

A HARDWARE-IN-THE-LOOP EXPERIMENTAL TESTBED FOR THE
EVALUATION OF POWER GRID STABILITY AND SECURITY

A Thesis
Submitted to
the Temple University Graduate Board

In Partial Fulfillment
of the Requirements for the Degree
MASTER OF SCIENCE
in ELECTRICAL ENGINEERING

By
James D. Kollmer
August 2020

Thesis Committee:

Saroj Biswas, Thesis Advisor, Electrical Engineering, Temple University

Liang Du, Committee Member, Electrical Engineering, Temple University

Li Bai, Committee Member, Electrical Engineering, Temple University

DECLARATION OF AUTHORSHIP

I, JAMES KOLLMER, declare that this thesis titled, ‘A HARDWARE-IN-THE-LOOP EXPERIMENTAL TESTBED FOR THE EVALUATION OF POWER GRID STABILITY AND SECURITY’ and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

ABSTRACT

This research presents the development of a hardware-in-the-loop testbed for a three-bus power grid interfaced with a simulated networked control system (NCS) for investigation of cyberattacks and their possible impacts on the power grid. The three-bus grid consists of two generator buses, configured as slack bus (constant voltage and angle) and PV bus (constant power and constant voltage), and a load bus (PQ bus). The synchronous generators are driven by dynamometers serving as prime movers, and the field circuits controlled by insulated gate bipolar junction transistors (IGBT). The load bus is comprised of resistors, capacitors, and inductors that are connected to the generator buses through transmission lines. The simulated NCS is implemented on an Opal-RT platform, which is a PC/FPGA based real-time simulator that can integrate hardware with software based simulations, commonly referred to as hardware-in-the-loop (HIL). In general, HIL setups have the advantage that physical elements under test interact in real time with a simulated model of a large scale system and provide a better insight of performance of both the physical system and the controller. In this HIL experimental setup, the data acquisition unit (DAQ), and the controller are both implemented on the Opal-RT platform. A baseline for the behavior of the three-bus system is first established by operating the generator under various load conditions for which the controller maintains the desired terminal voltage. Then various types of cyberattacks were initiated on the system that include bias attack, data attack, and Denial-of-Service (DoS) attacks. The closed loop generator control system maintained the stability of the system as well as the required bus voltages within a certain tolerance. With no attack prevention mechanism in place, the developed experimental platform provides a facility to observe and evaluate the impacts of various cyberattacks on a real physical microgrid.

ACKNOWLEDGEMENTS

I would like to thank my stepfather, Russell Valley, for all his love and support throughout my childhood and for being the ever vigilant force behind my collegiate career. I would not have made it to where I am today without you. I could not have asked for a better father. The completion of this thesis is dedicated to you. You are missed each and every day. I will continue to cherish the time we had together for years to come.

A special thanks goes to Dr. Saroj Biswas. I could not have asked for a better advisor. He was kind, caring, patient, supportive, informative, and always there for me whenever I needed him. Thank you for never giving up on me!

A special thanks goes to my friend and colleague, Robert Irwin, who contributed to the experimental platform discussed in this thesis. Thanks for all your help, it was a pleasure doing research with you!

I would also like to thank my mother and brother for their continued love and support.

Thank you Matthew Hardy, Bogdan Niemoczynski, and Derek Kropp for being such wonderfully supportive friends.

Special thanks to my advisor, Dr. Saroj Biswas, my committee members, Dr. Liang Du and Dr. Li Bai.

This research was supported in part by grants from the National Science Foundation CNS-1446574 and by the Office of Naval Research grant N00014-15-1-2922.

