2021

Cyber-Physical Security Assessment and Resilience of a Microgrid Testbed

Said Ahmed-Zaid
Boise State University

Sin Ming Loo
Boise State University

Andres Valdepena-Delgado
Boise State University

Theron Beam
Boise State University

Cyber-Physical Security Assessment and Resilience of a Microgrid Testbed

Said Ahmed-Zaid
Electrical & Computer Engineering
Boise State University
Boise, Idaho, USA
sahmedzaid@boisestate.edu

Sin Ming Loo
Electrical & Computer Engineering
Boise State University
Boise, Idaho, USA
smloo@boisestate.edu

Andres Valdepena-Delgado
Electrical & Computer Engineering
Boise State University
Boise, Idaho, USA
andresvaldepena@boisestate.edu

Theron Beam
Electrical & Computer Engineering
Boise State University
Boise, Idaho, USA
theronbeam@boisestate.edu

Abstract

In order to identify potential weakness in communication and data in transit, a microgrid testbed is being developed at Boise State University. This testbed will be used to verify microgrid models and communication methods in an effort to increase the resiliency of these systems to cyber-attacks. If vulnerabilities are found in these communication methods, then risk mitigation techniques will be developed to mitigate them.

Keywords: microgrid testbed

I. Introduction

Microgrids are becoming increasingly popular throughout the world. Their increase is due to a variety of reasons including increasing power reliability, support of critical infrastructure during grid outages, and providing power to rural areas. In 2019, 546 new microgrids were deployed, breaking all previous records [1]. Prior to the impacts caused by COVID-19 it was expected that utilities would increase microgrid capacity by nearly 500% by 2029 [2]. These microgrids consist of a variety of distributed energy resources (DERs). This includes photo voltaic, wind turbines and energy storage devices such as batteries. Due to the nature of these power sources, the integration and power feeding often require one or more inverters. Microgrids are also being attached to corporate networks, substation networks, and power protective devices. While this distributed approach to power generation has meaningful benefits, it also increases the attack surface for cyber criminals and rogue nations. The primary goal of this project is to develop a simulated microgrid testbed to investigate potential vulnerabilities present in these systems. Vulnerabilities found will be used to develop risk mitigation techniques that can be used to increase the resilience of microgrids to cyber-attacks.

II. Project Objective

A) Testbed Development)

To begin development of microgrid threat mitigation strategies, a practical simulated testbed is being developed using hardware and software currently available in the Boise State University Cyber Lab for Industrial Control Systems (CLICS). This lab has a variety of SEL protective devices, a real time digital simulator and servers which will make up the physical components of the system. To fully develop a practical simulated model the project has been broken down into five distinct tasks. Currently, we are working on the first task which is to development the testbed's physical and virtual systems including its network design. Once this development tasks is completed, the system will be moved into the verification task where the microgrid model will be analyzed to ensure that an appropriate model has been developed. The third task will be penetration testing for system vulnerabilities using penetration software and hardware available in the CLICS Lab. This phase can also be repeated using various communication types and protocols available in the lab. The available communication types are Ethernet, radio, and software defined network (SDN). Available protocols include Modbus, DNP3, Goose, and SEL. The fourth task of this project will be development of risk mitigation techniques that can be used to improve power reliability, safety, and overall system resilience. The fifth task will be to implement the developed risk mitigation techniques and further test for improvement in the systems security and resilience. The microgrid development, penetration testing, and risk mitigation can be repeated for each communication type and protocol to determine weaknesses that arise from various communication methods. More detailed information regarding hardware and software used to develop this simulated micro- grid can be found in the design and verification section below.

B) Microgrid Design and Verification

The system development task of this project will begin with the design of the simulated microgrid. The microgrid consist of an enterprise server that contains WonderWare which be used as the systems supervisory control and data acquisition (SCADA) system. The SCADA system will receive its data signals from the systems SEL real time automation controller (RTAC) which will serve as the data concentrator for the system. This RTAC will receive signals from the SEL protective devices connected to the simulated system and sent them to the SCADA system. This RTAC will also be used for mirrored bit communications between the system's protective relays. Networking for the systems physical devices is also needed. Separate networks will be created for the DER, Enterprise server, and simulated substations. A real time digital simulator (RTDS) will be used to simulate analogs and breaker signals for the system. This RTDS allows for simulation of grid side power, DER power generation, breakers, and power measurement devices such as current transformers. The RTDS also allows us to send these simulated power signals to SEL protective relays for hardware in loop (HIL) simulations. The hardware systems currently available in the CLICS lab are shown in Figure 1. At present a small microgrid simulation has been developed and the hardware necessary for simulation is being commissioned. The schematic for the proposed microgrid test bed can be seen in figure 2. This system consists of three protective devices to control the RTDS's simulated breakers. The first protective device is an SEL 751 feeder protection relay. It will be used to protect the main feeder transporting power from the grid to a critical load. The second protection device is an SEL 651 recloser control. Its purpose is to protect the critical load from fault conditions. The third and final protective device is an SEL 421 protection, automation, and control system. It will be used to control the breakers that connect the systems DER.

