# Design and Improvement of a Real-Time Simulated Microgrid and SCADA System for the University of Idaho Industrial Control System Testbed

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Electrical Engineering

in the

College of Graduate Studies

University of Idaho

by

Philip Andrew Richardson

Major Professor: Herbert L. Hess, Ph.D.

Committee Members: Brian K. Johnson, Ph.D., Yacine Chakhchoukh, Ph.D.

Department Administrator: Joe Law, Ph.D.

August 2020

## Authorization to Submit Thesis

This thesis of Philip Richardson, submitted for the degree of Master of Science with a major in Electrical Engineering and titled "Design and Implementation of a Real-Time Simulated MicroGrid and SCADA System for the University of Idaho Industrial Control System Testbed," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies for approval to the Collage of Graduate Studies.

Major Professor: ______________________________ Date: ____________
Herbert Hess, Ph.D.

Committee Members: ______________________________ Date:____________
Brian Johnson, Ph.D.

______________________________ Date:____________
Yacine Chakhchoukh, Ph.D.

Department
Administrator: ______________________________ Date:____________
Joe Law, Ph.D.

# Abstract

One of the main goals of this thesis is to expand upon a previously created simulation of a microgrid system to better emulate a real-world power system. By doing this, the system can function more dynamically and behave more realistically in test scenarios. The next goal is to implement substation hardware into the loop to simulate a utility SCADA system with network communication for testing the effect cyber-attacks can have on the system's operation. This will allow the testbed to be used to develop measures to detect attacks along with countermeasures to mitigate cyber-attacks and allow the system to recover faster from such attacks.

This research project successfully, designed, tested, and implemented improvements to the simulated system including the inclusion of dynamic loads, improved generator controls, and DC storage device. These improvements allow the simulated system to more accurately mimic a real-world power system while remaining within a stable operating region. The project also successfully configured and incorporated of substation equipment to simulate multiple substations along with designing and implementing a SCADA master used by operators to directly control the system from a remote location. This SCADA master consists of a human-machine interface, used to monitor and interact with the system, and a data historian, used to record system data points for future review and analysis. These improvements and incorporated hardware allow for the system to be utilized in future projects relating to system resilience and cyber threat analysis.

## Acknowledgments

I had the privilege of working with several extremely talented people who I would like to thank.

I would like to thank my major professor and advisor Dr. Herbert Hess for helping me with my graduate studies and for his help in putting this thesis together. I’d also like to thank Dr. Brian Johnson for helping me with this project, and walking me through many difficult concepts. Both of them were instrumental in not only the success of this project, but of my graduate studies as a whole. I greatly appreciate of all their efforts over the years.

I would also like to thank my colleagues and fellow students Hari Challa and Ibukun Oyewumi. Hari built the original version of this system and without his help and advice, I would not have been able make anywhere close to the amount of progress on this project. Ibukun designed and built pretty much the entire network infrastructure for the SCADA system, and was indispensable to the project as a whole. I cannot thank them both enough for all their hard work and contributions.

## Dedications

I would like to dedicate this paper to my loving and supportive family
my parents David and Marcia as well as brothers Arthur, Brian, and St. John
along with my sister Maggie.

## Table of Contents

## List of Figures

## List of Equations

## List of Tables

# Chapter 1: Industrial Control System Testbed Introduction

## 1.1 Project Background

In recent years, digital communications have become more integrated into large scale power transmission and distribution systems for use in protection and control schemes. This increase in communications has led to an increased concern for cybersecurity due to recent cyber-attacks  from both private entities, such as recent ransom-ware attacks, and foreign nation-states, such as the Ukraine attacks in 2017 [1]. Due to these concerns, many groups have begun looking into developing methods to detect and prevent these attacks by first studying them and the effect they can have on a system and then developing active defenses. Since investigating these attacks is not practical on an actual power distribution system, a simulated system is needed to properly study and analyze them to promote development of these active defenses.

## 1.2 Problem Statement

The simulated system shown in Figure 1.1 is based off work done by a previous graduate student at the University of Idaho. It represents a microgrid power distribution system with local power generation in the form of two hydroelectric generators, with local loads, split into three sections represented by different substations, and a connection to a larger grid. Since this system was designed to mimic an actual power system, it must stay within its desired operating regions for voltage and frequency at the various buses.

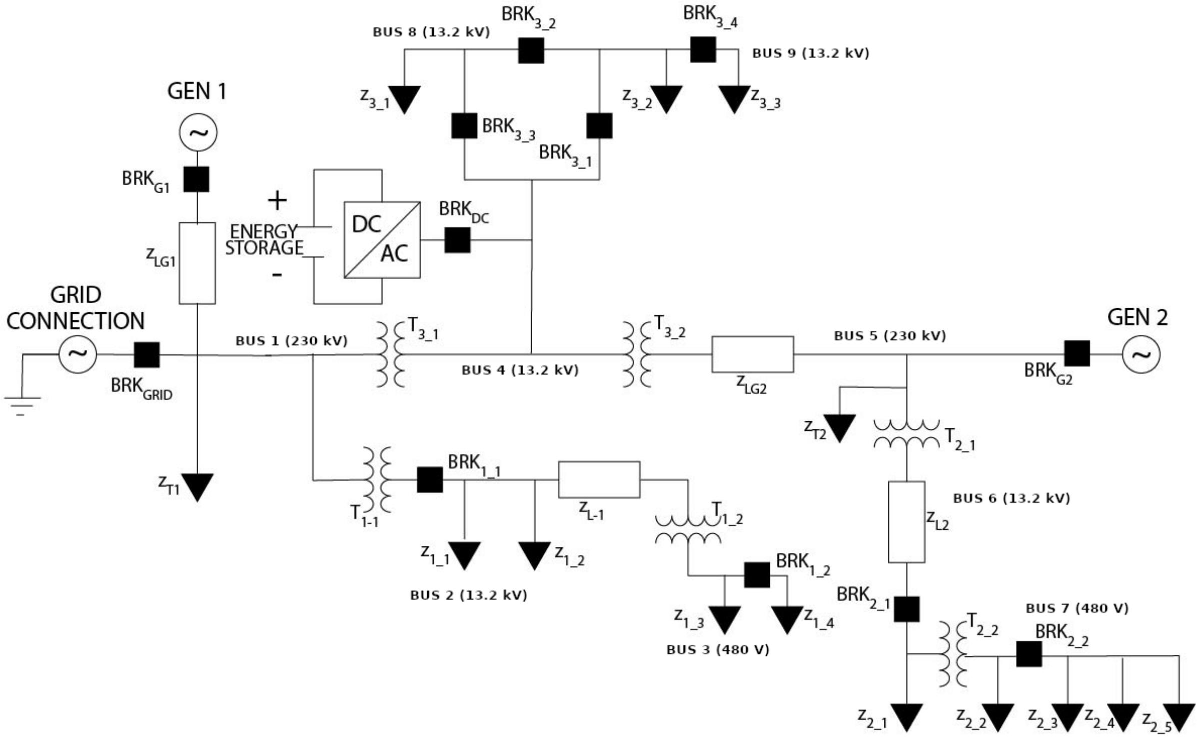


Figure 1.1: Simulated 9 Bus Microgrid System

A major problem faced when simulating a power distribution system is accounting for the dynamic changes that occur in the real world where the power drawn by loads in the distribution system changes over time as different devices are turned on and off. To account for this, simulated loads should vary over time to represent the load changes that occur during the day. Additionally, the local generators should also respond to these changes in power demand and respond to the system being disconnected from the larger grid. During these transitional periods, the simulated system must remain stable and must accurately represent the behavior of a real system.

A real power system relies on a large network of measurement, protection, and control devices to monitor and maintain the system. Typically, these devices communicate with each other through a supervisory control and data acquisition system (SCADA) using either serial or Ethernet communication schemes, such as IEEE 61850 (GOOSE) or distributed network protocol 3 (DNP3) for longer distance communications [2]. The communications between theses devices and with the control devices are the primary attack vector for cyber-attacks [3]. Therefore, the testbed will need to incorporate several hardware devices commonly found in substations, such as protective relays and real-time controllers. It will also need a centralized master with a human-machine interface that an operator would interact with to monitor and control the system.

Lastly, the simulated system should accurately replicate different scenarios with little difference so that tests can be easily repeated as well as respond to the same situations with little to no change in the recorded data. This ensures that test results can be easily replicated and properly analyzed over multiple experiments. It should also be easily changed and reconfigured to allow for the system to be used in in a variety of tests. Accordingly, the system needs to be flexible for different parameters and scenarios. Lastly the system should be well documented with archived access to documentation of the hardware and software setup of the SCADA devices.

### 1.3 Proposed Solution

To accurately replicate a real world microgrid, real time digital simulation will be employed that allows accurate data to be collected by physical substation equipment with a realistic communication and control network. Additionally, since this simulated system will be as a testbed for future research projects, it should be well documented and easily re-configurable so that multiple different scenarios can be carried out quickly and easily by other groups and students. This thesis will examine a few main topics, and primarily focus on the analysis and refinement of a single simulated model. It will assess the background and state of the previous simulation used as a basis for the testbed. It will analyze the impacts of proposed improvements to the simulation including adjustments made to the power flow of the simulation, the implementation of feedback control on the local generators along with local voltage controls at the distribution buses, and finally the implementation of an energy storage source that can provide the necessary power during sudden transitions within the system. These improvements aim to allow the cyberphysical simulation to run more dynamic and realistic scenarios and experiments.

Then, the thesis will evaluate the setup and configuration of the various pieces of substation equipment used to simulate the communication found in a real world microgrid. It will cover devices that are typically used in power grid supervisory systems and how they are configured and implemented in the testbed. It will also cover the role, design, and implementation of the SCADA system's master controller and its human-machine interface and its data historian. These improvements allow for accurate time aligned physical and communication data to be observed and collected for future analysis.

# Chapter 2: Background Information Review

## 2.1 Microgrid System Overview

Microgrids are small self-contained power distribution systems comprised of local power generators, such as small natural gas generators and photovoltaic generators, power storage units, such as flywheels and batteries, and dynamic loads. They can either function as part of the larger grid or independently when disconnected from the main grid and operate in islanded mode [4]. This allows the system to be more resilient and reliable than a typical grid reliant power distribution system. Microgrids also provide potential for a more efficient use of renewable energy sources with precise control of their local power generators and storage devices [4]. This is accomplished through active generator control maintaining the power and voltage levels of the system while keeping the system stable through a supervisory system monitoring and applying control signals to the system.

## 2.2 Supervisory System Overview

Supervisory systems are used to monitor and control large scale systems with multiple inputs and outputs. A SCADA system is a common form of supervisory system for large power transmission systems. SCADA systems are typically comprised of five layers starting at level zero [3]. Level zero consists of sensor and measurement devices that directly monitor the system. In power systems, these devices are typically collected and re-transmitted by remote terminal units and, more recently, are based on time synchronized phasor measurement units (PMU) and phasor data concentrators (PDC). Level one consists of input/output devices that directly control the system. Level two consists of the supervisory computers and devices that monitor and collect data from the lower level for automated control processes and human operators. Level three contains the automatic control schemes that take the control inputs from operators, processes them, and passes them to the input/output devices to be applied to the system. In a power distribution system, levels one to three, and sometimes level zero, are usually combined into a single device, such as intelligent electronic devices, real-time automation controllers, and relays. The last level, level four, is the SCADA master used by operators to monitor and set control set-points for the system. In power transmission systems, this is typically a human-machine interface that allows operators to monitor and directly control remote parts of the system from a centralized location. Additionally, power transmission systems usually contain another system called a data historian that records system data to a separate database for future review and analysis [5].

Since power SCADA systems collect and transfer data over a large area, they must employ some form of communication between devices. In the past, this communication was done over analog lines, but in recent years, many systems have made the move to digital communication over Ethernet networks. This move to Ethernet has allowed faster and more accurate system monitoring and control but has also introduced a new threat of cyber-attacks originating from either inside the SCADA network or from an outside connection [5]. To study the effect these attacks can have on a power distribution system, the University of Idaho has developed the Industrial Control System (ICS) testbed [6].

To properly simulate a real-world SCADA system, several pieces of physical hardware have been configured and incorporated into the ICS to mimic multiple substations. Alongside these simulated substations, a functioning HMI and data historian have been implemented using General Electric's iFIX software. The configuration and setup of these simulated substations and the design and implementation of the HMI will be discussed more in chapter 4 of this thesis.

## 2.3 Generator Control Overview

The simulated microgrid contains two hydroelectric generators that supply the majority of the microgrid's power during grid operation and essentially all of the power while the system is islanded. The generators' turbines are driven by water stored in reservoirs. By varying the rate of flow of water used to turn the turbines and the water pressure, the amount of power produced by the generators can be changed over time. These reservoir driven generators can change their power output on command and even store excess energy by pumping water back into the reservoir. In contrast, run-of-river hydro generators are driven by the natural flow of water through a river or stream so their maximum power output is limited by the flow rate of the river [4]. The voltage output of the two hydro generators is determined by the speed of the generator and its excitation field. In synchronous machines the speed is kept constant at the speed for the nominal system frequency; therefore, voltage is controlled by changing the voltage and current of the field windings [7]. The exciter control scheme will be discussed in-depth in chapter 5 of this thesis.

Hydro generators have a few inherent issues that must be accounted for when incorporating them into a power system. First, the reservoir used to store water has a physical limit to the amount water that can be stored at any one time and operating constraints on changing the water level. These can limit the amount of energy that can be produced and stored by the generator over time. This issue is beyond the scope of this thesis, it is assumed that there is an ample supply of water for operation since the issue of water storage capacity is a well understood control and operation challenge. Next, synchronous generator rotors have inertia preventing their output from changing instantaneously. It is a physical characteristic of the masses of the generator rotors and turbines that prevents the generator from suddenly changing its rotational speed. Similary, the field current characteristics limit the response time for changes in the field current. These characteristics limit sudden power and voltage changes. It also helps smooth relatively rapid fluctuation in the power and voltage levels. Unfortunately, this inertia also limits the generator's ability to respond to sudden changes in the system's power requirements. This issue is solved in this project by implementing an energy storage system to provide the needed power during these transitional periods.

### 2.4 Energy Storage System Overview

The energy storage system uses a battery to store and release energy from and into the system. Power is transferred over an AC-DC converter that functions as either an inverter or rectifier depending on the power requirements of the system. The output power and grid side voltage of the AC-DC bridge is controlled by a switching signal [8].

An energy storage system has several advantages when implemented into a microgrid system. Primarily, it allows for less reliance on the grid during transitional periods when local generators move to new power and voltage set-points or when there is a mismatch between the system's required power output and the amount of power being produced by the local generators. Due to their lack of mechanical components, energy storage systems have a significantly smaller inherent inertia than traditional generators. This lack of inertia allows energy storage devices to provide necessary power much more quickly during transitional periods than hydro generators [7]. Conversely, energy storage devices can rapidly change to act as a load and absorb any excess power produced by the generators. By storing this excess energy for later use, an energy storage device improves the efficiency of the power system by reducing the amount of power wasted.

Energy storage systems introduce a few issues that must be addressed to correctly function in the microgrid. Primarily, the charge/discharge signal must be accurately controlled to ensure the energy storage device responds properly to changes in the microgrid within the power and energy limits of the energy storage system. The development and implementation of this control scheme will be covered in depth later in chapter 6. The next issue for an energy storage device is the limit to the power that can be safely transferred through the converter and into or out of the battery. To achieve these limitations, the control scheme needs to be designed to limit the maximum power transfer of the storage device. This will also be examined in chapter 6 when discussing the design and modeling of the energy storage system. Additionally, when implementing an energy storage system, the size and physical properties of the battery used to store and release power must be considered. The design, modeling, and implementation of an actual battery is not necessary to accomplish the scope of this thesis; therefore, this battery will be modeled as an ideal DC voltage source in the simulated microgrid.

### 2.5 Chapter 2 Summary

This Chapter has detailed background information pertaining to the topics discussed in this thesis. It gave a brief overview of microgrid systems and their operation. An overview of the primary generators used in the simulated system and the issues inherent to them, such as their inherent inertia. It then discussed the implementation of an energy storage system into the microgrid model. Finally, it gave an overview of SCADA systems used to supervise large power distribution systems.

# Chapter 3: Simulated System Prior Work and Analysis

## 3.1 Initial System State

The University of Idaho’s ICS testbed is derived from a system previously built by another graduate student at the University of Idaho for a project with the Idaho National Laboratory (INL). The system was designed to simulate a microgrid power system in a real time digital simulation and output measurement data over DNP3 to a SEL 3530 real-time automation controller (RTAC). This measurement data was then re-transmitted to another RTAC which acted as a SCADA master and interface to a data historian. Cyber-attacks were carried out on the link between the two RTACs. The network traffic was collected and analyzed by a separate group of graduate students at Virginia Commonwealth University to train a machine learning algorithm to detect system disturbances and anomolies [9]. This system was focused primarily on producing network traffic that could be used as a baseline for normal network traffic and observing disturbances in network traffic caused by cyber-attacks. The classes of attacks were limited to types of attacks that could occur once an adversary had penetrated the SCADA network. The actual methods for penetration were not simulated. The original simulated system is shown in Figure 3.1 and the original hardware setup is shown in Figure 3.2. However, since it was an initial limited design it had several shortcomings that became more apparent as the project progressed.

