. Sujil, S. Agarwal and R. Kumar, "Centralized multi-agent implementation for securing critical loads in pv based microgrid," *Journal of Modern Power Systems and Clean Energy*, pp. 77-86, 2014.

[2] IEEE, "IEEE standard for smart energy profile application protocol," IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013), 2018.

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

[4] R. A. Ducey and M. Johnson, "Overview of US army microgrid efforts at fixed installations," *2011 IEEE Power and Energy Society General Meeting*, pp. 1-2, 2011.

[5] SPIDERS, "N. F. E. Command".*(2014, October) SPIDERS Phase 2 Fort Carson Technology Transition Public Report.*.

[6] PG&E test system in GridLab-D, Avaiable online: http://gridlab-d.sourceforge.net/wiki/index.php/PGE_Prototypical_Models".