Contents

DECLARATION OF AUTHORSHIP	i
ABSTRACT	ii
ACKNOWLEDGEMENTS	iii
LIST OF FIGURES	vi
LIST OF TABLES	viii
ABBREVIATIONS	ix
1 INTRODUCTION	1
1.1 Background	1
1.2 Motivation	2
1.3 Goals and Objectives	3
1.4 Outline of the Thesis	4
2 POWER SYSTEM STABILITY	6
2.1 Single Machine Infinite Bus	6
2.2 Prime Mover	9
2.3 Excitation System	13
2.4 Swing Equation	14
3 HIL CYBER PHYSICAL SYSTEM	17
3.1 HIL Overview	17
3.2 Opal-RT Simulator	18
3.3 The Physical System - Three Bus Grid	20
3.3.1 Generator Excitation System	21
3.4 Generator Parameters	22
3.4.1 Synchronous Generator Constants	22
3.4.2 Determination of Armature Resistance R_a and Field Resistance R_f	23

3.4.3	Evaluation of the Field Inductance L_f	24
3.4.4	Determination of the Stator Inductance L_s	25
3.4.5	Evaluation of the Magnetization Constant K_f	26
4	MULTIBUS SYSTEM	28
4.0.1	Load Model	29
4.0.2	Grid Model	30
4.0.3	Combined Generator and Grid Model	31
4.0.4	Swing Equation	32
4.0.5	Excitation System	33
4.0.6	Prime Mover	34
4.0.7	Complete System Model and Control Design	35
4.1	Simulation Results	35
5	EXPERIMENTAL RESULTS	42
5.1	Baseline Performance	43
5.2	Cyberattack on a 2-Bus System	46
5.2.1	Constant Bias Attack	46
5.2.2	Ramp Bias Attack	48
5.2.3	Random Data Injection	49
5.2.4	DoS Attack	50
5.3	DoS Attack on 3-Bus System	51
6	CONCLUSION	55
6.1	Summary	55
6.2	Future Research	57
	BIBLIOGRAPHY	59

List of Figures

2.1	Single Machine Infinite Bus	7
2.2	Single Machine Infinite Bus Equivalent Circuit	8
2.3	Torque Equation Lever Example	10
2.4	Steam Powered Turbine-Generator system	11
2.5	Rotor Field Circuit	13
3.1	Schematic of Closed Loop NCS	18
3.2	OP5600 and OP8660 from left to right	19
3.3	Opal-RT High Level Control Loop	20
3.4	Three-Bus Electrical Network	21
3.5	Experimental Setup	21
3.6	Generator Excitation System	22
3.7	Complete Excitation Control System	23
3.8	Experimental Evaluation of L_f	25
3.9	Plot to find L_s	26
3.10	Plot to find K_f	27
4.1	Excitation System	34
4.2	Excitation System	35
4.3	3-Bus System	36
4.4	Frequency Swing	37
4.5	Bus Voltages	37
4.6	Bus Voltage Angles with respect to Bus 1	38
4.7	Rotor Angles with respect to Bus 1	39
4.8	Power Supplied by the Generators	39
4.9	Reactive Power Supplied by the Generators	40
4.10	Excitation Voltage of the Generators	41
5.1	Bus Voltages for Load Switching	43
5.2	Bus Currents for Load Switching	44
5.3	Duty Cycle Ratio of Slack Bus Generator for Load Switching	45
5.4	Generator Speed (PV Bus)	46
5.5	Constant Bias Attack	47
5.6	Ramp Bias Attack	48
5.7	Random Bias Attack	49
5.8	Dos Attack	50

5.9	Bus Voltages (DoS Attack on PV Bus Generator)	52
5.10	Bus Current (PV Bus)(DoS Attack)	53
5.11	Duty Cycle Ratio (DoS Attack)	53
5.12	Generator Speed (PV Bus)(DoS Attack)	54

List of Tables

3.1 A List of Synchronous Generator Constants	23
---	----

ABBREVIATIONS

DoS	Denial of Service
NCS	Networked Control System
DAQ	Data Acquisition
IGBT	Insulated Gate Bipolar Transistor
ADC	Analog to Digital Converter
MCU	MicroController Unit
EMF	ElectroMotive Force
RPM	Revolutions Per Minute
w.r.t.	with respect to