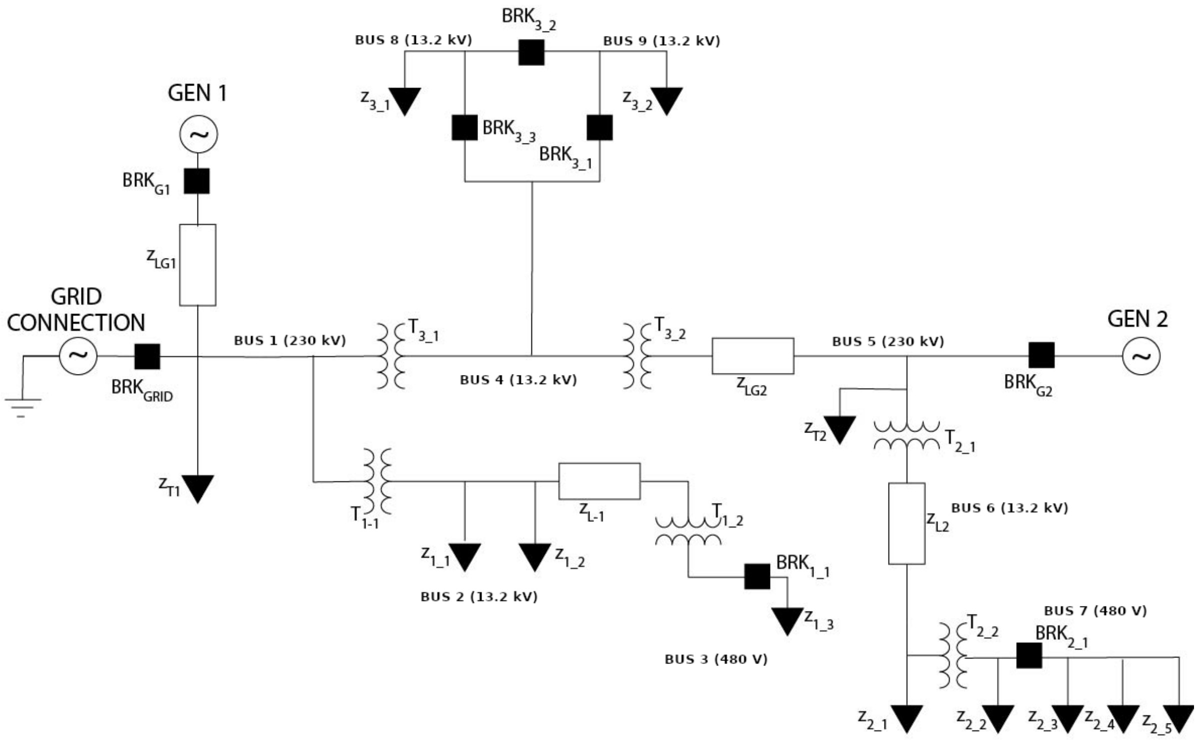


Figure 3.1: Previous Microgrid Simulation

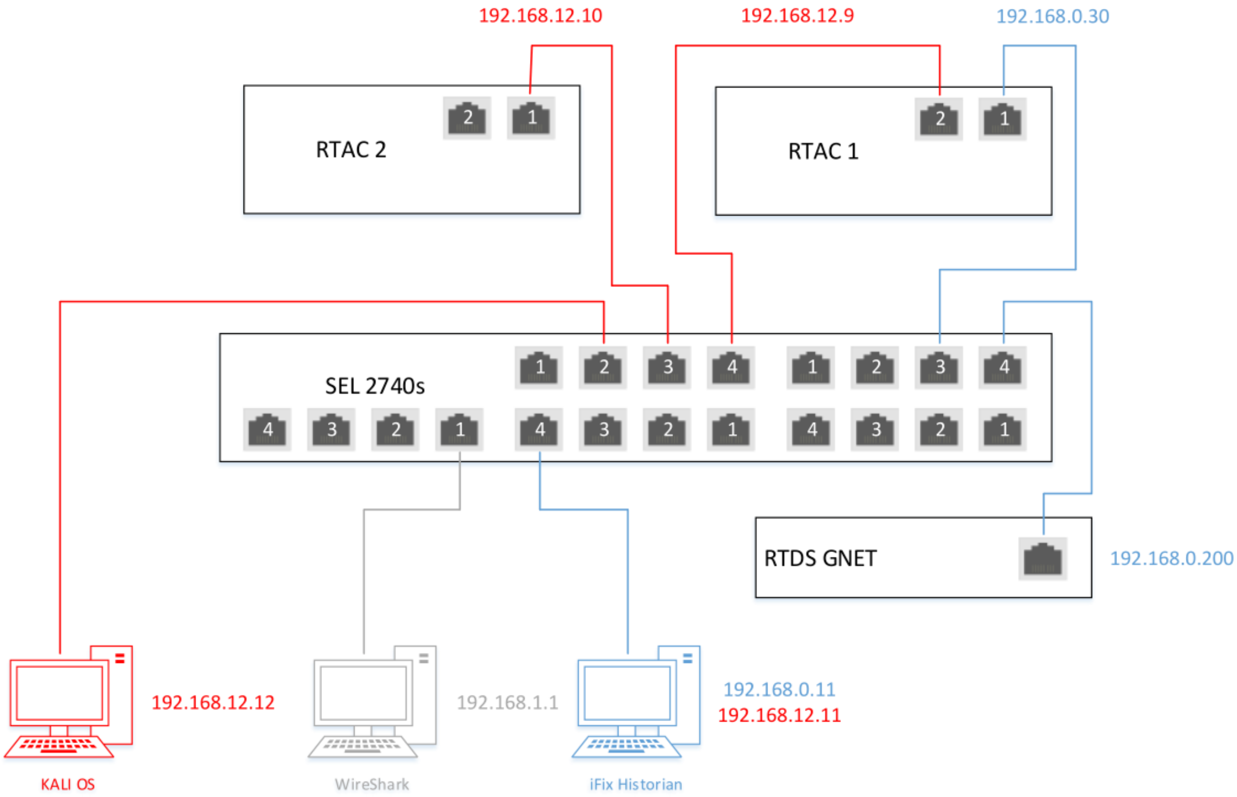


Figure 3.2: Previous Communication Network Configuration with Two Networks

### 3.2 Power Flow Analysis

The most notable shortcoming of the previous system was a lack of adaptability in the control of the power system. The loads were locked in a static state and the generators were locked at a fixed rotor speed, power output, and voltage level. An in-depth analysis of this system needed to be performed before it could be redesigned to allow for dynamic changes to be made during run time and still remain stable. This was done by conducting a power flow analysis of the system using PowerWorld®. The PowerWorld® simulation results for one operating state can be seen in Figure 3.3.

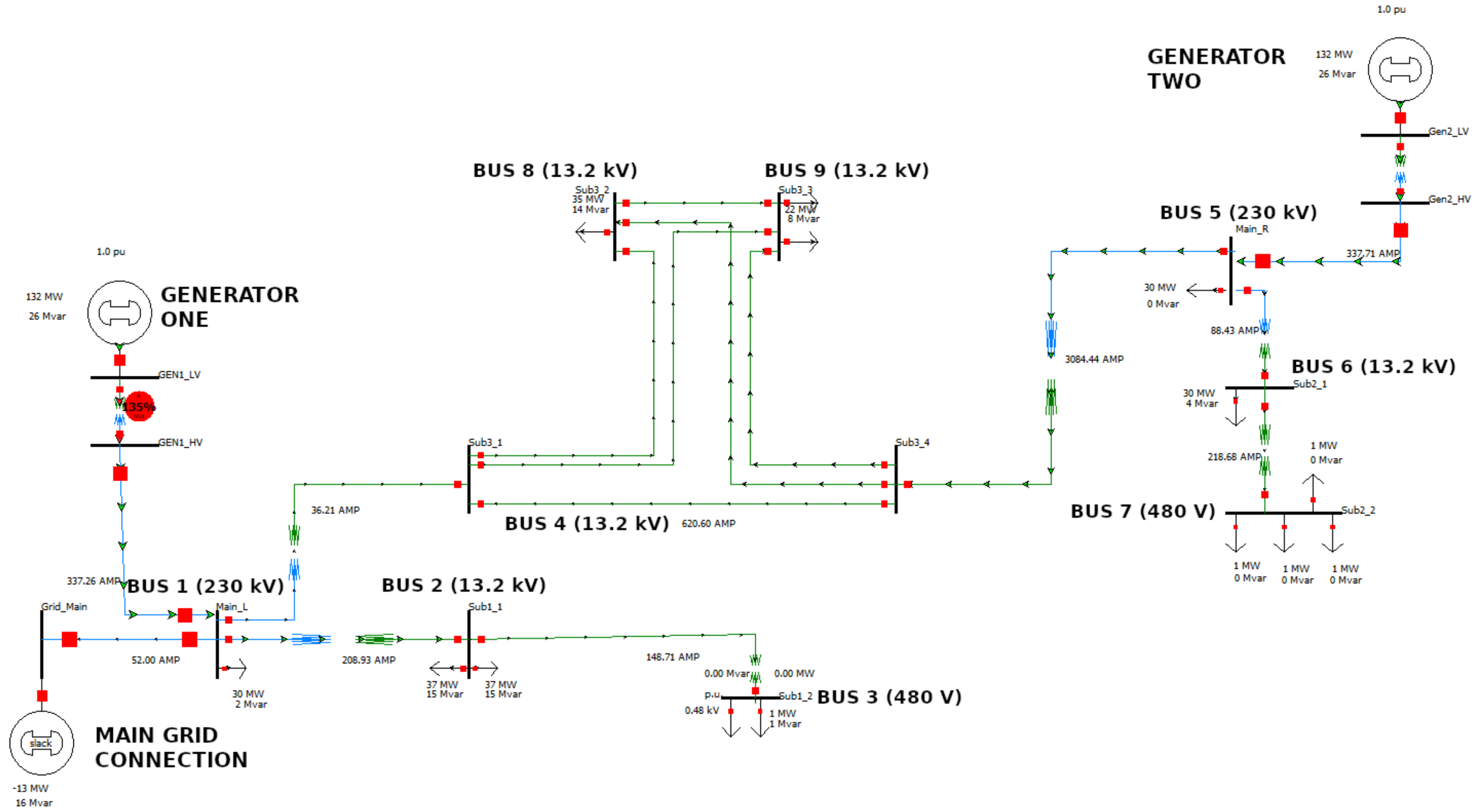


Figure 3.3: PowerWorld Simulation of the Microgrid Model

This analysis revealed that the loads in the simulation were not absorbing a realistic amount of power compared to examples from a real power system. To correct this, the load set-points were updated to better represent a typical power system, and in turn used to find new power set-points for the system's generators. These power set-points are then used by the system operators to control the power output of the generators in a manner similar to a power forecast used by actual power system operators using the SCADA master HMI.

### 3.3 EMTDC Simulation and Analysis

The original system was designed to run in real time using the University of Idaho's real-time digital simulator (RTDS). The RTDS is a specialized computer made to run complex simulations and exchange data essentially in real-time with external protection and control hardware. RTDS simulations have several advantages over traditional physical model power systems and off-line simulations. Physical model power systems allow for real-time testing and analysis but are difficult and time consuming to modify. Off-line simulations are easy to modify and do not require any special hardware to run but cannot exchange data in real-time with control devices and cannot fully model that hardware. Real-time simulations combine the best traits of both physical model power systems and off-line simulations allowing the system to be modified quickly and easily while still allowing data to be collected and the system to be controlled in real-time on the scale of the control hardware. However, they have their own drawbacks – most notably, the need for specialized hardware to run the simulation. Since the RTDS can only run one simulation at a time, it can be difficult to schedule time for making and testing improvements on the system. Additionally, RTDS simulations run constantly and it can be difficult to properly analyze the effect certain changes may have on the system. To help develop improvements to the real-time simulation, an offline time domain simulation of the system was developed to test and verify modifications before they were applied to the actual system. The PSCAD/EMTDC graphical interface for the simulation is shown in Figure 3.4.

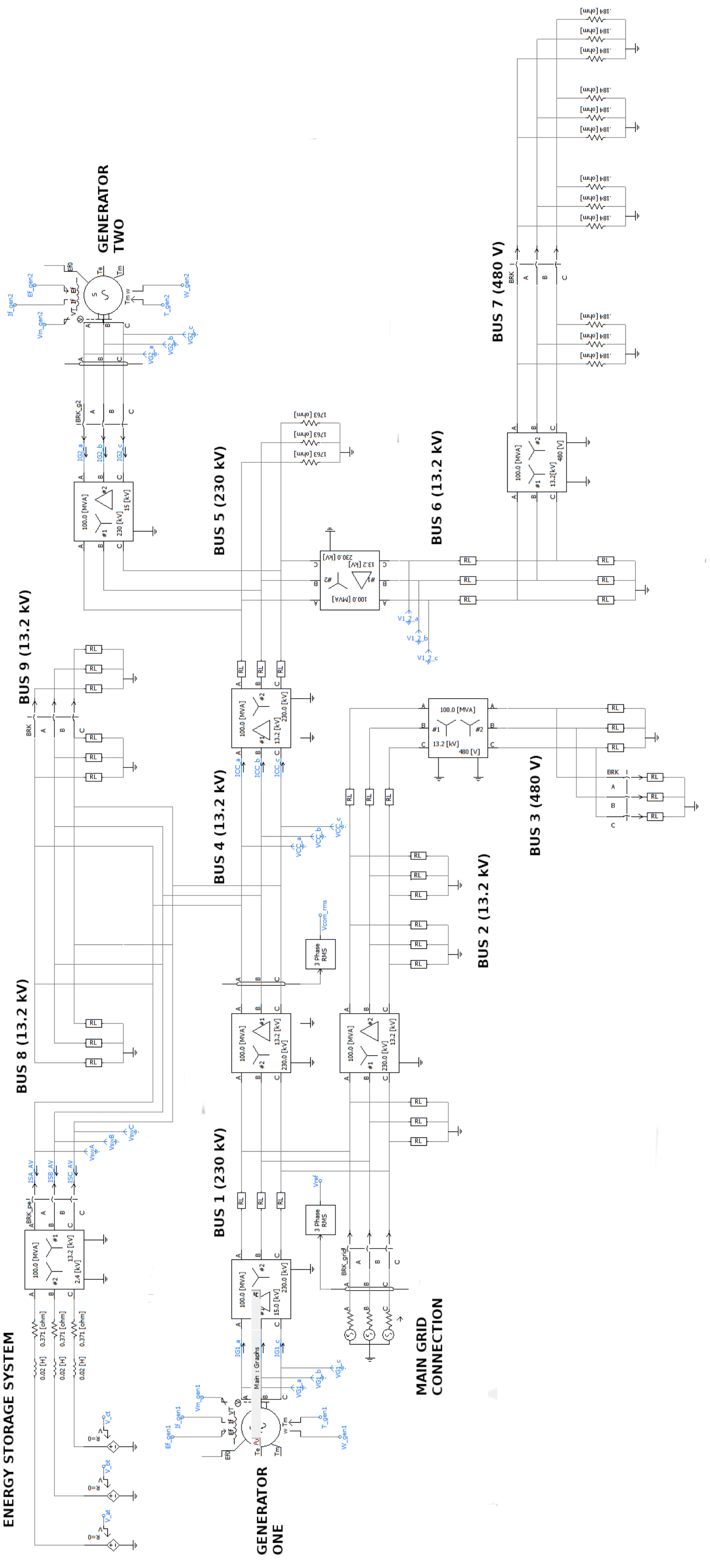


Figure 3.4: PSCAD Schematic for the Offline EMTDC Simulation

The offline simulation has many advantages bridging the transition between the PowerWorld simulation and the real-time simulation when designing and testing the improved generator control schemes and the energy storage system controls. First, the offline simulation allows the dynamic behavior of the system and controls to be verified. By creating a simulation model identical to the real-time simulated system, it can be shown that the system is functioning properly. Second, an advantage of the offline simulation is its ability to run on any windows computer with no special hardware required. This decreased development time significantly since time did not need to be scheduled to run tests on the RTDS. Third, real-time simulations must be separately compiled and then downloaded to the RTDS each time changes are made to the system. Conversely, the offline simulation can be compiled and run locally helping to speed up development even more. The fourth and last advantage of the offline simulation is its ability to easily define and reproduce test conditions during development before they go to the RTDS. As noted earlier, simulations on the RTDS are constantly running and make it difficult to replicate test scenarios when designing system improvements because of the introduction of undesirable extra variables. Therefore, designing and testing system improvements is much easier in the offline simulation than in the real-time simulation. The use of the PSCAD/EMTDC simulation will be covered more in depth in later chapters related to the design process of the generator control scheme and the energy storage system.

### 3.4 Chapter 3 Summary

This chapter explored the original system that was used as a basis for ICS testbed and focused on the original system's design and functions along with its shortcomings. It then examined the different simulation tools needed to properly analyze and improve upon the system. This included a PowerWorld® simulation used to analyze the steady state power flow of the system. It also covered the design and modeling of an offline simulated version of the system along with its uses and advantages over the real-time simulation for developing and testing model improvements on test cases before running them on the RTDS. A second drawback of the preliminary system developed by the previous student was the over simplified communication network. Chapter 4 will discuss the modifications made to expand upon that network.

# Chapter 4: SCADA System and Hardware Setup

## 4.1 SCADA System Overview

Industrial control systems rely on a multitude of hardware devices to monitor and control large scale systems. Power systems typically employ multiple devices located at substations to both monitor normal operation and protect the system from power swings and faults. RTUs, PMUs, and relays are used to measure the voltage, current, power factor, and power flow through the transmission and distribution buses. Relays are also used to control circuit breakers in case a fault or any other dangerous conditions occur. These relays usually function automatically in response to dangerous conditions, such as overcurrent or overvoltage conditions in the substations. Since these conditions can cause significant and lasting damage to the power system, multiple detection schemes have been designed and employed to detect these events as quickly and accurately as possible to prevent system failures or false positives from occurring. Relays are also typically connected to IEDs which act as data collectors and local controllers. These IEDs collect and report local data to a control center along with event records during trip events. They can also send independent trip commands from operators to the relay or breakers during abnormal system conditions, such as grid instability or large power swings, that could go undetected by the relay's protection schemes.

Relays and IEDs typically communicate using specialized communication schemes. These include analog serial schemes in older installations and Ethernet communication schemes in newer stations using MODBUS, GOOSE messages, or other proprietary vendor based protocols. These communication schemes are generally deployed between devices located within the same substations since they are designed to quickly report data and send event files from the system. For communication between different substations and the operator control center more scalable schemes with a slower refresh rate are used like DNP3. DNP3 can be implemented as a master-slave protocol in which the master polls the slaves for data at fixed intervals. There is an option for the slaves to instead send unsolicited packets; however, due to the risk of network congestion and packet collisions, the use of unsolicited packets should be limited to only critical messages such as fault alarms or for remote buses with very limited communication bandwidth and low loading. To reduce packet size and improve transmission speeds, DNP3 has an option to employ a dead-band for data points. In such cases, updated data points will only be sent when their values change enough to overcome this dead-band, usually between one and five percent of the previous measured value [5]. In large power systems DNP3 messages are usually polled on a relatively large time frame of between 10 seconds and a minute depending on the criticality of the data points to the system. This is due to the large number of substations, low communication bandwidth, and large size of the data packets.

Data collected by IEDs are typically sent over DNP3 to a central control system referred to as the SCADA master. The SCADA master sends the polling requests and receives responses from other devices. The SCADA master consists of an HMI used by operators to observe and control the system, software to perform post-processing on the measured data, and a data historian used to record the system's data points for future review and analysis. HMIs display an overview of the processed system data and are usually focused on the bus voltages and power consumption. From here, operators can make changes to the system's power generation and load status to regulate the system. As discussed in later chapters of the thesis, the power generation and consumption of the system must be closely matched to keep the system in within its desired operating regions. By observing the values at the system's buses, operators can update the power generation setpoints of the system, and even shed non-critical loads during critical times in a demand response scheme. Operators typically rely on load power forecasts to set the power generation for the system throughout the day. These forecasts are derived by observing the typical power use of the system from previous days and months and adjusted based off other factors, such as the weather forecast. The forecasts are also based on the predicted power generated from renewable resources, such as wind and solar power. Since the output of most most renewable energy sources generate power depending on the weather, they are usually configured to transfer the maximum power produced to maximize revenue for their owners. To account for this, non-passive resources, like gas and hydro plants, should vary their power production to balance load to maintain system frequency within standard regulations. Utility companies pay heavy fines if they fail to meet these standards. The ICS testbed incorporated the system elements discussed above into its SCADA system design to realistically imitate a power utility SCADA system.

The current goal of the ICS testbed is to generate, capture and analyze realistic network traffic of a power utility system to observe the effects of potential cyber-attacks on the power system. This data is used to find ways of detecting cyber intrusions and prevent the negative effects they can have on the system. To accomplish this, the network traffic between the devices must accurately mimic the traffic found in a real SCADA system.

### 4.2 Simulated Substation Setup

To accurately simulate a typical power system's SCADA system four racks with substation communication and control hardware have been setup and configured to duplicate real substations. Each rack consists of a protective relay, a RTAC, an industrial computer running Windows 10, a satellite clock, a software defined network switch, and a network security gateway. Additionally, each rack also contains a SEL Axion controller, a unit consisting of different modules including a protective relay, RTAC, and digital and analog inputs and outputs. The Axion devices can replicate several different SCADA devices; however, due to time constraints, they have not been properly integrated into the ICS testbed at the time this was written. Each substation is responsible for monitoring a different part of the system. Therefore, the microgrid was separated into four main parts consisting of the two lower left distribution buses (Substation one), the two lower right distribution buses (Substation Two), the three upper center distribution buses (Substation Three), and the remaining transmission buses connected to the local generators, the energy storage system, and the main grid connection (Substation Four). Figure 4.1 shows the monitoring area for each substation.