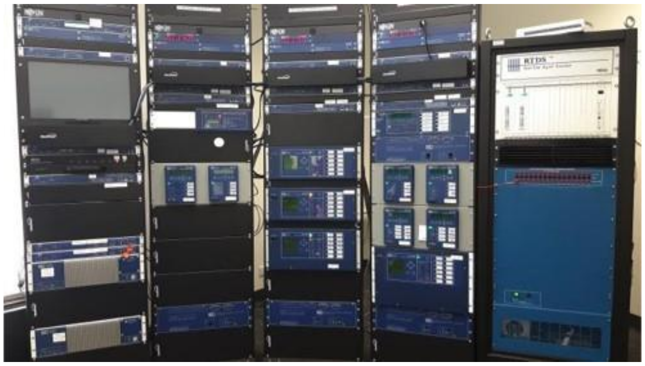

Figure 1: Protective Devices and RTDS

After the analog, digital, and network communications have been verified then the SCADA and HMI will be developed.

C) Current and Future Research Direction

This project is currently in the design phase. Once this phase is completed, we will be begin the verification of the model by testing the system's communication protocols and analog outputs. After verification is completed, then testing for vulnerabilities of the system's communication protocols will begin. Initially the system will be configured with DNP3 and Radio DNP3 communications. The communication types used though out the system will be varied over time which will allow us to see if certain communication types have inherent risks and to determine threat mitigation strategies for the most used protocols in the power industry for microgrid communications

III. Conclusion

This microgrid testbed will enable research, development, and testing of threat mitigation strategies to improve system resiliency to cyber-attacks. It would also serve as a research platform that can be utilized by industry partners for testing or developing microgrids using this simulated environment. If additional funding is obtained, then this system can be expanded to include larger simulations, physical or simulated inverters and an energy management system. Expansion of this testbed would also further enhance research capabilities, industry partnerships and educational opportunities for students throughout Idaho.

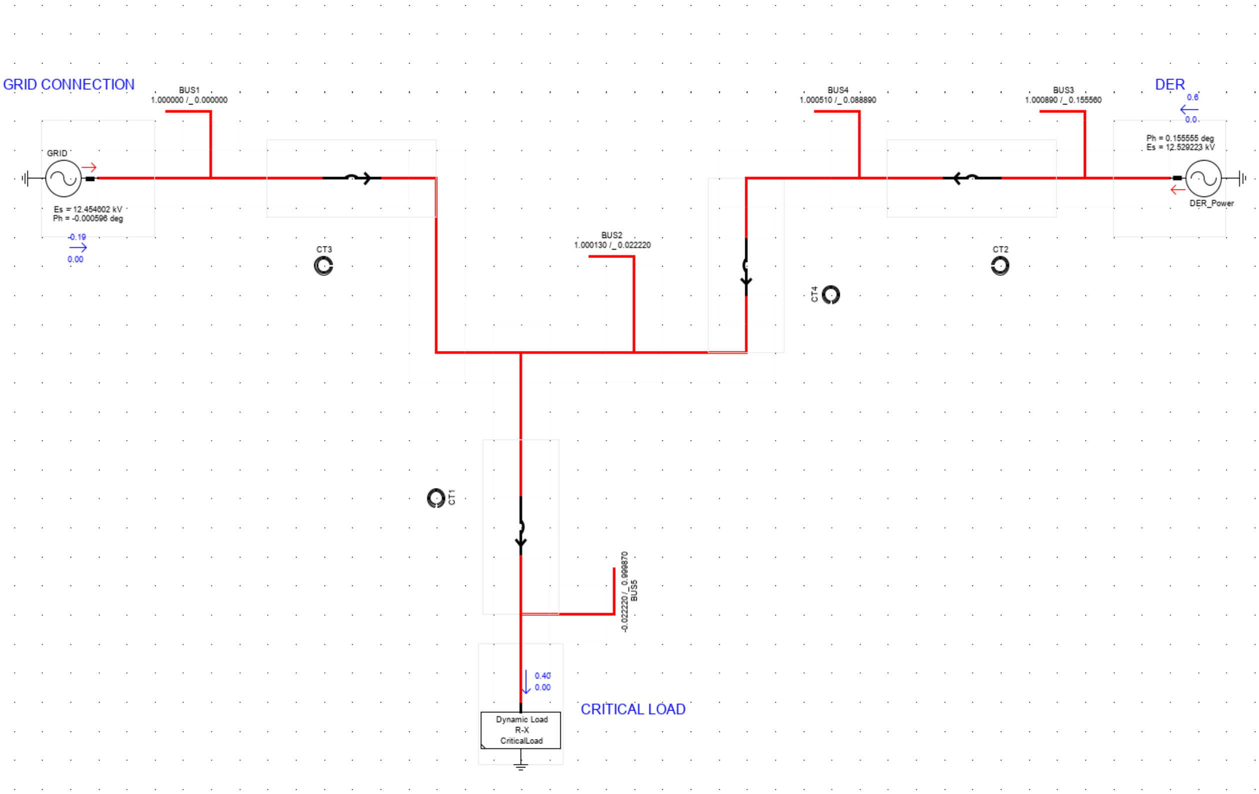

Figure 2: Microgrid Testbed RSCAD Schematic

References

[1] Nhede, 2020 [Online] Available: https: //www.smart-energy.com/industry-sectors/distributed-generation/ microgrid-installations-hit-new-record-in-the-united-states

[2] N. Burton, D. Sarpong, and N. O'Regan, "Architectural correspondence, architectural misting, and innovation: New perspectives," pp. 5–11, 2020. [Online]. Available:, 10.1002/jsc.2305; https://dx.doi.org/10.1002/jsc.2305