Chapter 1

INTRODUCTION

1.1 Background

The U.S. power grid forms the core of all infrastructures, defense, and commerce in the United States which makes it a prime target [1], [2], [3], [4] for cyber terrorism. In recent years, there have been many incidents of cyberattacks on the power grid all over the world including the Ukrainian grid cyberattack [5] in December 2015 that disrupted power supply to over 230 thousand customers for up to 6 hours. Whether or not it is possible to prevent cyberattacks on the grid is debatable, it is necessary to develop control system tools that could keep the smart grid stable and operational in the events of such attacks. Over the last decade, there have been significant efforts on the development of security hardware and software for industrial control systems, nevertheless a general consensus is that the power sector is not yet prepared to combat cyberattacks [2], [6], [7], [8], [9], [10] and [11].

Control theoretic analysis of power security has drawn significant attention in recent years which could be classified in two broad categories: a) attacks impacting long term operation affecting power system state estimation, such as [12–14], and b) attacks impacting short term transients and stability [15], [16], [17]. Adversarial

dynamics is another important factor that must be included in understanding and mitigating the effects of cyberattacks on the grid. Recent results in this direction can be found in [18].

This research investigates the development of an unguarded hardware-in-the-loop experimental testbed that could be used to investigate the effects of cyberattacks on the grid, and develop and test security countermeasures to minimize any detrimental effects that may destabilize the overall grid.

1.2 Motivation

Replicating a realistic power grid in the laboratory using physical hardware is difficult and expensive. This primarily relegates the power systems security research to the domain of purely simulation only experiments. One example of such simulation platforms is the GridGame [19], an interactive simulation platform developed at Idaho National Laboratory (INL) that is played between two players in which the grid operator attempts to maintain a constant grid frequency by taking defensive actions in the events of various types of attacks launched by cyberattackers. Similarly, the Aurora Generator Test (a hardware based testbed) at the INL in 2007 is probably the earliest experimental demonstration that showed the effects of a possible cyberattacks on the power grid.

In recent years, hardware-in-the-loop (HIL) experiments have drawn considerable interest as a way of testing physical hardware in a real world environment. In HIL experiments, physical elements under test interact in real time with a simulated model of a large scale system and/or a controller and data acquisition system through appropriate analog and digital interfaces, and provides a better insight of the performance for both the physical system as well as the controller. Examples of HIL experiments include interaction of a voltage source converter

with an electric ship power grid [20], control of inverters and buck converters [21], evaluation of an industrial level generator excitation control system with the turbine-generator system [22], photovoltaic generation and power interface [23], active power control of wind power plant [24], MVDC integrated power system for electric ships [25], and many more. Various requirements and characteristics for the implementation of HIL experiments including bandwidth, accuracy, and stability have been outlined in several recent references (e.g., see [26], [27], [28], and [29]).

This research pertains to the development of a hardware-in-the-loop experimental setup and investigation of stability of multibus power systems. Some of the results of this HIL development were presented by the author at recent ASEE conferences [30–32].

1.3 Goals and Objectives

The main contribution of this thesis is the development of a novel experimental HIL platform for demonstrating the effects of cyberattacks on a three-bus power system. The cyber component of the HIL platform is based on an Opal-RT real-time PC/FPGA-based simulator, and the physical component of a three-bus power grid is based on the LabVolt EMS8000 series power generators and loads. The three-bus grid is configured as a slack bus (constant voltage and angle), a PV bus (constant power and voltage), and a PQ bus (constant real and reactive power) or load bus of switchable resistors, inductors and capacitors. Two synchronous generators are connected to the grid slack bus and the PV bus, respectively, with the slack bus generator configured to run at constant speed. The instrumentation layer of the system includes various sources and sensors within the OP8660 HIL controller and data acquisition interface that measures voltages and currents on all of the buses, and speed of the synchronous generators. The computational

engine of the HIL system implemented on the Opal-RT includes a control algorithm for the generator field circuit, data processing, computation of real and reactive power, and other pertinent quantities, and for launching simulated cyberattacks. The feedback loop is completed through the OP8660 HIL controller and data acquisition interface that sends the control signal from the Opal-RT to the gate of the insulated-gate bipolar transistor (IGBT) which ultimately controls the applied voltage of the generator field coil, and hence the induced electromotive force (EMF). Additional details of the HIL setup is given in Chapter 3.