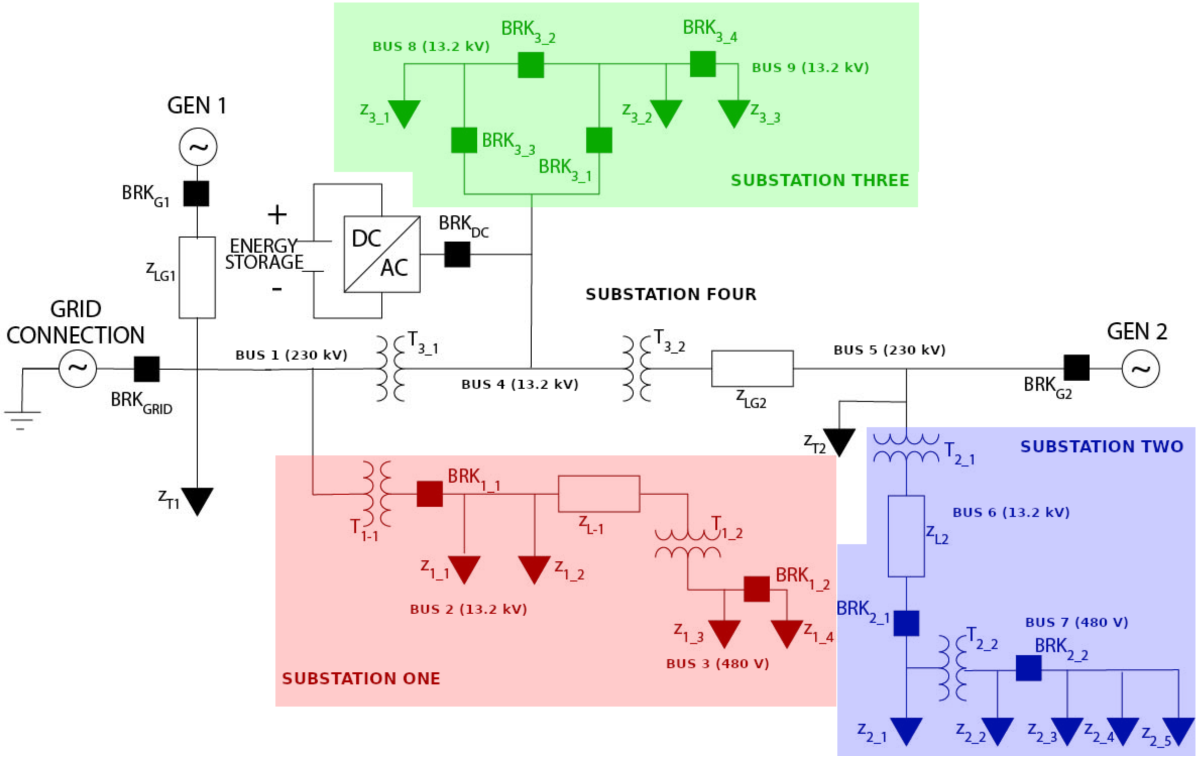


Figure 4.1: Substation Monitoring Locations

The substation relays are primarily configured to generate SCADA measurements from the system. Low voltage analog signals are sent from the RTDS to some of the relays using the relays' low voltage test interface. This method allows the relays to generate accurate real-time measurements from the system without the use of voltage amplifiers. The measurements are then sent to substation RTACs over serial communication using SEL's interleave fast meter scheme [10]. Due to the RTDS's limited number of analog outputs, only two relays could be configured to act as measurement devices at this time. The configured relays monitor the voltage, current, power factor, and frequency at the end buses of substations one and two. The potential future uses of the remaining relay will be discussed in more detail in the future works section of this thesis.

The substation RTACs are configured to collect data from the simulation and pass that data to the SCADA master using DNP3 over Ethernet. The simulated system runs at an accelerated rate to simulate a twenty-four-hour day in twenty-four minutes. To account for this, the polling rate for the SCADA master was increased to better represent the rate data is collected in a real power SCADA system. The polling rate was set to a one second interval between each polling cycle. As previously stated, analog measurements can only be taken from two of the four relays. To compensate for this, the remaining system measurements are sent directly from the RTDS to the substation RTACs via the GOOSE messaging protocol. This simulates the communication that would normally occur between a RTAC and either a PMU, meter, or relay. Currently, the RTACs simply act as data collectors instead of actual system controllers, and all control signals are sent directly from the SCADA master to the RTDS. The potential for moving the control signals from the SCADA master to the RTACs is discussed in more detail in the future work section of this thesis.

The substation rack computers are used to configure each individual device in the rack. They can also be used to monitor the metering and event data from the relays and RTACs in their racks.

The switches were configured to allow the different pieces of substation equipment to communicate with each other over Ethernet. The SDN switches can be configured to prevent unauthorized communications between different devices and from outside connections. This makes the system significantly more resistant to cyber-attacks. However, due to the type of cyber-attacks currently being carried out on the ICS testbed at the request of the research sponsor this functionality has not been implemented, since it would effectively prevent these attacks from being carried out. These security elements could be implemented at a later date once effective attacks have been designed with them in mind. A block diagram of the configuration of the system as a whole can be seen in Figure 4.2.

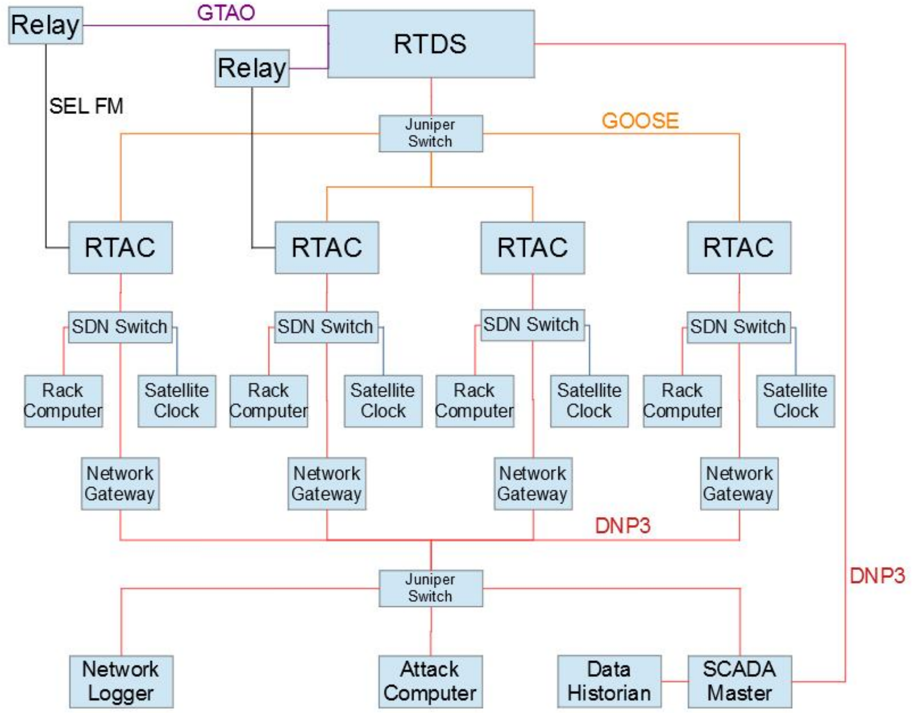


Figure 4.2: SCADA System Hardware Setup Block Diagram

### 4.3 HMI and Data Historian Setup

The HMI was built using GE iFix to give an operator level overview of the system's measurement data along with the status of the breakers. It also shows the power output of local generators, the energy storage system, and the main grid connection. Data is received from the substation RTACs over DNP3 and is stored in iFix's local database. Control signals, such as the power set-points or breaker trip and re-close commands, are sent back directly to the RTDS over DNP3. Figure 4.4 shows the HMI as seen by the operators.

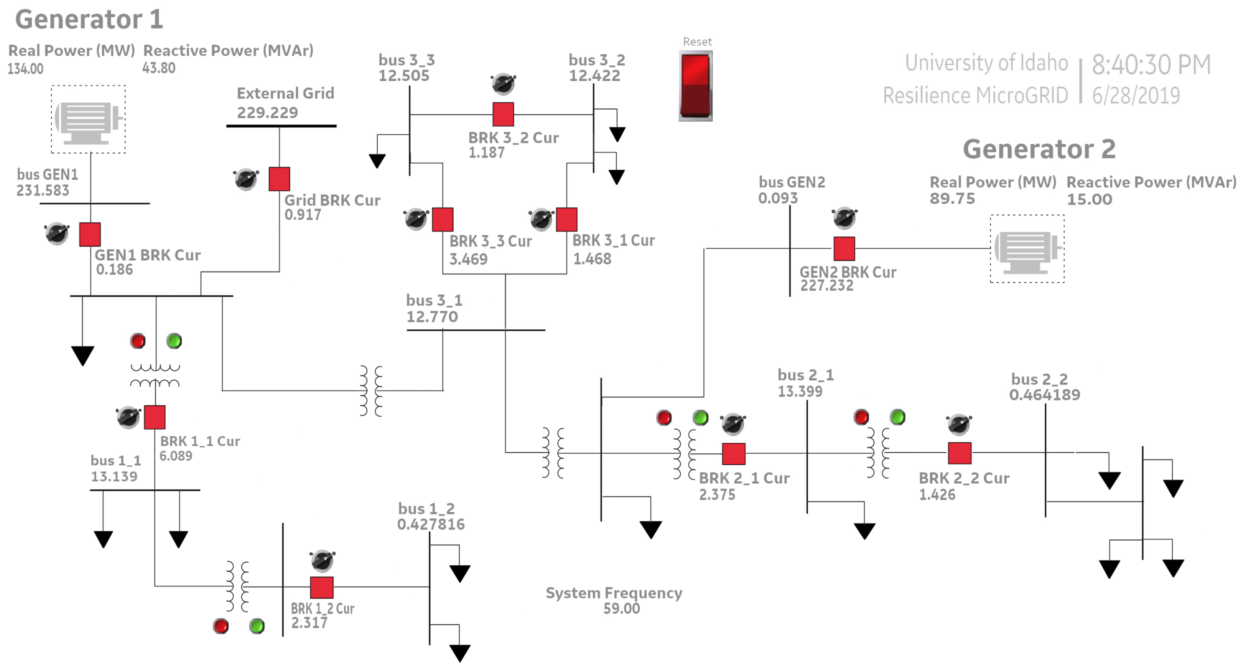
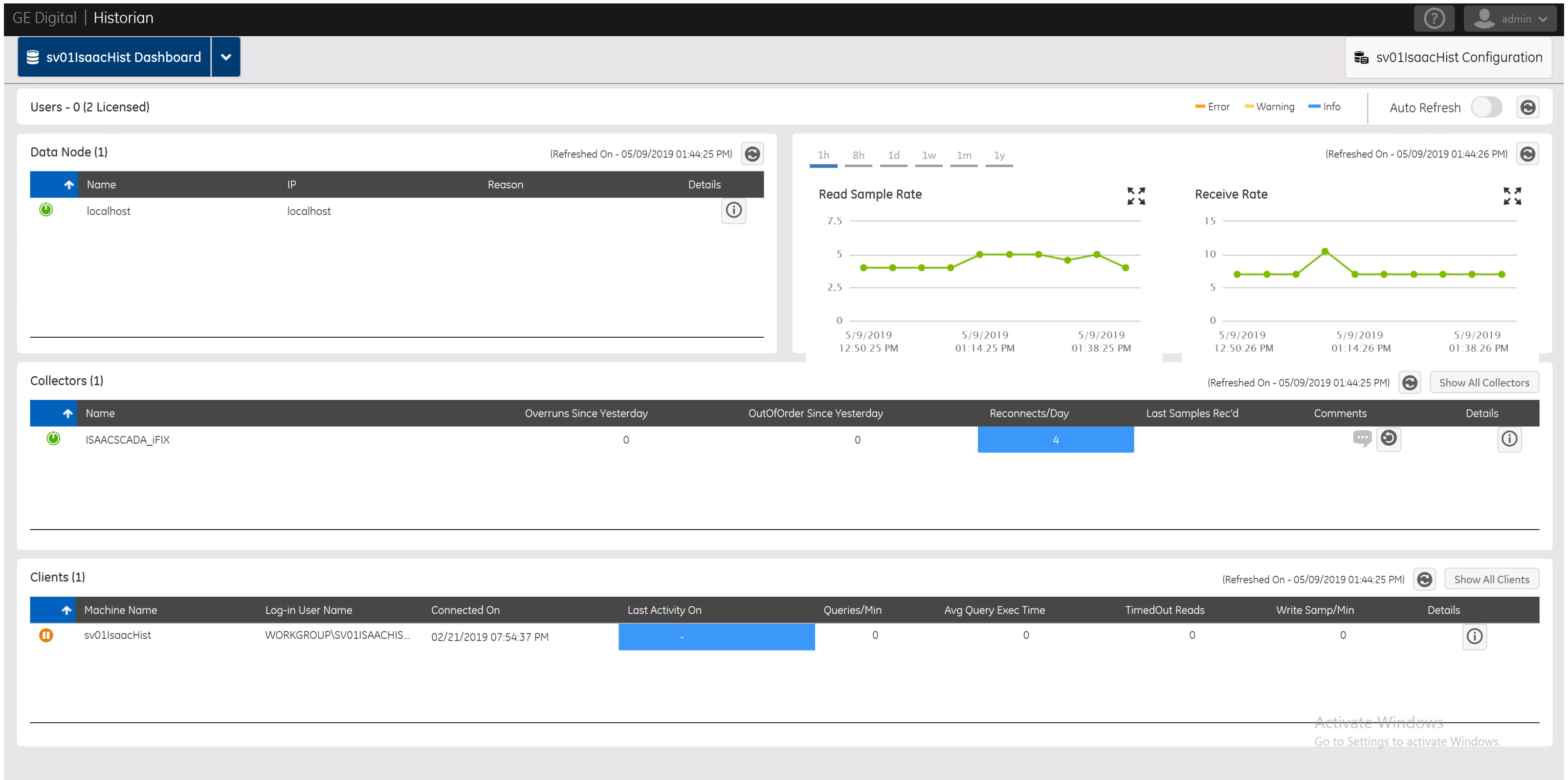


Figure 4.3: Operator HMI in GE iFix

Every time new data is polled from the RTACs, the data historian is updated, and the new data is recorded in its archives. The data historian is configured to monitor various tags in the HMI database that correspond to different system measurements. The historian can also output the recorded data as a CVS file for future analysis. This recorded data can be used as a comparison to the data points recorded by monitoring and dissecting the captured network packets, thus acting as a method of verification for the system's performance. The data historian interface is shown in Figure 4.5.



Users - 0 (2 Licensed)

Data Node (1) (Refreshed On - 05/09/2019 01:44:25 PM)

| Name | IP | Reason | Details |
|---|---|---|---|
| localhost | localhost | | |

(Refreshed On - 05/09/2019 01:44:26 PM)

Collectors (1) (Refreshed On - 05/09/2019 01:44:25 PM)

| Name | Overruns Since Yesterday | OutOfOrder Since Yesterday | Reconnects/Day | Last Samples Rec'd | Comments | Details |
|---|---|---|---|---|---|---|
| ISAACSCADA_iFIX | 0 | 0 | 4 | | | |

Clients (1) (Refreshed On - 05/09/2019 01:44:25 PM)

| Machine Name | Log-in User Name | Connected On | Last Activity On | Queries/Min | Avg Query Exec Time | TimedOut Reads | Write Samp/Min | Details |
|---|---|---|---|---|---|---|---|---|
| sv01IsaacHist | WORKGROUP\SV01ISAACHIS... | 02/21/2019 07:54:37 PM | - | 0 | 0 | 0 | 0 | |

Figure 4.4: Data Historian Interface

The HMI and data historian are hosted on a series of virtual machines (VM) running on the University of Idaho server rack. Alongside these VMs, multiple other VMs have also been setup that are responsible for recording the system's network traffic and launching cyber-attacks on the system. By virtualizing these machines, they can easily be dynamically scaled based on the processing and memory needs of each system. It also allows for the system to be remotely accessed from either the RTDS lab, the RADICAL lab, or the IRIC building at any time and keep the systems consistent between each of the different locations.

## Chapter 4 Summary

This chapter covered the basics of industrial SCADA systems used in power systems. This includes the general setup of different devices in the system and their roles, along with the common communication schemes used to connect these devices. The chapter then went over the hardware setup of the ICS testbed and the role of the various pieces of substation equipment.  Finally, it covered the implementation on the HMI and the data historian used by system operators.

# Chapter 5: Generator Controls

## 5.1 Synchronous Generator Overview

The hydro generators used in the simulation are comprised of two key-components: a three-phase synchronous machine and a hydraulic turbine. The turbine applies torque to the synchronous machine's rotor, causing it to spin within the applied excitation field and converting mechanical energy to electricity that can be utilized as a power source for the microgrid. In steady-state conditions, a balanced generator rotor will spin at a fixed speed related to the electrical frequency of the system and the number of poles. This relationship is expressed in (5.1) where n is the synchronous speed in revolutions per minute, *f* is the frequency in Hertz, and *P* is the number of poles the machine has.

$$n=\frac{120*f}{P} \tag{5.1}$$

If the ratio of the real power output by the generator and the input from the turbine is unity, then the rotor speed, along with the electrical frequency, will remain constant. If more mechanical power is applied than the loads require, then the excess energy is converted to kinetic energy on the rotor, the rotor speed will increase along with the frequency. If less mechanical power is applied than the system requires, then the frequency will decrease. This relationship can be used to actively control the system's frequency by regulating the amount of mechanical torque applied to the rotor shaft [9]. When connected to the grid, the system frequency will be regulated to the grid's frequency if the total capacity of the main grid’s generators are significantly greater than those of the microgrid. During this time, any imbalance between the amount of real power generated and used by the local generators and loads will be compensated by the grid's power balance. However, once the microgrid has entered islanded mode, the system frequency will begin to drift with power imbalances in the system. To prevent this change in frequency, the real power production of the generators must be actively controlled by a govener to match the power requirements for the loads as they change over time.

The voltage produced at the generator's terminals is directly controlled by the synchronous machine's magnetic field produced by the excitation coils in the rotor. When the rotor is spun a magnetic field applied to the stator windings, a voltage is produced at the terminals proportional to the current applied to the exciter coils. This relationship between the terminal voltage and the exciter's voltage is used as a basis for controlling the AC terminal voltage created by the generator. However, due to losses and inductive voltage drops over the transmission lines, the voltage at the generator's terminals will not equal the voltage found at the distribution bus. It can be difficult to maintain the transmission bus voltage by only regulating the generator terminal voltage. The reactive power of the system can be correlated to the voltage level similar to how the real power can be related to the system frequency [9]. For this research project the system was designed to have the operator set a reactive power setpoint for the generators, although this method of control is rare in practice.

### 5.2 Generator Real Power Control Design

The generator turbine controller uses an IEEE type 1 turbine-governor model [11]. As previously discussed, the electrical power output of the generator at synchronous speed is directly related to the mechanical torque applied to the rotor shaft by the turbine. The controller has two inputs: the reference speed and the real power. The rotor speed is compared to the rated speed and the error is passed to a pole-zero pair with an applied gain. The output of this controller is fed back into the main feedback loop along with the power set-point. The speed controller output and the feedback from the feedback loop is subtracted from the power set-point. The difference is then divided by a time constant to produce the rate of change which is integrated to produce the position of the turbine. Additionally, both the rate and position outputs are limited by the mechanical limitations of the generator. The position is then fed back to the power set-point and the speed controller output. The turbine position is then divided by a single pole with only a time constant. The output is multiplied separately by a gain and another single pole with a time constant and a gain. These two values are then added together again. Finally, this output is divided by the generator speed to find the mechanical torque needed to produce the desired electrical power. The complete controller for the system is shown in Figure 5.1.

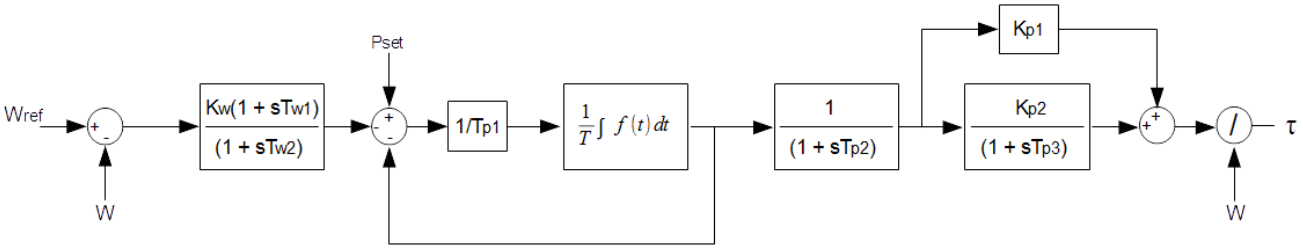


Figure 5.1: Speed Governor Controller

The constants and time constants for the speed governor controller are shown in Table 5.1.

Table 5.1: Governor Parameters

| | Generator 1 | Generator 2 |
|---|---|---|
| Kw | 25 | 15 |
| Tw1 | .8 | 1 |
| Tw2 | .05 | .25 |
| Tp1 | 0.25 | 0.25 |
| Tp2 | 0.01 | 0.01 |
| Tp3 | .005 | .005 |
| Kp1 | 0.7104 | 0.7152 |
| Kp2 | 0.456 | 0.48 |

These values were found using the offline simulation to improve the ease of testing and tuning the governors. Generator one was tuned initially by disconnecting the other power sources, generator two and the main grid, and placing the rotor into a locked state were the simulation regulated its rotation to the generator’s rated speed. This was done to reduce the number of variables that needed to be considered when testing the initial parameters. The initial parameters were chosen based off common values for other similar controllers. These initial values were then tuned by hand until a satisfactory response was produced. Once sufficient values were found the rotor was unlocked and its speed was allowed to vary. The speed governor was then tuned until the rotor speed could be accurately maintained. The process was then repeated for generator two using the controller values found for generator one as a starting point. Once both generators had been configured individually they were both connected at the same time, along with the main grid connection, and then fined tuned to reduce any unintended interactions.

### 5.3 Generator Reactive Power Control Design

As stated previously, the generator's reactive power is regulated by controlling the exciter's voltage which in turn regulates the field current. The control loop for the generator's exciter is based off an IEEE type ST1 excitation system [12]. The reactive power controller can be separated into three main parts: the reactive power controller shown in Figure 5.2, the voltage controller seen in Figure 5.3, and the exciter voltage and current limiter found in Figure 5.4. The reactive controller compares the operator's set-point to the generator's reactive power output to create an error value. The error is then passed to a zero-pole pair controller that regulates the error to zero. The reactive power controller is shown in Figure 5.2.

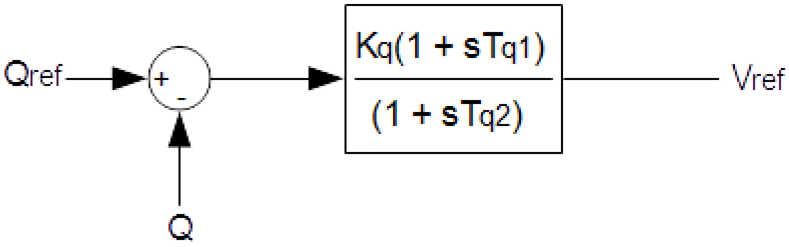


Figure 5.2: Reactive Power Controller

The output of this controller is used as the reference voltage for the voltage control loop. The voltage control loop uses the terminal voltage and current as feedback for the system and the reference voltage derived from the reactive power setpoint. The terminal voltage and feedback from the applied voltage is compared to the reference voltage to generate an error value. The error value is then passed to a controller consisting of one zero and two poles and multiplied by a gain. The output of this controller is used as feedback and fed to a control block with a zero at the origin and a pole before being compared to the reference voltage. The Voltage Controller is seen in Figure 5.3.

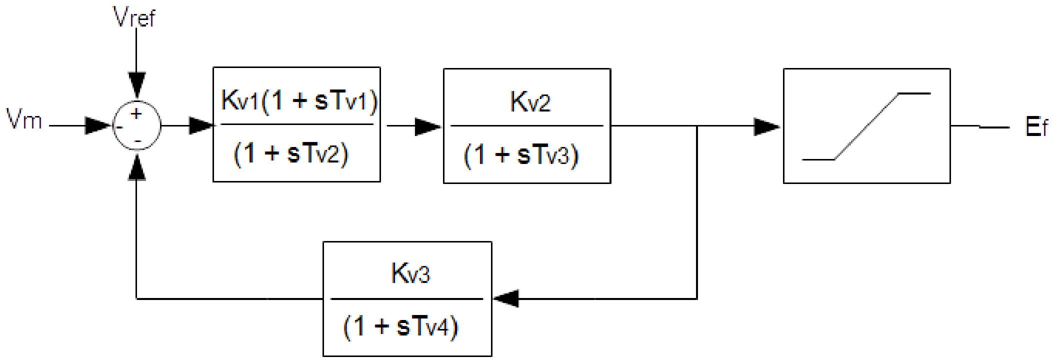


Figure 5.3: Voltage Control Feedback Loop

The output of the feedback loop is limited to prevent damage to the generator's windings. The maximum and minimum voltage is determined by multiplying the terminal voltage and current by the parameters designed to keep the generator operating within its safe limits. These parameters were determined by the size of generator and the typical voltage limits used by real world generators. The exciter voltage and current limiter can be seen in Figure 5.4

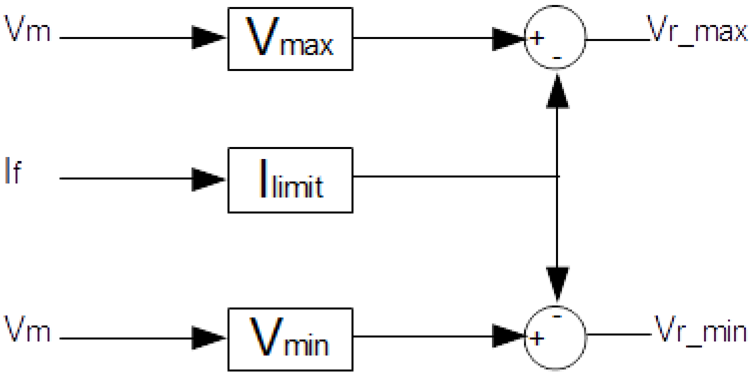


Figure 5.4: Exciter Voltage and Current Limiter

The parameters for the reactive and voltage controllers are shown in Table 5.2 and Table 5.3, along with the constants for the exciter voltage and current limiter, Table 5.4.

Table 5.2: Reactive Power Controller Parameters

| | Generator 1 | Generator 2 |
|---|---|---|
| Kq | 30 | 30 |
| Tq1 | 0.03 | 0.03 |
| Tq2 | 3.2 | 3.2 |

Table 5.3: Voltage Controller Feedback Loop Parameters

| | Generator 1 | Generator 2 |
|---|---|---|
| Kv1 | 1 | 1 |
| Kv2 | 20 | 20 |
| Kv3 | .01 | .01 |
| Tsv1 | .2 | .2 |
| Tsv2 | .01 | .01 |
| Tsv3 | .01 | 0.01 |
| Tsv4 | .2 | .2 |

Table 5.4: Exciter Voltage and Current Limiter Parameters

| | Generator 1 | Generator 2 |
|---|---|---|
| Vmax (kV) | 5.7 | 5.7 |
| Vmin (kV) | -4.9 | -4.9 |
| Ilimit (kA) | 0.175 | 0.175 |

The reactive power controllers were tuned in a similar manner to the speed governor controller were each generator was first tuned individually. Additionally, as with the governor controller the exciter voltage controller was first tuned on its own without the reactive power lead-lag controller. The voltage controller was tuned by first choosing initial values for the controllers. These initial values were then tuned, moving from left to right, to shape the generator's voltage response. Once the desired voltage response was achieved the reactive power controller was reconnected and tuned. Generator two's values were then found and shown to need no additional tuning to produce a desirable response.

### 5.4 Controller Implementation and Results

The generators used in the simulation have a MVA rating 1220 MVA and a rated voltage of 15 kV, additionally their rated speed is 1800 RPM. The real and reactive power controllers were implemented into the simulated system so that operators could send set-points as reference values to the controllers. The controllers were tested by setting the generator outputs to a starting point of 100 MW and 100 MVAr. A step command was then sent to move the set points up to 110 MW and 110 MVAr and down to 90 MW and 90 MVAr. The controllers were first tested in the offline simulation and results can be seen in Figure 5.5, showing the real power response of generator one and two for the step-up test.

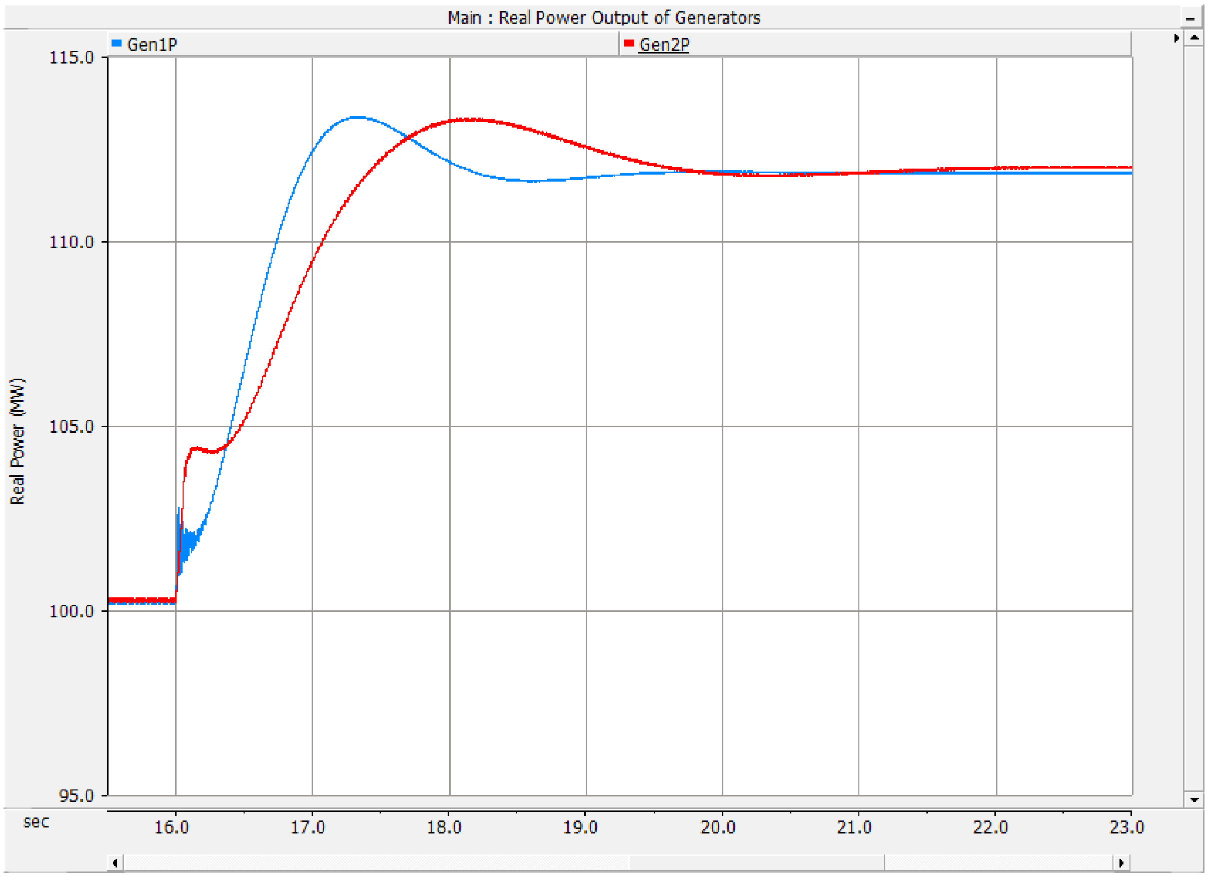


Figure 5.5: Real Power Response for Step-up Test in the Offline Simulation

The reactive power response for the generators during the same test can be seen in Figure 5.6.

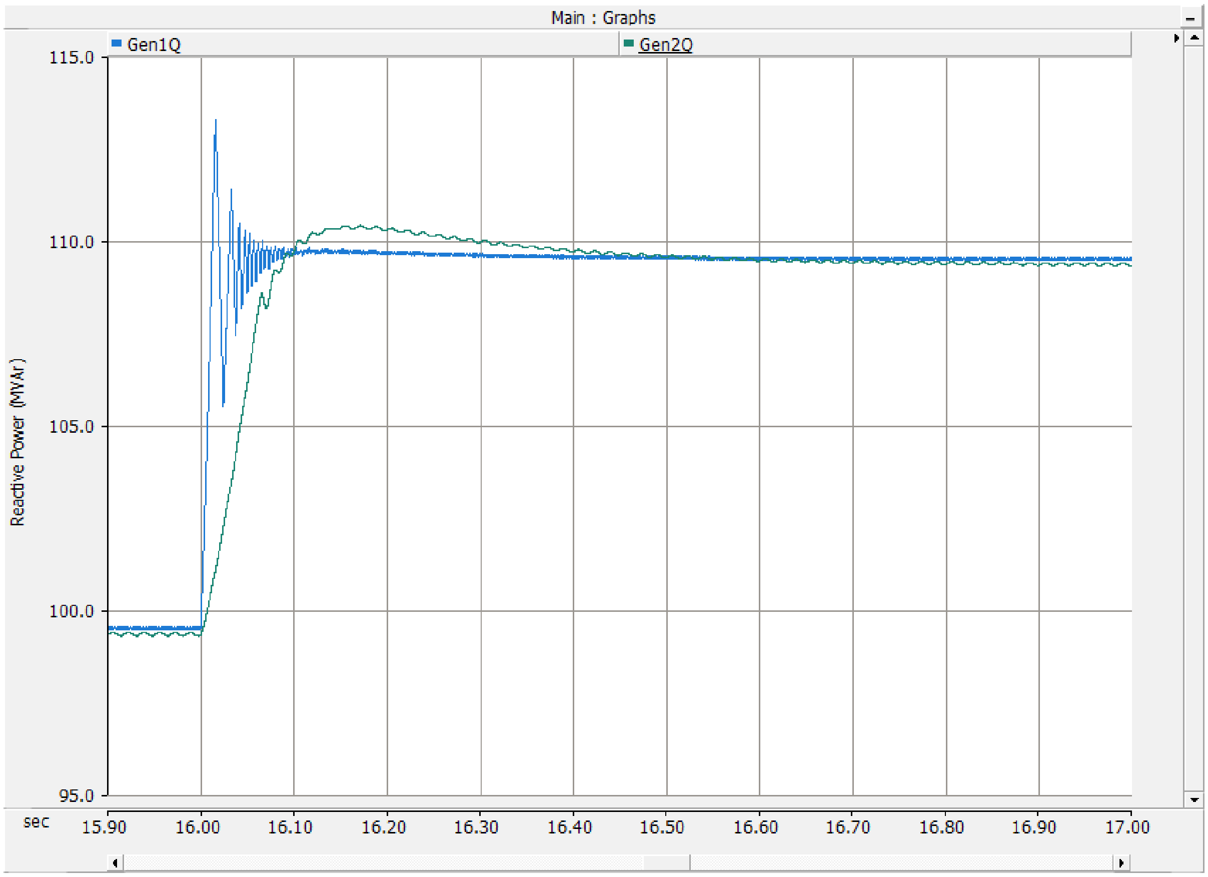


Figure 5.6: Reactive Power Response for Step-up Test in the Offline Simulation

The results for the step down test can be seen in the following figures with Figure 5.7 showing the real power response of the generators.

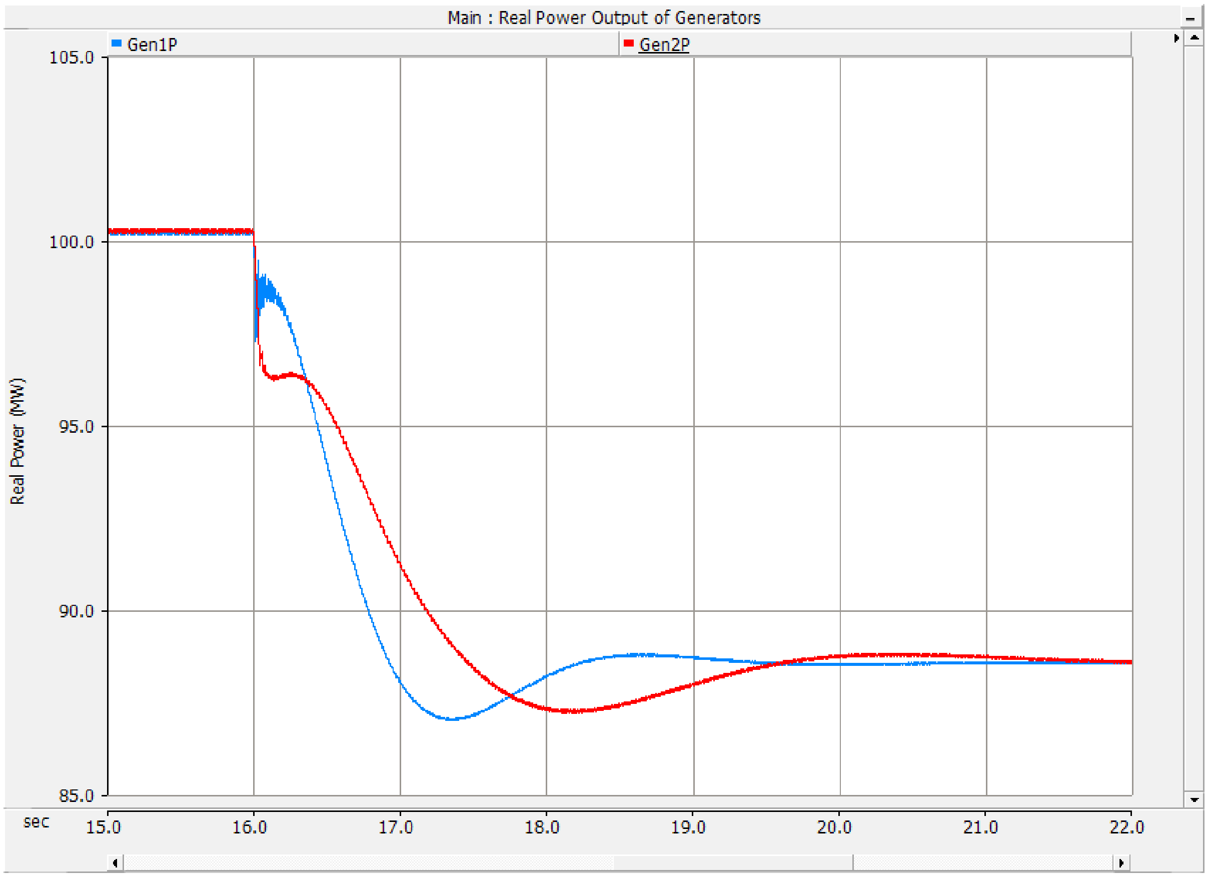


Figure 5.7: Real Power Response for Step-down Test in the Offline Simulation

Figure 5.8 contains the reactive power response for the step-down test.