Experimental results are presented that include normal operating state of the three bus grid, and that of the system under denial-of-service attacks. A baseline for the behavior of the three-bus grid is first obtained by running the system under normal operating conditions. This experiment demonstrated the effectiveness of the controller in maintaining stability of the grid and desired voltages at various buses as the system load on the PQ bus was varied.

The three bus system was then subjected to simulated cyberattacks, such as bias attack, data attack, and denial-of-Service (DoS) attacks. Notably a series of simulated denial-of-service attacks were launched on the controller of the PV bus generator by increasing the probability of packet drop in the control loop of the network, modeled by an i.i.d. Bernoulli process. The generator control system was able to maintain closed loop stability as required. With no attack prevention mechanisms in place, this platform provides a facility to observe and evaluate the impacts of various cyberattacks on a real, physical power generator.

1.4 Outline of the Thesis

The rest of this thesis is organized as follows: Chapter 2 presents the basics of power system stability, especially single machine infinite bus system which

is typically used for understanding stability of power networks and the effect of faults on the transmission line. Chapter 3 presents the development of the HIL hardware platform using LabVolt EMS8000 series equipment and Opal-RT real time simulator. Mathematical modeling of the general multibus power grid is presented in Chapter 4. Chapter 5 provides experimental results of baseline experiments followed by cyberattacks on the three-bus system. Concluding remarks and future plans in Chapter 6.

Chapter 2

POWER SYSTEM STABILITY

The purpose of this chapter is to provide the fundamentals of power system stability theory. A detailed description of the single machine infinite bus is discussed. The prime mover dynamics of the synchronous generator are also described. The development of the excitation system for the experimental platform is discussed in detail. This all culminates in the discussion of the swing equation which is the fundamental equation for determining the stability of a generator in the presence of transient disturbances.

2.1 Single Machine Infinite Bus

In an interconnected power system such as that in North America, a number of generators operate normally in synchronism with one another. They share loads based on economic dispatch and optimum power flow. But major disturbances, such as a fault in the system, loss of generation, sudden loss of load, or cyberattacks can threaten this synchronous operation. The ability of a power system to maintain synchronism, in the face of these disturbances is referred to as transient stability. As power generators are commonly equipped with excitation control and prime

mover control systems, interconnected power grids have enough damping to retain dynamic stability [33], nevertheless, power grid can lose stability in the event of large disturbances.

Transient stability can be explained by a simple system with one generator connected through a transformer and transmission line to an infinite bus, with a constant voltage of $E_2 \angle 0$, as shown in Figure 2.1 [33]. This is commonly referred to as a single machine infinite bus system.

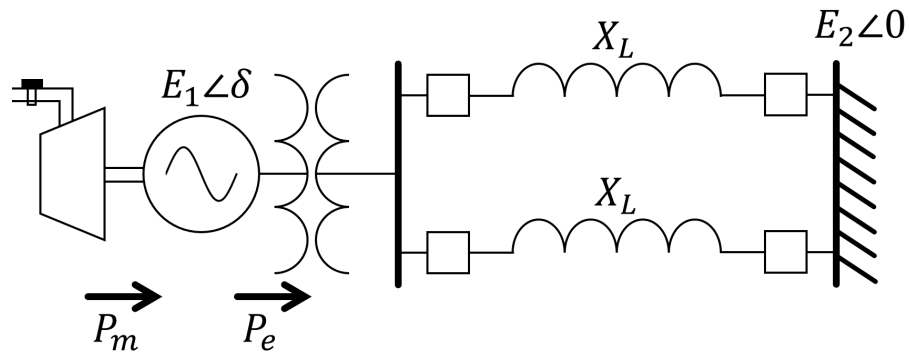


FIGURE 2.1: Single Machine Infinite Bus

Power delivered by the mechanical input P_m is usually greater than the electrical output P_e due to friction and other various losses, but for the sake of simplicity it will be assumed that the losses are zero and that P_m is equal to P_e at steady state. Under transient conditions, assuming constant flux, a synchronous generator can be represented as a voltage source of constant amplitude at the back of the generator transient reactance X'_d as shown in Figure 2.2. In Figure 2.2, X_{tr} is the leakage reactance of the transformer and $\frac{X_L}{2}$ is the reactance of the parallel transmission lines [33]. For simplicity, we neglect resistance of the transmission line and the transformer. During transients, the generator rotor starts to swing which causes the rotor angle δ to oscillate, and in the absence of adequate control systems, the rotor swing angle δ can grow with time leading to instability of the generator.

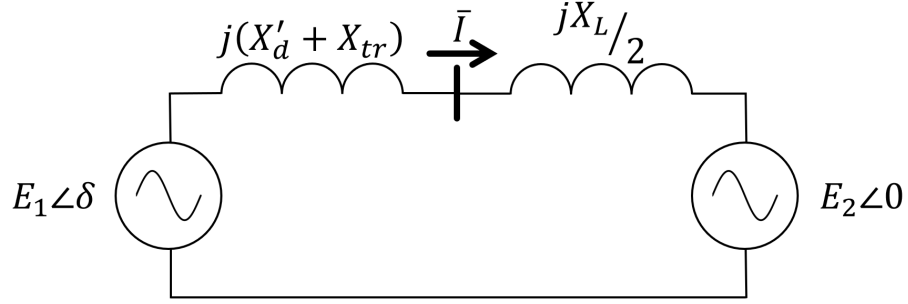


FIGURE 2.2: Single Machine Infinite Bus Equivalent Circuit

Ignoring all of the losses in the system of Figure 2.2, the derivation for the apparent power of the system at the infinite bus is given by

$$\bar{I} = \frac{\bar{E}_1 - \bar{E}_2}{j(X'_d + X_{tr} + \frac{X_L}{2})} = \frac{\bar{E}_1 - \bar{E}_2}{jX_{T1}} \quad (2.1)$$

At the infinite bus, the apparent power can be written as

$$S_2 = P_2 + jQ_2 = E_2 \bar{I}^* \quad (2.2)$$

Using the complex conjugate from Equation (2.1) into Equation (2.2), we have

$$P_2 + jQ_2 = E_2 \left(\frac{E_1 \angle(-\delta) - E_2}{-jX_{T1}} \right) = \frac{E_1 E_2 \sin \delta}{X_{T1}} + j \left(\frac{E_1 E_2 \cos \delta - E_2^2}{X_{T1}} \right) \quad (2.3)$$

The electrical power P_2 delivered by the generator to the infinite bus is given by

$$P_2 = \frac{E_1 E_2 \sin \delta}{X_{T1}} \quad (2.4)$$

where E_1 and E_2 are the magnitudes of the two voltages in V that are at angle δ (in electrical radians) apart and are connected through X_{T1} (in Ω) which is the total reactance of the line.

The above equation describes the electrical output of the generator in a lossless system, and is fundamental in understanding the transient behavior of the generator during transients. During short term transients, the excitation control system may not respond fast enough so that the generator voltage E_1 may be assumed to be constant. Likewise, the turbine governor control, whether steam or a hydro turbine, cannot react in such a short duration of time. Therefore, the mechanical power input P_m from the turbine to the generator can be assumed to be constant [33]. Thus any change in the electrical output of the generator due to a disturbance, such as a short circuit, will cause an imbalance between the generator mechanical input and the electrical output which is the onset of rotor oscillations and stability. The impacts of such oscillations are further discussed in the sequel.

2.2 Prime Mover

In conventional power plants, steam, hydro, or gas turbines act as the prime mover that provides the mechanical input power to the synchronous generators. Hydro turbines typically rotate at very low speeds (\sim hundreds of RPM) which requires a very large number of magnetic poles in the synchronous generator's construction to produce the $60Hz$ three-phase electrical power output. Steam or gas turbines typically operate at high speeds such as at 1800 RPM for producing the $60Hz$ output.