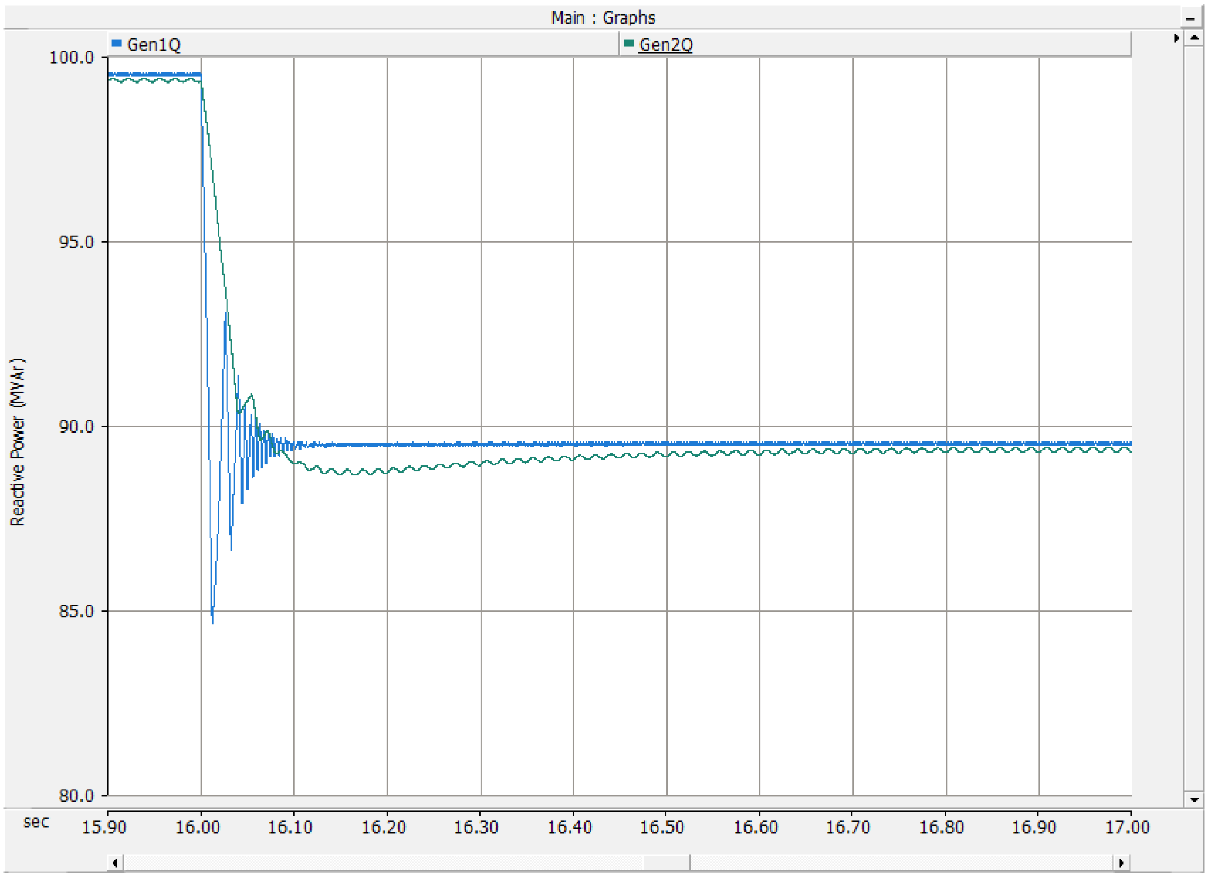


Figure 5.8: Reactive Power Response for Step-down Test in the Offline Simulation

The speed governor controllers have relatively long rise times, around one second for generator one and one and half seconds for generator two. Along side this both generators have relatively long settling times, approximately one and half seconds for generator one and two seconds for generator two. These long response time were considered acceptable since they are due to the inherent inertia of the rotors and turbines, and could not be effectively reduced by the governor. The governor produced little real power overshoot, around 2%, and a steady state error of approximately 2% at worst. From these results the governor controller was considered acceptable for design goals of this research project.

The reactive power controller responds much faster with generator one having a rise and settling time of around .03 seconds and .06 seconds respectively. Generator two responds slower with a rise and settling time of around .07 seconds and .23 seconds. While slower these values were still sufficent for the goals of this research project. Generator one experience an overshoot of around 5% for the reactive power, which while not ideal was still acceptable. Generator two’s reactive power overshoot was significantly smaller around 1%. Both generators experienced a steady-state error of less than 1%. From these results the reactive controllers were determined to be more than sufficient for the purposes of this research project.

After being designed and tested in the offline simulation the governor and reactive power controllers were then implemented into the real-time simulation. Once implemented the controllers were tested in the same manner with the results shown below. The real power output of the generators for the step-up test can be seen in Figure 5.9.

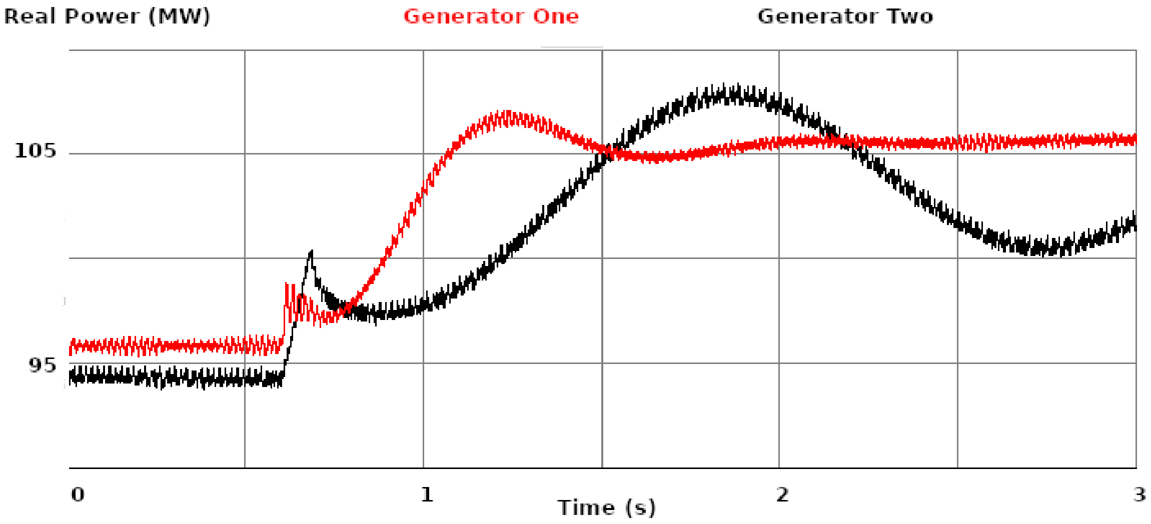


Figure 5.9: Real Power Response for Step-up Test in the Real-Time Simulation

Figure 5.10 contains the reactive power response for the step-up test.

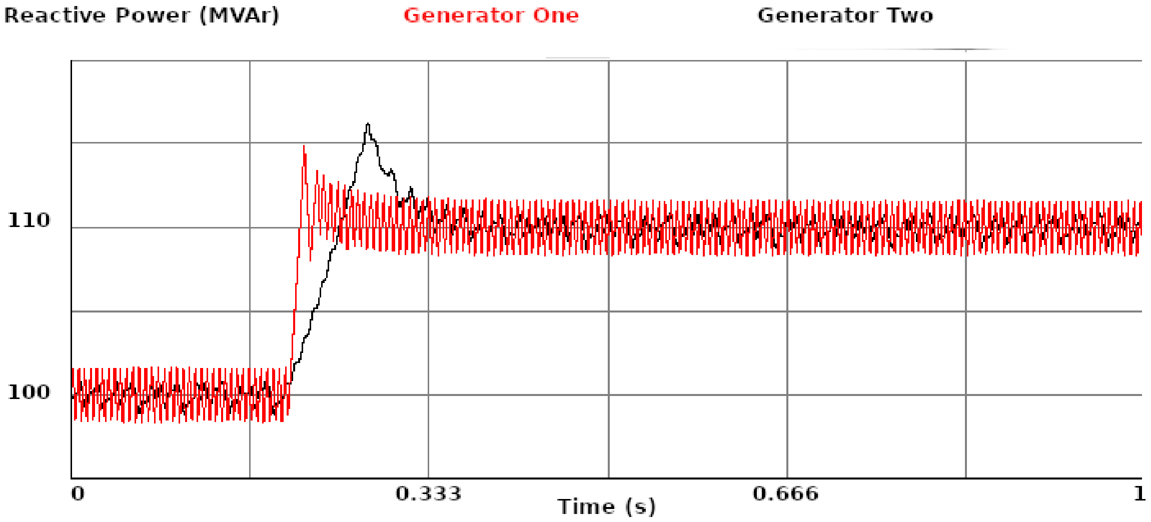


Figure 5.10: Reactive Power Response for Step-up Test in the Real-Time Simulation

The results for the step-down test on the real power output is seen in Figure 5.11.

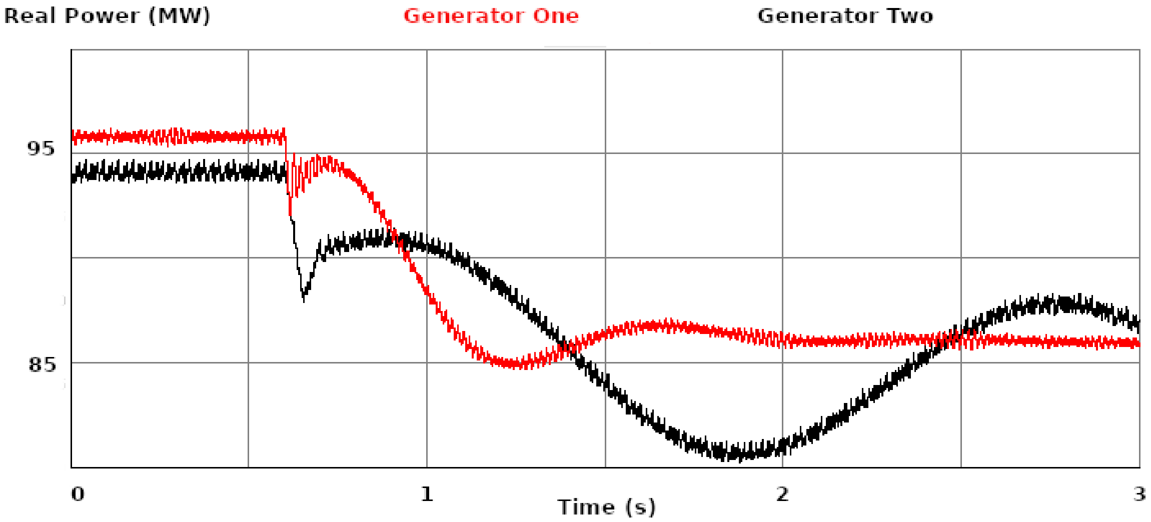


Figure 5.11: Real Power Response for Step-down Test in the Real-Time Simulation

The reactive power response ins shown in Figure 5.12.

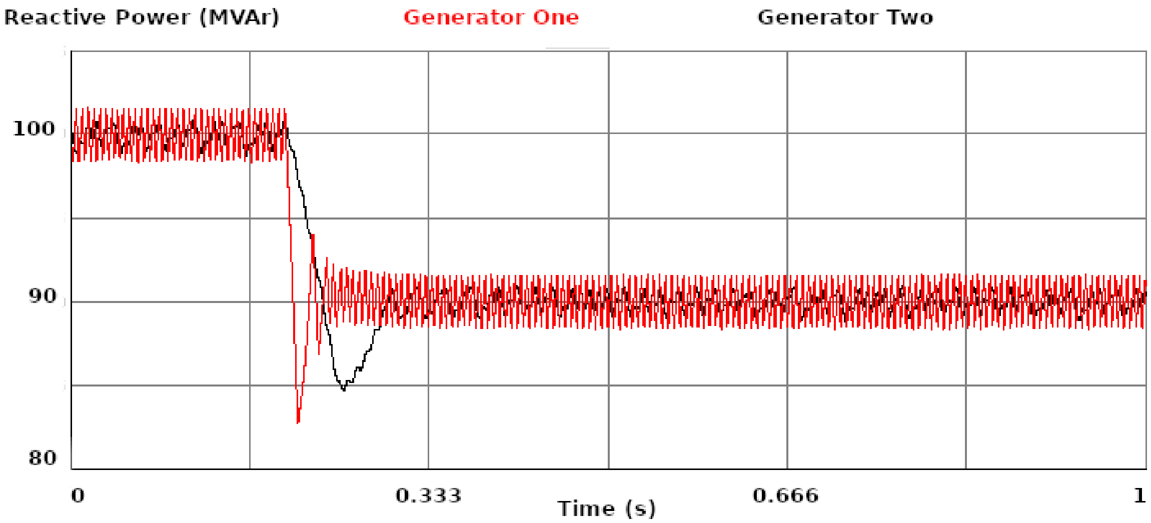


Figure 5.12: Reactive Power Response for Step-down Test in the Real-Time Simulation

The governor controllers performs similarly in the real-time simulation to how they did in the offline simulations. The differences can be attributed to difference in test conditions for each and could be reduced with minor fine tuning. Generator two performance closely matches that of the offline model, except for a small amount of added noise. Generator one's reactive power response also parallels the offline model, except it contains a third harmonic oscillation of approximately 4 MVAr. These under-damped responses could likely be reduced by finer tuning the voltage controller, however due to time restraints this could not be accomplished at this time. Despite these issues the governor and reactive power controllers will still be able to effective for this research project.

### 5.5 Chapter 5 Summary

This chapter covered the design and implementation of the generator control loops for the system's generators. It provided a simple overview of how synchronous generators function and how real and reactive power is controlled. The relationship between the mechanical torque applied by the turbine and the real power produced by the generator was discussed, along with the relationship between the voltage applied to the field windings and the reactive power produced. The design of the real and reactive power controllers was then discussed in depth covering their design, their parameters, and the methods used to tune them. Finally, the controllers were implemented into the offline and real-time simulations and the results were shown for typical step inputs that would be applied to the system. From these tests, it was determined that the controllers were operating properly, but suffered from varying amounts of noise. Despite this the controllers were concluded to be acceptable for the goals of this research project.

# Chapter 6: Energy Storage System Design and Implementation

## 6.1 Energy Storage System Overview

Energy storage systems are typically proposed to store excess energy during periods where the capacity of inexpensive generation exceeds load and supply extra energy during periods when expensive energy sources are not needed to meet load. The battery needs to be able to switch autonomously between charging and discharging depending on the system requirements. In a microgrid, it can be assumed that the system will always have adequate power when grid connected due to the grid supplying any needed power to the system. Therefore, when the microgrid is operating in grid-connected mode, the energy storage system will function as a static load unless its energy storage potential has reached maximum capacity. When shifted in islanded mode, the energy storage device will begin to operate dynamically by supplying and absorbing power from the system depending on the its power balance.

Detection of the microgrid entering and exiting islanded mode can be done in a number of ways. The easiest and simplest way is to monitor the breaker status of the grid connection. This method is easy to implement and has little chance of generating false positives but can cause the storage system to respond slowly to loss of grid power. Another method for detecting islanding of the system is to monitor the voltage or frequency of the system at the transmission bus and look for sudden changes. Since the main grid parameters should ideally keep the transmission bus stable at the rated voltage and frequency it can be assumed that large changes will only be experienced when the grid connection is lost, or a major disturbance has occurred [13]. This method has the advantage of not needing communication of the breaker status and allows for the system to detect a loss of grid connection if the grid is lost in anyway other than the through the use of the circuit breaker. It can, however, generate false positives in detection during power swings where the voltages and frequency oscillate [13]. Due to a lack of time, the second method could was not implemented into the system and its use in the system can be considered future work for the project.

The energy storage system consists of a three-phase converter bridge, a DC source, and a three-phase transformer used to step up the output voltage to the level of the transmission bus. The converter bridge is made up of series of insulated-gate bipolar transistors (IGBT) and diodes that allow current to flow back and forth based off a switching signal. These IGBTs are grouped into three pairs representing the three phases commonly used in utility power systems. The pairs of switching refrences are offset from each other by one hundred twenty degrees. They are comprised of a primary signal and an inverter signal such that the upper IGBTs are turned on and conducting while the lower IGBTs are turned off blocking current from flowing through them and vice versa. Current is allowed to flow back to the DC source through the paired diodes.

The power output of the AC-DC bridge is controlled by applying a modulation signal to the switching signal that controls the length of time each IGBT is turned on and off. Through this signal the amount of current that flows through the IGBTs, and accordingly the amount of power through the converter, can be actively controlled. This method of control is referred to as pulse width modulation and is commonly used to control the output of DC to AC converters [14]. Therefore, the output of the control loop must be converted into a modulation signal before it can be applied to AC-DC bridge. The modulation signal is used to control the voltage level and frequency offset of the AC output by varying the length of time the IGBTs are turned on. The real and reactive power output of AC-DC bridge is therefoe controlled by changing the angular offset and voltage level respectively. [14].

### 6.2 Energy Storage System Control Overview

To simplify the control scheme, the voltage and current measurements used in feedback are converted from the three-phase stationary ABC reference frame to a two-phase synchronous rotational DQ reference frame. The rotational reference frame transformation changes the output of the steady-state voltage measurements from a time varying sinusoidal waveform to a constant waveform similar to a DC signal. Additionally, the Q-axis voltage will be regulated to approximately zero by the synchronization control to simplify the calculation used in the current controller. This simplifies the calculations needed to convert the reference power set-points to current set-points that can be used to control the modulation signal. This allows the real and reactive power produced by the converter to be tied to the D and Q axis currents as shown in equations (6.1) and (6.2) [7].

$$P=\frac{3}{2}*(V_d*I_d+V_q*I_q+V_0*I_0) \tag{6.1}$$

$$Q=\frac{3}{2}*(V_q*I_d-V_d*I_q) \tag{6.2}$$

### 6.3 Storage System Design Goals

As shown in the previous chapter, the hydro generators supply the majority of the system power during normal steady-state operations. However, due to their inertia, they can be slow to respond to sudden changes in the power system — taking multiple seconds to respond to large system changes. During this time, the voltage and frequency of the system can vary wildly. To solve this problem the energy storage system was designed and implemented in the simulation to respond and supply the needed power during these transitional periods where the generator output does not match the systems power requirements, within the rated power limits of the converter and the energy capacity of the battery. Once the generators have adjusted their power output, the energy storage system should shift back into a neutral or charging state.

Normally the peak power capacity and energy capacity of the battery is a prominent design concern for an energy storage system, but since the generators keep the power stable during normal operations, the energy storage system should only be active during transitional periods as the generators move to new set-points. Since it can be assumed the battery will never be completely drained at any point during normal operations, the battery has been modeled as an ideal DC voltage source to simplify its simulation. For the previous assumption to remain true, the power output of the energy storage system must be limited to max power output of 40 MW and 40 MVAr at any time, based on the max power output of real world energy storage systems [4]. Additionally, the transmission bus voltage must be kept within an operating range of plus or minus five percent of the rated levels or 13.2 kV and the frequency kept within. 5 Hz of its nominal value of 60 Hz. Since the voltage limit of the IGBTs is far below the level of the transmission bus, a step-up transformer was employed to increase the voltage from 2.4kV to 13.2 kV. When in grid connected mode, the DC storage system was designed to act as static load absorbing 1 MW from the system to simulate charging the battery.

### 6.4 Droop Control Overview

As previously stated, the AC-DC converter's power output is controlled using real and reactive power set-points mapped to the Q and D axis currents. However, the energy storage system needs to be able to adjust its power output automatically to keep the voltage and frequency of the transmission bus within its operating region. Because of this, operator defined set-points cannot be used to control the energy storage system. To rectify this, droop control is employed to establish voltage and frequency set-points.

Droop control is used to relate the frequency and voltage magnitude to the real and reactive power output of the energy storage system. To do this, the current through the line impedance is used with the voltage drop over the impedance to find the power flowing out of the voltage source converter as shown in Figure 6.1 and (6.3).