To begin describing the mechanical dynamics, one must first define what torque is and how it applies to a rotating system. Torque is the rotational equivalent to linear force, and is given by

$$T = r \times F \quad (2.5)$$

In equation (2.5), when an external force F is applied to a rigid body in a perpendicular direction at a radius r from a pivot point, then a torque T is produced that causes the object to rotate as seen in Figure 2.3.

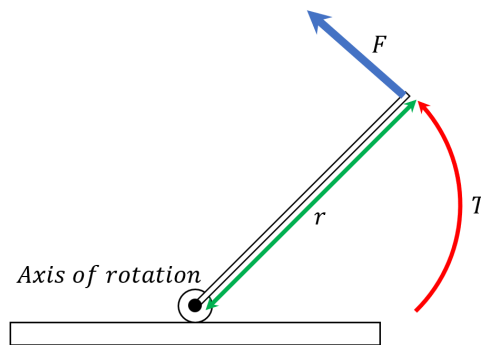


FIGURE 2.3: Torque Equation Lever Example

This base definition of torque in equation (2.5) correctly describes the torque T_m that causes the rotation of a turbine and synchronous generator connected by a shaft such as the one depicted in Figure 2.4.

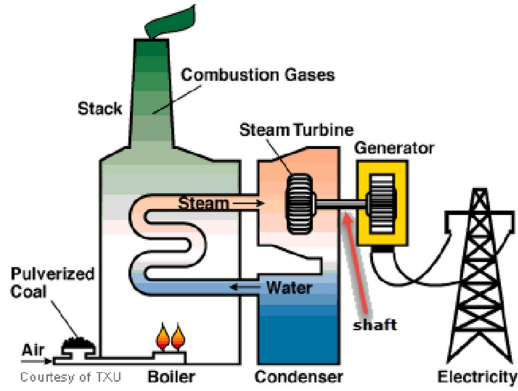


FIGURE 2.4: Steam Powered Turbine-Generator system

In a rotational system, the angular acceleration due to a net torque acting on it is determined by the moment-of-inertia J_m of the entire system. The net torque T acting on a rotating body of inertia J causes it to accelerate. This is similar to systems with linear motion where $F = ma$, Newton's law in rotational systems becomes [33]

$$T_{net} = J_m \alpha_m \quad (2.6)$$

where angular acceleration α_m in rad/s^2 is defined as

$$\alpha_m = \frac{d\omega_m}{dt} = \frac{T_{net}}{J_m} \quad (2.7)$$

The turbine produces the mechanical torque T_m applied to the generator shaft. The bearing friction and wind resistance (losses) can be combined with the synchronous generator electromagnetic torque T_e opposing the rotation. The net torque, the difference between the applied mechanical torque and the developed electrical torque opposing it, causes the combined inertia of the turbine and the generator to accelerate according to equation (2.7) where $T_{net} = T_m - T_e$ and J_m is the equivalent combined inertia of the system [33].

Equation (2.7) shows that the net torque is the quantity that causes acceleration, which leads to changes in speed and position. Integrating $\alpha(t)$ w.r.t. time, we have

$$\begin{aligned}\omega_m(t) &= \omega_m(0) + \int_0^t \alpha(\tau) d\tau \\ \theta(t) &= \theta(0) + \int_0^t \omega_m(\tau) d\tau\end{aligned}\tag{2.8}$$

where $\omega_m(0)$ and $\theta(0)$ are the speed and the rotor angle at $t = 0$. These equations show that torque is the fundamental variable for controlling speed and position of the generator rotor [33].

In a rotational system, if the net torque T causes the turbine and in turn the synchronous generator to rotate by a differential angle $d\theta$, then the differential work done is

$$dW = Td\theta\tag{2.9}$$

If this differential rotation takes place in a differential amount of time dt , then the power can be expressed as

$$p = \frac{dW}{dt} = T \frac{d\theta}{dt} = T\omega_m\tag{2.10}$$

where $\omega_m = d\theta/dt$ is the angular speed of rotation.