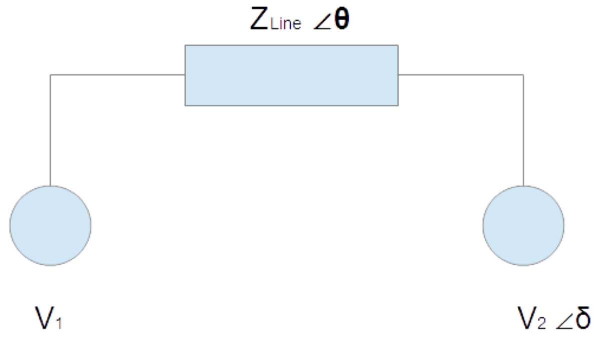


Figure 6.1: Voltage Source Converter Compared to Grid Side Connection

$$S=\frac{|V_1|*(|V_1|-|V_2|\angle\ \delta)}{Z_{Line}\angle\ \theta} \tag{6.3}$$

Where S is the apparent power, $V_1$ is the inverter voltage magnitude, $V_2$ is the system voltage magnitude, δ is the system voltage phase angle, R is the line resistance, and X is the line inductance. From here, the apparent power can be separated into the real and reactive power based on the real and imaginary components, as shown in (6.4) and (6.5).

$$P=\frac{|V_1|^2}{Z_{Line}}\cos(\theta)-\frac{|V_1|*|V_2|}{Z_{Line}}\cos(\theta+\delta) \tag{6.4}$$

$$Q=\frac{|V_1|^2}{Z_{Line}}\sin(\theta)-\frac{|V_1|*|V_2|}{Z_{Line}}\sin(\theta+\delta) \tag{6.5}$$

Typically, the inductance in a transmission line is much larger than the resistance. Therefore, the resistance (R) can be ignored. Additionally, it can be assumed that the phase angle of the system side voltage (δ) will be sufficiently small, so that sinδ = δ and cosδ = 1. With these assumptions the above equations can be simplified to:

$$\delta \simeq \frac{XP}{|V_1||V_2|} \tag{6.6}$$

$$|V_1| - |V_2| \simeq \frac{XQ}{|V_1|} \tag{6.7}$$

As shown in (6.6) and (6.7), the system voltage magnitude and phase angle can be related to the reactive and real power respectively. The phase angle is directly related to the frequency of the system with an inverse relationship to $V_1$. Through these relationships the real and reactive power of the energy storage system can be related to the frequency and voltage shown in (6.8) and (6.9) [15].

$$f_0 - f_{meas} = k_p * (P_{cmd} - P_{set}) \tag{6.8}$$

$$V_0 - V_{meas} = k_q * (Q_{cmd} - Q_{set}) \tag{6.9}$$

Where $f_0$ and $V_0$ are the nominal frequency and voltage for the system, $P_{cmd}$ and $Q_{cmd}$ are the baseline real and reactive power output, $P_{set}$ and $Q_{set}$ are the real and reactive power set-points sent to the converter controller, and $k_P$ and $k_Q$ are the linear gains used to convert between values and implement the droop. These gains remain linear for small changes in the voltage and frequency, and can be set to vary the power output based off small changes in the system's voltage magnitude and frequency measured at the point of interconnect between the storage system and the microgrid. The gain can be found using (6.10) and (6.11).

$$k_p = \frac{\Delta f}{\Delta P} \tag{6.10}$$

$$k_q = \frac{\Delta V}{\Delta Q} \tag{6.11}$$

Where Δf and ΔV are the difference between the system frequency and voltage and the reference frequency and voltage. Accordingly, ΔP and ΔQ are also the difference between the system's power output and the reference set-points. The gains can be arbitrarily set to control how much power the storage system either absorbs or releases to correct small changes in the voltage and frequency [16].

### 6.5 **Energy Storage System Design and Implementation in Fixed Time Simulation**

The energy storage system was first implemented in the offline simulation as a simplified averaged model. The simplified model uses controlled voltage sources instead of the switching model of the converter. These sources mimic the steady state and slowly varying dynamic operation of the converter. The use of this model helps simplify the designing and testing of the controller, by removing the complexity if the switching behavior from the system, such as the switching frequency harmonics. The averaged model is shown in Figure 6.2 [7].

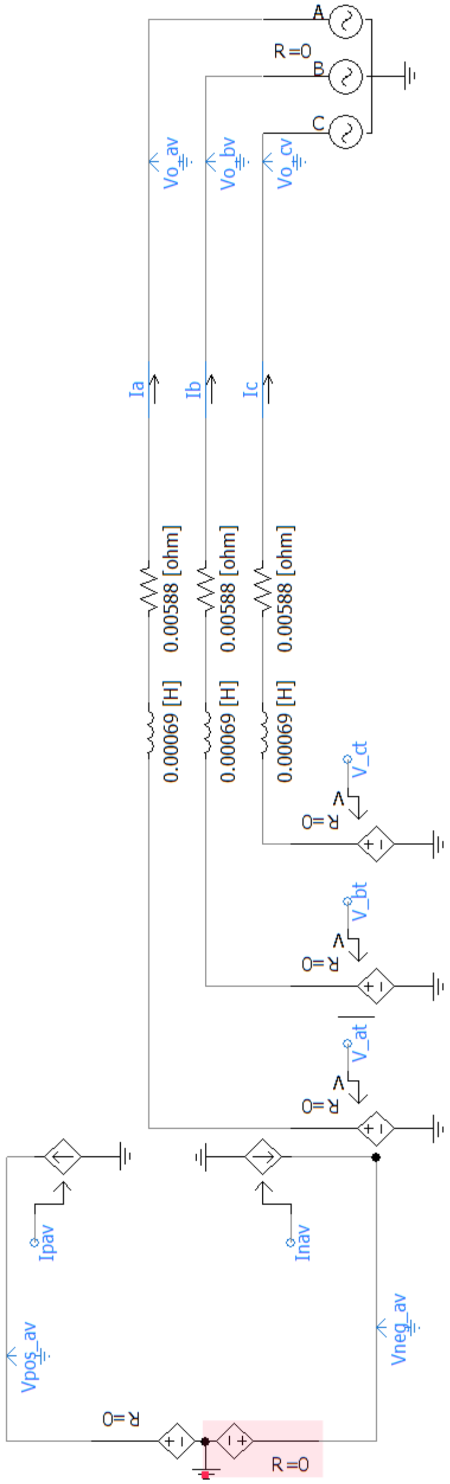


Figure 6.2: Averaged Model of a Voltage Source Converter

The energy storage system was placed at bus 4, the common connection between the two generators. A transformer was used to step the voltage of the inverter from 2.4 kV to the bus voltage of 13.2 kV. The droop gain was set based off the desired maximum power output for the storage system with respect to changes in the system frequency and voltage. These gain values are shown in Table 6.1.

Table 6.1: Droop Control Values

| | Gain |
|---|---|
| Kp | 534.5 |
| Kq | 5.488 |

A proportional-integral (PI) controller was selected to regulate the power output of the storage system because of its inherent stability and ease of tuning. The possibility of incorporating a more sophisticated higher order controller is discussed in further detail in chapter 7. The PI controller was tuned using a modified Ziegler-Nichols method [17]. By using the Ziegler-Nichols method the proportional gain was increased until the system output began to oscillate. This gain value, called the unity feedback gain amplitude, was used to find the initial values for the proportional and integral gains which were then further tuned by hand. The proportional and integral gains are shown in Table 6.2.

Table 6.2: PI Controller Gains

| | Real Power Controller | Reactive Power Controller |
|---|---|---|
| K | .538 | .538 |
| Ts | .0055 | .005 |

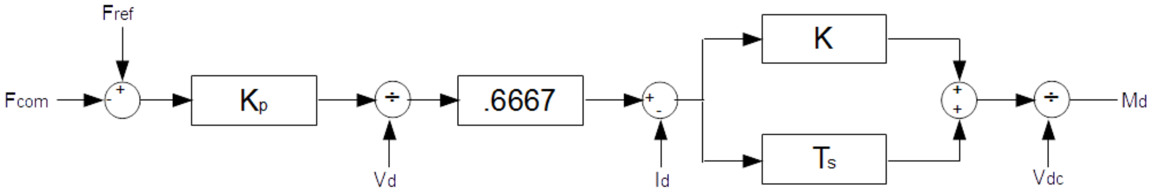


Figure 6.3: Frequency Controller

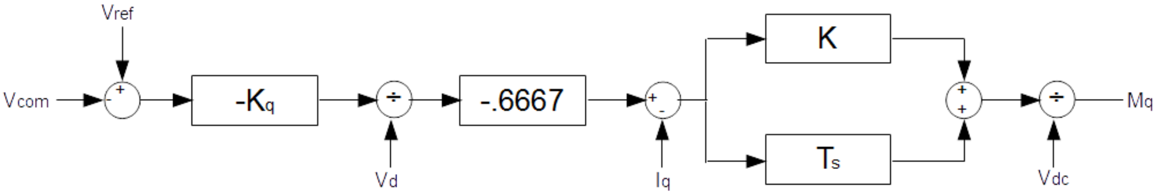


Figure 6.4: Voltage Controller

Figures 6.3 and 6.4 show the frequency and AC voltage magnitude controllers for the storage system. Once the system was implemented into the offline simulation, it was tested for typical conditions such as changes in power demand on the system and disconnecting from the main grid. The voltage, frequency, and power response of the storage system for a decrease in the power demand of the system are shown in the following figures both without and with the storage system.

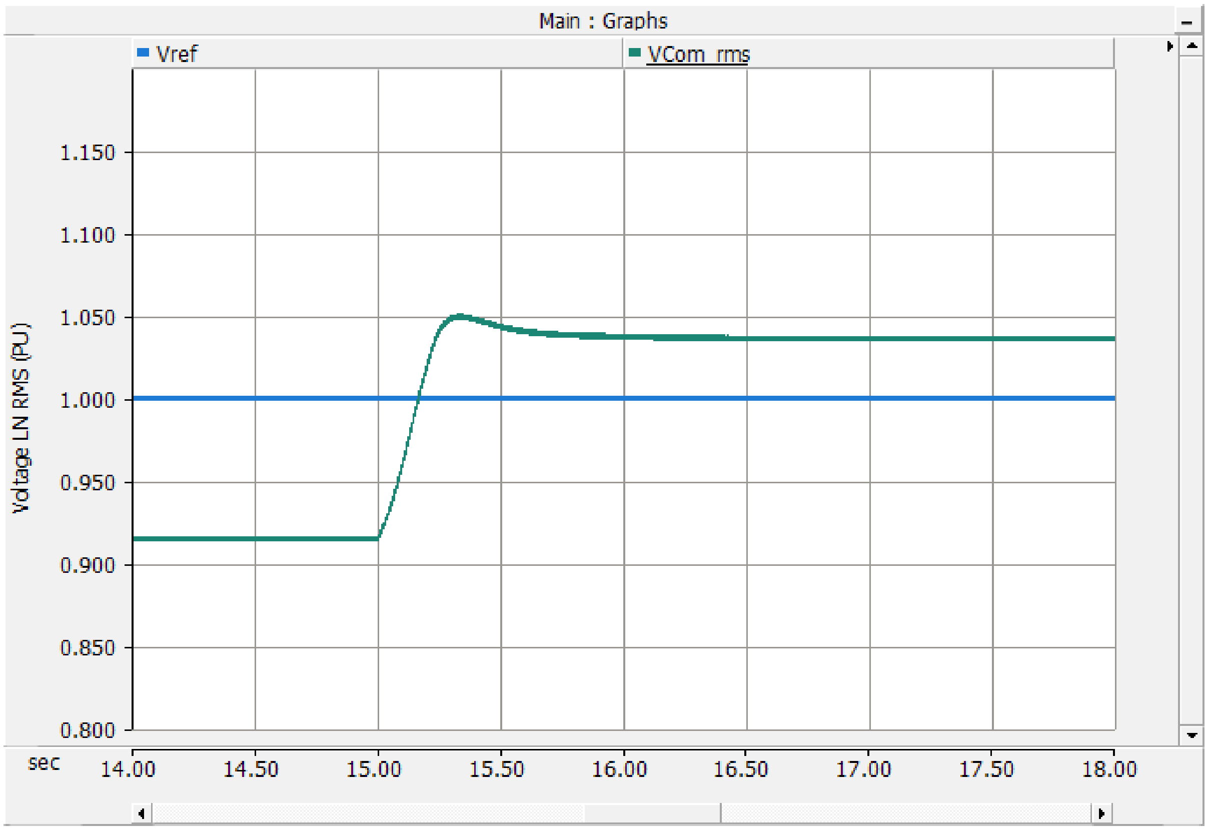


Figure 6.5: Voltage Response of the Offline Simulation for a Decrease in the Power Demand of the System without the Storage System Implemented

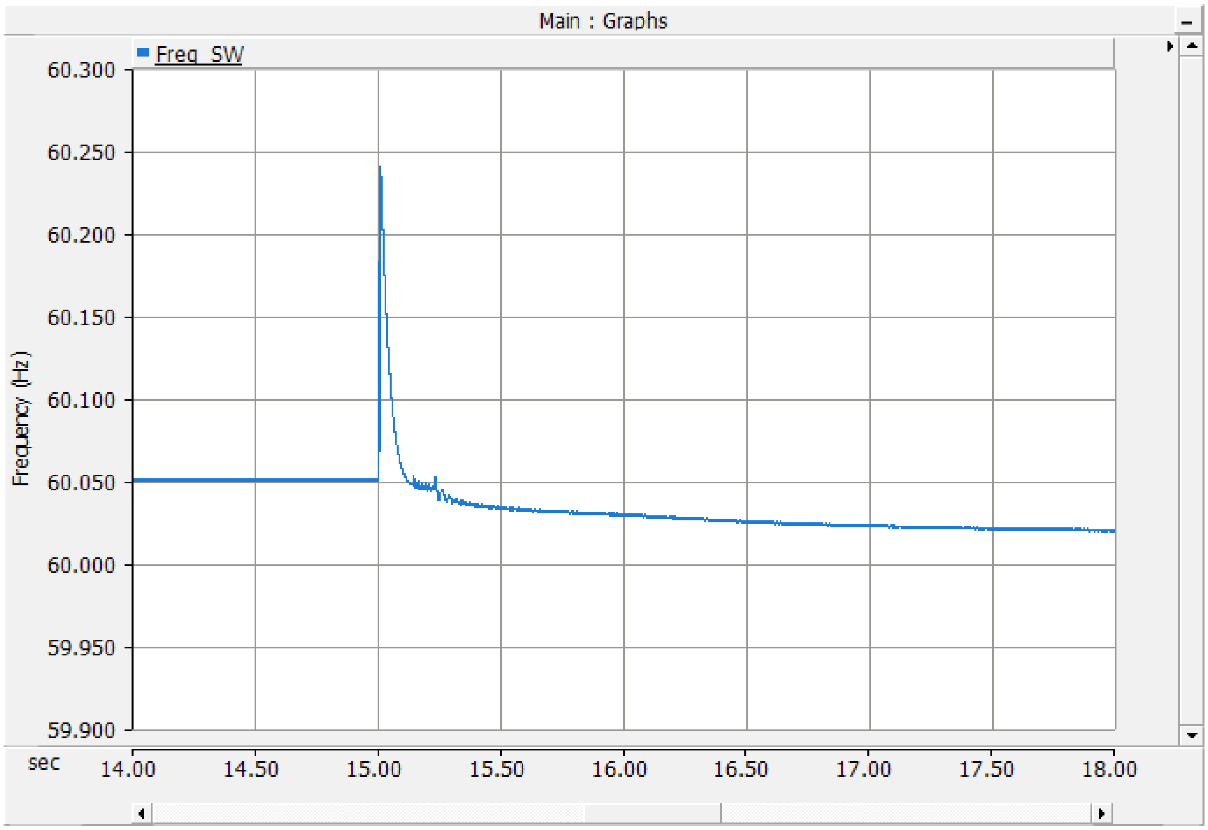


Figure 6.6: Frequency Response of the Offline Time Simulation for a Decrease in the Power Demand of the System without the Storage System Implemented

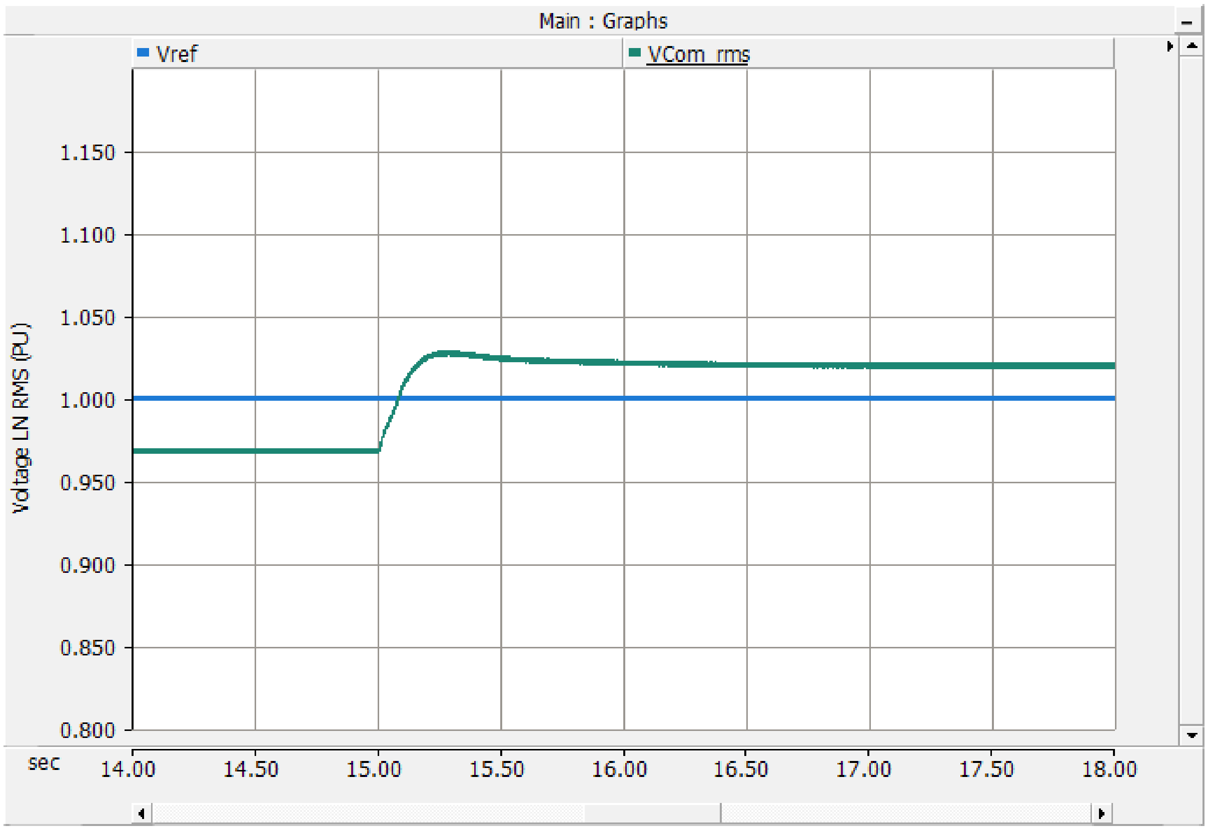


Figure 6.7: Voltage Response of the Offline Simulation for a Decrease in the Power Demand of the System with the Storage System Implemented

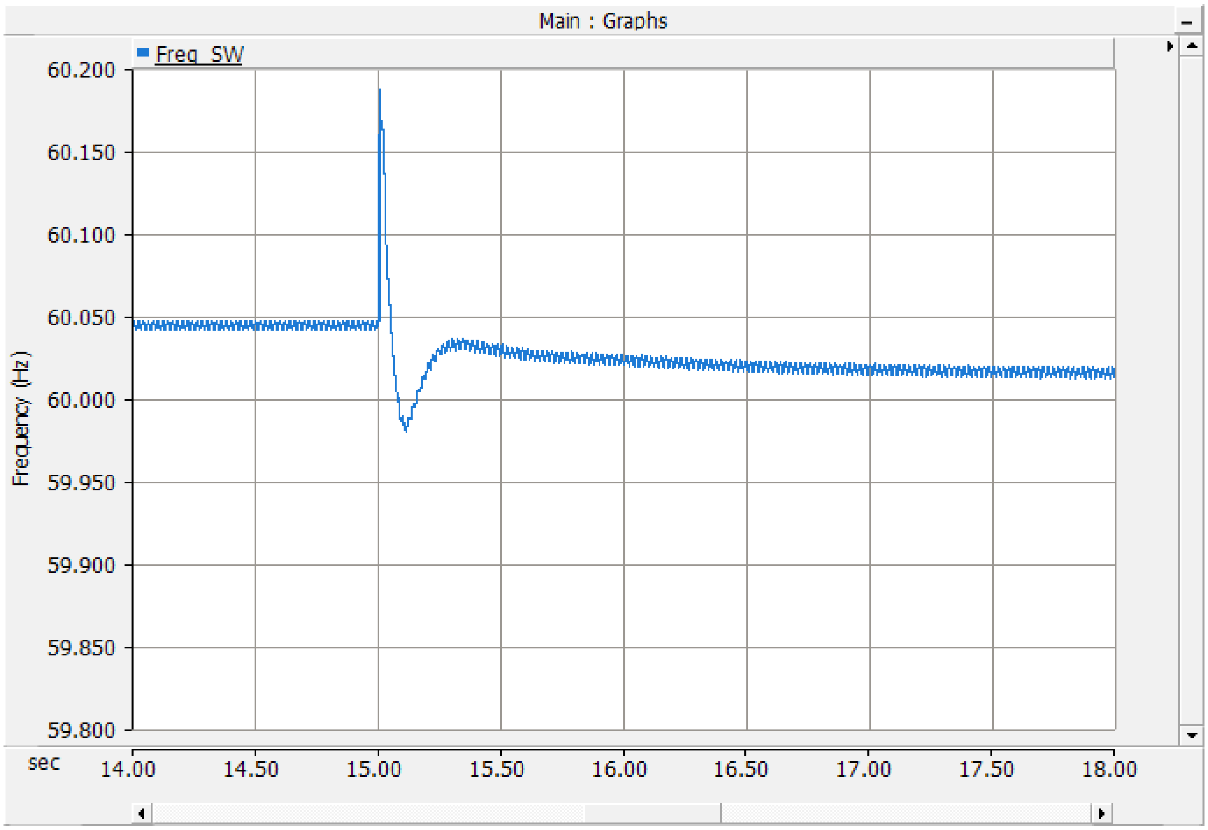


Figure 6.8: Frequency Response of the Offline Time Simulation for a Decrease in the Power Demand of the System with the Storage System Implemented

The above test was completed by suddenly removing several loads from the system while it was running in steady-state. The sudden loss in loading will cause the systems frequency and voltage to increase until the power being produced by the generators can be reduced. As can be seen in Figure 6.5 and 6.7 the voltage at the transmission bus increased when the loads were disconnected but was prevented from leaving the operating region, of +/-5% nominal value, by the storage system. Figure 6.6 and 6.8 shows that while the frequency never left its operating region it was better regulated with the storage system implemented. The results for the next test, a sudden loss of the grid connection, can be seen in the following figures.

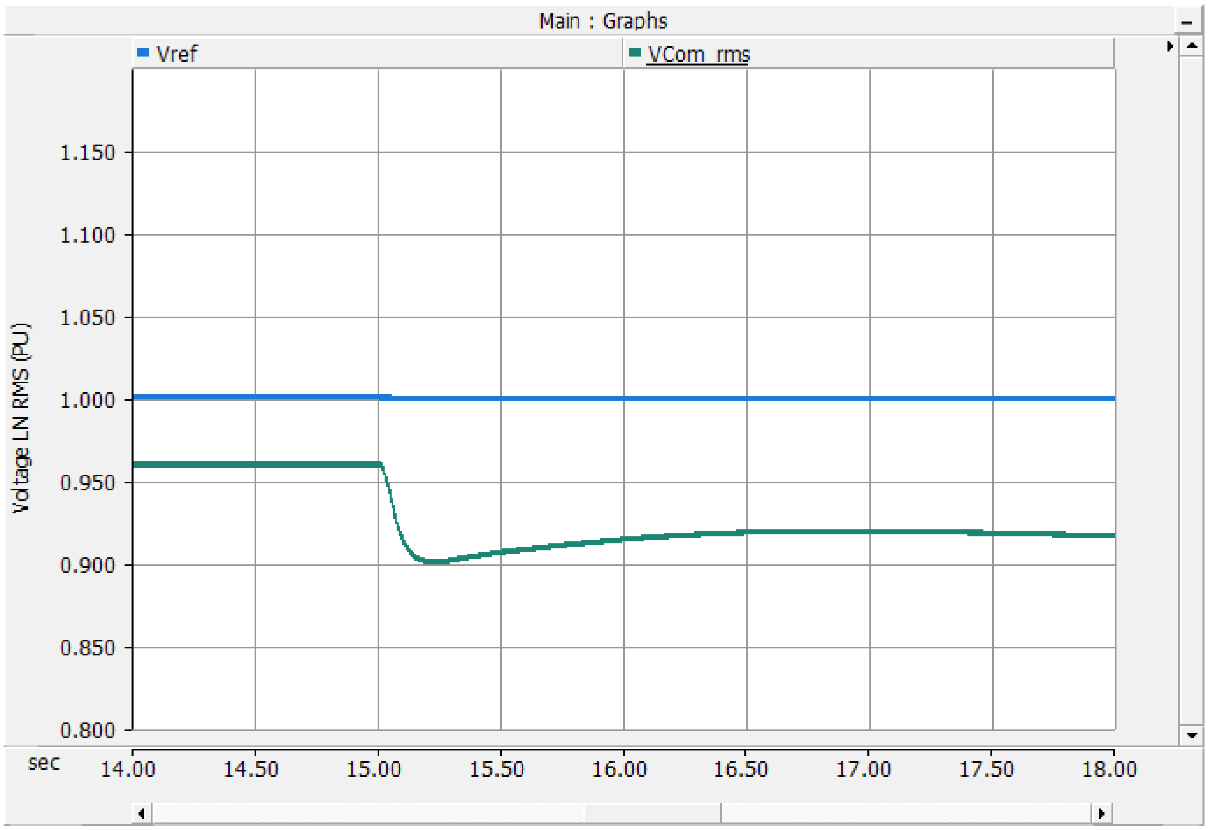


Figure 6.9: Voltage Response of the Offline Simulation to the Microgrid Entering Islanded Mode without the Storage System Implemented

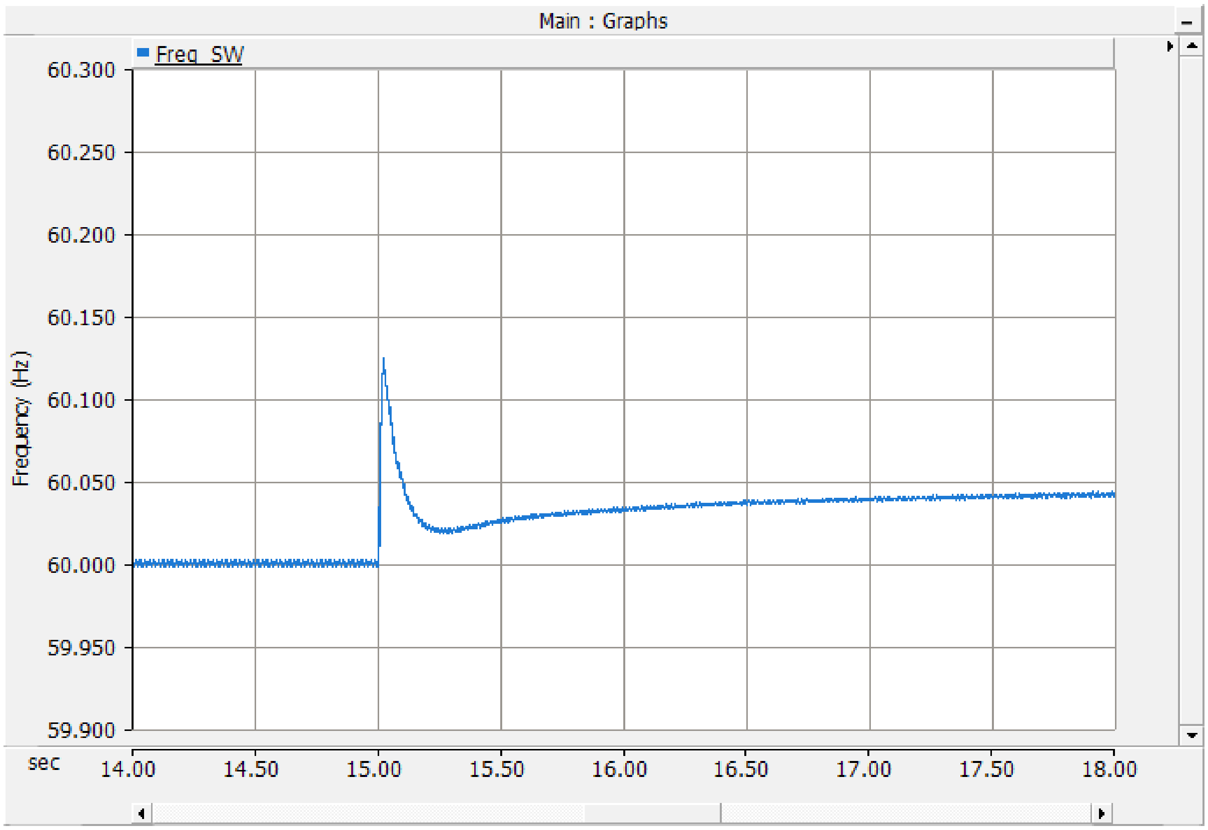


Figure 6.10: Frequency Response of the Offline Time Simulation to the Microgrid Entering Islanded Mode without the Storage System Implemented

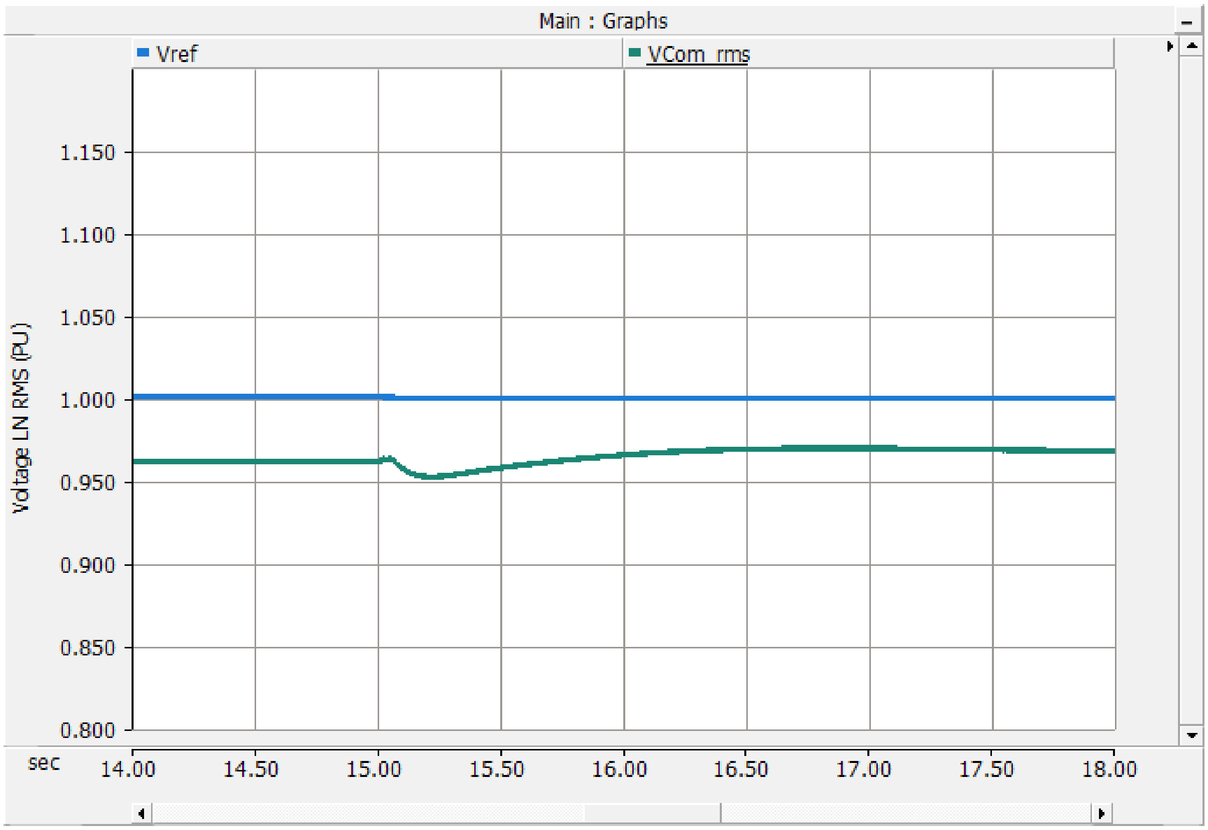


Figure 6.11: Voltage Response of the Offline Simulation to the Microgrid Entering Islanded Mode with the Storage System Implemented

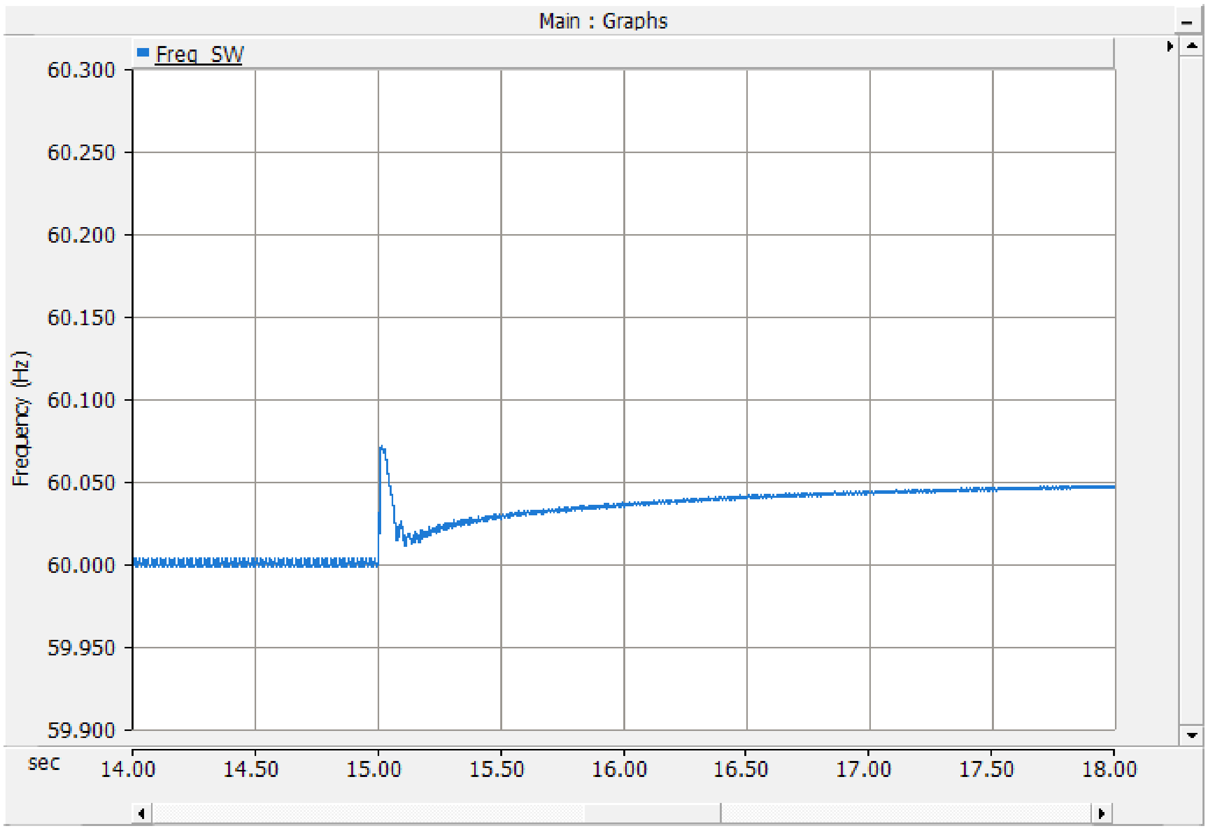


Figure 6.12: Frequency Response of the Offline Time Simulation to the Microgrid Entering Islanded Mode with the Storage System Implemented

When the system enters islanded mode, there will typically be a power imbalance, for both real and reactive power, from the loss of power supplied by the main grid. As seen in Figures 6.9 and 6.11, the storage system is once again able to properly regulate the voltage and prevent it from leaving the operating region. The frequency responded similarly to the previous test, as shown if Figures 6.10 and 6.12 with a sudden increase that the storage system was able effectively limit. Since the storage system responded adequately to these tests, the next step was to implement it into the real time simulation model.

### 6.6 Real Time Simulation Implementation and Testing

The energy storage system was implemented as a full switching model with an inverter switching frequency of 2400 Hz in the real time simulation. The RTDS calculates the state of each element of the simulation at a fixed time step of about 50 μs, which is capable of accurately simulating the behavior of most elements of the system. However, this time step is too slow to properly model the behavior of a power electronic converter switching at 2400 Hz. To correctly model these devices, the RTDS partition the converter in a small time simulation space with interface to the 50 μs simulation. This allows the converter to be simulated at a much faster time step of around 5 μs and interpolated to the rest of the system. Once the storage system was properly implemented into the real time simulation, the same tests from the previous section were performed again — once without the energy storage system and once with it implemented — to test it performance. The results from the first test, the sudden loss in loads, is shown in the following figures.

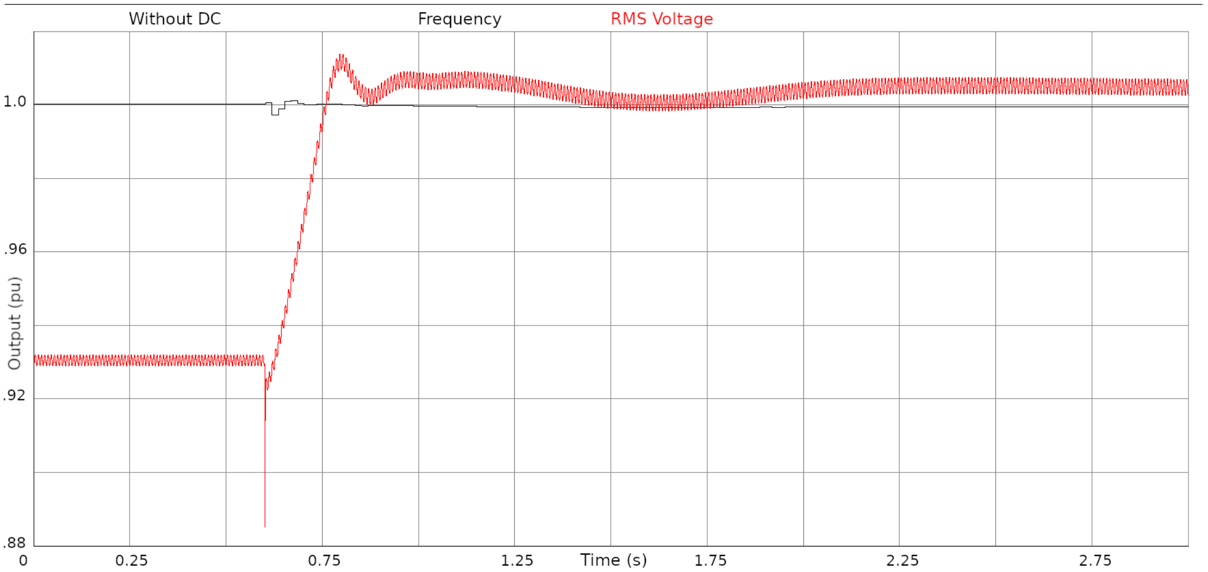


Figure 6.13: Normalized Voltage and Frequency Response of the System in the RTDS for a Decrease in the Power Demand of the System without the Energy Storage System

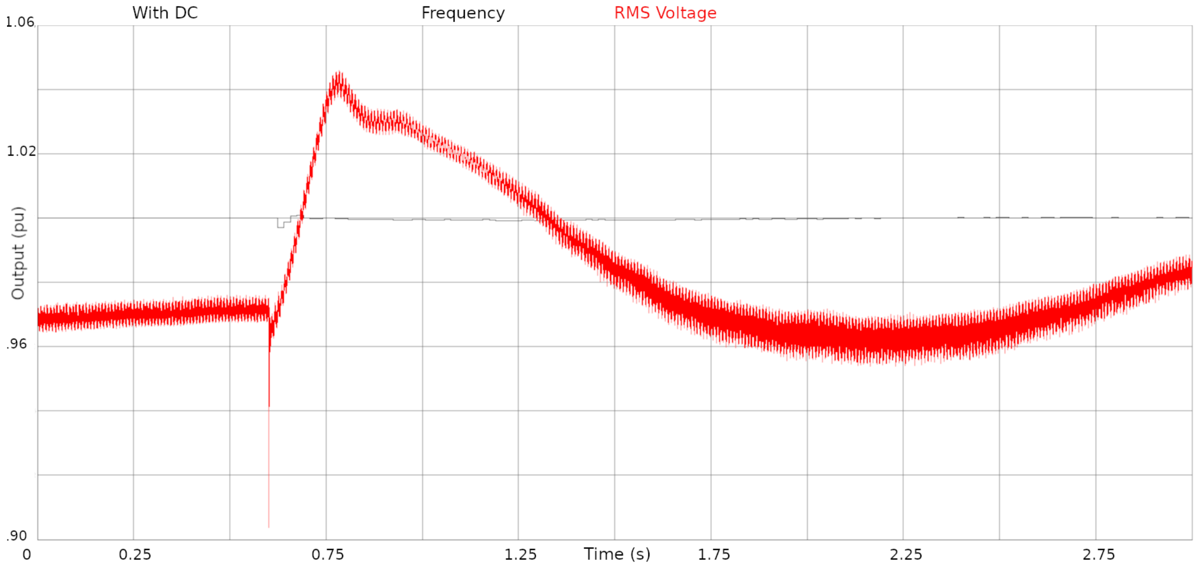


Figure 6.14: Normalized Voltage and Frequency Response of the System in the RTDS for a Decrease in the Power Demand of the System with the Energy Storage System

Figure 6.13 shows that the voltage response from a decrease in power without the storage system was a sharp drop of approximately 10% and settled out to around 8% of the nominal voltage. The frequency fluctuated rapidly, but never left the operating region. Figure 6.14 shows the voltage with the storage system dropped but recovered back to its nominal level. There was a minor overshoot in the voltage, but it was not a large concern. The energy storage system did introduce a large amount of high frequency distortions during the transition. These distortions appeared to be harmonic of the switching frequency, but their exact frequency was difficult to determine due a lack of resolution in the RTDS run-time's default graph. As such, the removal of these disturbances was considered beyond the scope of this thesis and potential solutions are discussed in Chapter 7. The frequency did not oscillate as much with the storage system implemented. The storage system’s behavior does not exactly match that found in the offline simulation, but its performance still satisfies the design goals of this research project.

For the next test the system was once again disconnected from the grid to show how it responded to the sudden power imbalance. The generator real and reactive power outputs were set to slightly under the predicted system requirements for this test. Additionally, to reduce possible variables and to highlight the effects of the energy storage system the generators' output were set to not change with constant power and excitation voltage for the duration of the test. The system response with both the energy storage system implemented and disconnected are shown in Figures 6.15 and 6.16.

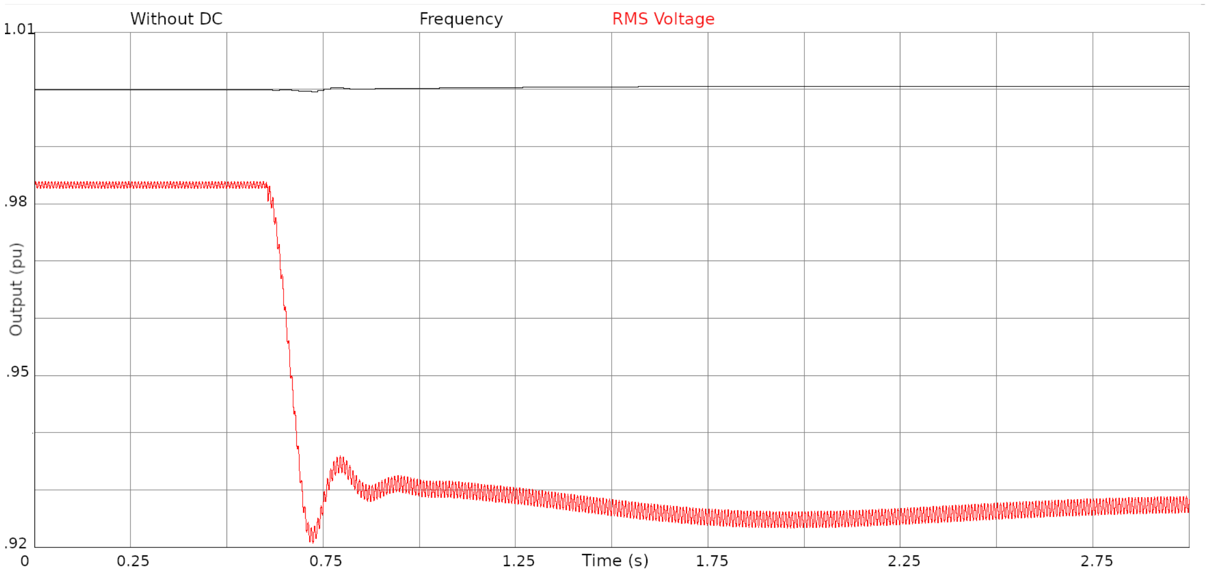


Figure 6.15: Normalized Voltage and Frequency Response of the System in the RTDS for a Loss of the Grid Connection without the Energy Storage System

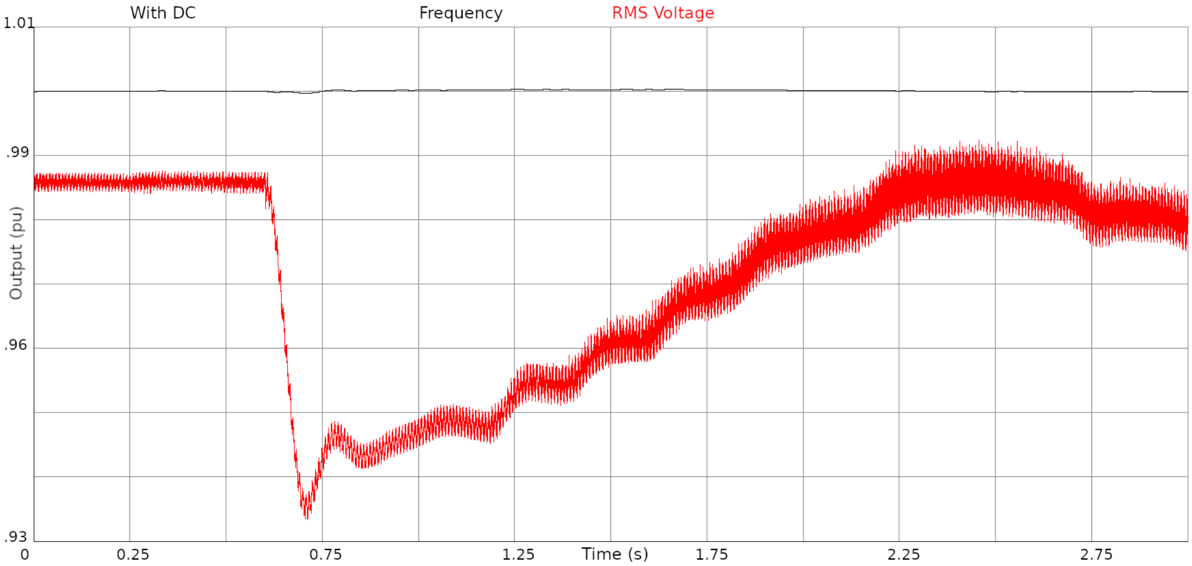


Figure 6.16: Normalized Voltage and Frequency Response of the System in the RTDS for a Loss of the Grid Connection with the Energy Storage System

Without the energy storage system, the voltage fell well below the nominal value and settled at a little under 93% of the nominal voltage. The frequency increased a negligible amount in both cases. When the energy storage system was implemented, the voltage dropped slightly out of the operating region for approximately half a second before it recovered, and settled to within the operating regions. The cause of this slow response was due to the limits on the power output of the storage system. The storage system could not transfer the required power across the AC-DC converter due to its current limit. Despite this the storage system still behaved in the expected manner and the results are consistent with those from the offline simulation. Once again there was no noticeable change to the frequency during the test. Based on these results the energy storage system was able to improve upon the system response .

## 6.7 Chapter 6 Summary

This chapter went over the design and implementation of the energy storage system to the real time simulation. It explained the concepts behind the design of the energy storage system model, the control scheme used to regulate its power output, and how droop control is used to regulate the power output based on the voltage and frequency of the system. Then, the system's implementation in the offline simulation was explored along with the results from different tests used gauge the system’s performance. Finally, the chapter showed the implementation of the storage system in the real time simulation and compared the performance of the simulation with and without it connected to the microgrid.

## Chapter 7: Summary and Future Work

### 7.1 Summary

The goal of this thesis was to improve and expand upon the University of Idaho Industrial Control System testbed to more accurately imitate a real world microgrid capable power system using both a real-time simulation and physical substation hardware. The physical hardware was used to create a realistic SCADA system to monitor and control the system. The thesis explained the role and configuration of the devices used in creating the SCADA system, along with setup of the HMI and data historian. This expanded network of devices allowed the system to somewhat realistically mimic how real world utility power systems monitor and control the flow of power through the system.

The thesis also explained the improvements made to the existing real-time simulation model allowing it to better represent the behavior of a real world microgrid system. These improvements included refining the controllers used to regulate the generators' real and reactive power outputs. Originally, the generators operated based on static set-points for power output. These improvements allowed the generators to be able to respond accurately to changes issued by system operators while remaining stable. However, the generator controllers had noticeable shortcoming when the system was islanded from the main grid that could not be easily solved with the generators alone. To make up for these shortcomings, an energy storage system was implemented into the simulation.

The energy storage system was initially designed and tested in an offline simulation tool modeling the microgrid system, using a simplified model of the energy storage system without a switching model of the power electronics. Once the design was verified using the offline simulation, it was implemented in the real-time simulation using an approximate switching model for the power electronics. The energy storage system successfully accounted for the shortcomings of the generator controller while the system was islanded. Through these improvements, simulation was able to produce somewhat more accurate and realistic data for modeling how a real world microgrid system responds to different scenarios.

## 7.2 Future Work

### 7.2.1 SCADA System Expansion

Currently, only two of the substation racks available in the testbed have been configured for the system using analog measurements from relays. While the configuration files for the RTACs have been setup and tested, they have not been implemented on each of the racks, due to the system currently being used for a different project. The GOOSE messaging has also only been configured and tested for one of the RTACs. Future researchers will need to create and implement the files to properly simulate a complex SCADA network. Also, the relays are only functioning as metering devices at this time, but they can be re-configured to also act as protection devices to allow future projects to implement more complex and robust protection schemes in addition to the SCADA scheme.

Each substation rack contains an SEL Axion that is not implemented into the system at present. These are modular devices containing a RTAC, relay, and digital input and output points. These devices can be incorporated into the SCADA system. At this time, the control signals and set-points are sent directly from the SCADA master to the RTDS over DNP3 communication. Ideally, these signals should be sent to the RTACs or Axions and then sent to the RTDS to create a more accurate representation of the operation of a real SCADA system. This will allow the second Ethernet port on the RTDS to be used for other purposes, such as sending sampled values (SV) messages to the relays [18]. With SV messaging, simulated voltage and current measurements can be sent over high speed Ethernet within the substation, and allowing more flexible protection schemes to be implemented on the relays without the limitations from analog measurements. Through this, future projects will be able to work around the limited number of analog outputs available on the RTDS and represent these digital substation coming into application in the industry.

### 7.2.2 Simulation Improvements

The generator controls currently function well, but suffer while the system is islanded and the set-points do not match the power requirements of the loads. A more realistic generator control scheme that matches the control applied on dispatchable generation in practice is needed during islanded mode. One possible scheme for the islanded system is to use frequency droop control on the generators along with the operator set-points to allow automatic adjustments to their power output. This would allow the generators to actively correct power mismatches and reduce the amount of power the energy storage system needs to supply or absorb while islanded. An under frequency load shedding scheme or an over frequency generator shedding scheme could also be used to improve the islanding operation of the model.

Future projects can also expand upon the energy storage system by implementing a more accurate battery model into the system. This will require creation of design specifications and goals along with a charging and discharging control algorithm. The charging control algorithm will control the rate that the battery stores and releases energy into the system to increase the lifespan of the battery and prevent damage to the power electronics. Thus, the energy storage system will behave more realistically with a limited rate of power flow and cut-off points for energy both spent and stored [7]. Another area where the DC storage system can be improved is by utilizing a filter or compensator on the output to remove the switching harmonics. As demonstrated Chapter Six, the switching model of the AC-DC bridge introduces distortions into the system at the harmonics of the switching signal frequency.

The energy storage system's controls can be improved by replacing the PI controllers with more complex, higher order controllers. These controllers will allow the storage system to respond more rapidly and more accurately. A stable control system must have a positive phase when the gain crosses zero. Whenever a time delay occurs, whether it's between the measurement device and the controller input or between the controller and machine's inputs, the starting phase for the system decreases. Therefore, the phase margin is the amount of time delay that can occur before the system becomes unstable. Any scheme to implement a higher performance controller will need to carefully consider the phase margin of the controller.

## Appendix: Acronyms and Technical Terms

| | |
|---|---|
| DNP3 | Distributed Network Protocol 3 |
| GOOSE | IEC 61850 Generic Object Oriented Substation Event |
| ICS | Industrial Control System |
| IGBT | Insulated-Gate Bipolar Transistor |
| INL | Idaho National Laboratory |
| PDC | Phasor Data Concentrator |
| PI | Proportional Integral Controller |
| PMU | Phasor Measurement Unit |
| RTAC | SEL 3530 Real-Time Automation Controller |
| RTDS | Real-Time Digital Simulator |
| SCADA | Supervisory Control and Data Acquisition |
| SV | Sampled Values |
| VM | Virtual Machines |

## References

[1] Liang, G., Weller, S., Zhao, J., Luo, F. and Dong, Z. *The 2015 Ukraine Blackout: Implications for False Data Injection Attacks*. “IEEE Transactions on Power Systems”, 32(4), pp.3317-3318.

[2] Edsel Atienza. “Testing and Troubleshooting IEC 61850 GOOSE-Based Control and Protection Schemes” *12th Annual Western Power Delivery Automation Conference* Spokane, Washington April 13–15, 2010

[3] Ahmed, Irfan & Obermeier, Sebastian & Naedele, Martin & Richard III, Golden G. *SCADA Systems: Challenges for Forensic Investigators*. Computer. 45. 44-51. 10.1109/MC.2012.325.

[4] N. Hatziargyriou, *Microgrids: Architectures and Control*. John Wiley & Sons, 2014.

[5] Thomas, M. and McDonald, J. *Power System SCADA and Smart Grids*. CRC Press.

[6] I. A. Oyewumi *et al*., "ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed," *2019 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, USA, 2019.

[7] Hirofumi Akagi, Edson H. Watanabe, Macuricio Aredes; *Instantaneous Power Theory and Applications to Power Conditioning*. John Wiley & Sons, 2007

[8] K. D. Brabandere, B. Bolsens, J. V. D. Keybus, A. Woyte, J. Driesen, and R. Belmans, “A Voltage and Frequency Droop Control Method for Parallel Inverters,” *IEEE Transactions on Power Electronics*, vol. 22, no. 4, pp. 1107–1115, 2007.

[9] K. Amarasinghe, C. Wickramasinghe, D. Marino, C. Rieger and M. Manic, "Framework for Data Driven Health Monitoring of Cyber-Physical Systems," *2018 Resilience Week (RWS)*, Denver, CO, 2018, pp. 25-30.
doi: 10.1109/RWEEK.2018.8473535

[10] D.J. Dolezilek, “SEL Communications and Integration White Paper,” Schweitzer Engineering Laboratories 2000, Pullman, Washington.

[11] “IEEE Guide for the Application of Turbine Governing Systems for Hydroelectric Generating Units - Redline," in *IEEE Std 1207-2011 (Revision to IEEE Std 1207-2004) - Redline* , vol., no., pp.1-139, 20 June 2011

[12] Rodolfo J. Koessler, “Techniques for Tuning Excitation System Parameters,” *IEEE Transactions on Energy Conversion*, Vol 3, No 4, December 1988

[13] A. Sheikh, T. Youssef, and O. Mohammed, “AC Microgrid Control Using Adaptive Synchronous Reference Frame PLL,” *2017 Ninth Annual IEEE Green Technologies Conference (GreenTech)*, 2017.

[14] Abdelkrim Benchaib; *Advance Control of AC/DC Power Networks*. John Wiley & Sons, 2015

[15] J. F. Hu, J. G. Zhu, and G. Platt, “A droop control strategy of parallel-inverter-based microgrid,” 2011 International Conference on Applied Superconductivity and Electromagnetic Devices, 2011.

[16] Tatjana Kalitjuka, *Control of Voltage Source Converters for Power System Applications* (Master's thesis, Norwegian University of Science and Technologies), 2011.

[17] O'Brien, J. *Frequency-domain control design for high-performance systems*. Stevenage: Institution of Engineering and Technology, 2012.

[18] V. Skendzic and D. Dolezilek, “New and Emerging Solutions for Sampled Value Process Bus IEC 61850-9-2 Standard – An Editor’s Perspective” *International Conference and Exhibition – Relay Protection and Automation for Electric Power Systems*, April 2017

[19] Y. Chen, J. Zhao, K. Qu, and F. Li, “A PQ control strategy for voltage-controlled inverters applied in low-voltage power system,” *2014 International Power Electronics and Application Conference and Exposition*, 2014.

[20] Suleiman M. Sharkh, Mohammad A. Abusara, Georgios I. Orfanoudakis, Babar *Hussain: Power Electronic Converters for Microgrids.* John Wiley & Sons, 2014

[21] MD Tanjimuddin *Reactive Power Control in Grid-Connected Converters* (Master's thesis, Tampere University of Technology), 2018.

[22] Amirnaser Yazdani, Reza Iravani; *Voltage-Sourced Converters in Power System. IEEE Press*, John Wiley & Sons, 2010