This covers the basis for the prime mover dynamics which will be needed to both understand and define the swing equation which will be covered in section 2.4.

2.3 Excitation System

The generator excitation system consists of the generator field winding and the associated control system for controlling the field supply. Voltage is induced in the generator armature by electromagnetic induction due to magnetic field produced by the field winding of the rotor. The field winding is mounted on the rotor, and is fed by a DC voltage V_f . The resulting current I_f in the field winding produces magnetic flux that links with the stator winding to produce the induced voltage. By controlling the field-voltage V_f and hence the field-current I_f , one can effectively control the magnetic field produced by the rotor, and thus control the induced emf of the generator and control the real and reactive power delivered by the generator [33].

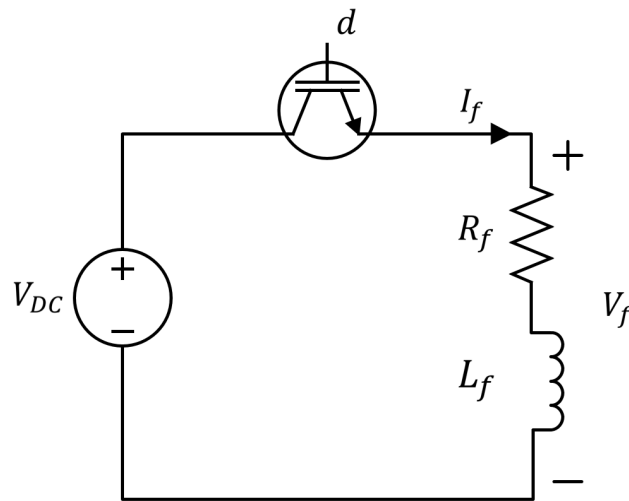


FIGURE 2.5: Rotor Field Circuit

In this research, we use an IGBT to control the DC voltage in the field circuit. The rotor field circuit in Figure 2.5 is made up of a DC voltage source V_{dc} , a field coil L_f with a coil resistance R_f , and an IGBT with the gate controlled by a PWM signal. The PWM signal's duty cycle d is modulated according to the

control system's feedback loop. The effective DC field-voltage V_f is related to V_{dc} by the duty cycle as given by

$$V_f = d V_{dc} \quad (2.11)$$

Equation (2.11) essentially states that the effective field-voltage is equivalent to the modulated DC voltage source. The corresponding field current is then given by

$$I_f = \frac{V_f}{R_f + sL_f} \quad (2.12)$$

where s is the Laplace variable. The field-current generates the magnetic field that induces an EMF E_a on the stator coils in accordance to Faraday's law, thus controlling the output voltage of the generator. Neglecting saturation, the induced emf is given by

$$E_a = K_f I_f \quad (2.13)$$

According to Equation (2.13), the induced EMF E_a is linearly related to field-current I_f by the magnetization constant K_f . Determination of the magnetization constant K_f is discussed in detail in Section 3.4.5.

2.4 Swing Equation

The rotor of the synchronous generator starts to swing when there is an imbalance between the mechanical input torque T_m and the electrical output torque T_e , i.e., the electrical torque T_e does not equal the mechanical torque T_m . Using the Newton's law, this rotor oscillation can be described by

$$J_m \frac{d^2 \delta_m}{dt^2} = T_m - T_e \quad (2.14)$$

where J_m is the moment-of-inertia of the rotational system including the prime mover rotor and the generator rotor. The difference between the mechanical input torque T_m and the electrical output torque T_e is the accelerating torque. The rotor angle δ_m is the measure of change of angular position of the rotor with respect to a synchronously rotating reference frame. Multiplying both sides of equation (2.14) by the rotor mechanical speed ω_m yields

$$\omega_m J_m \frac{d^2 \delta_m}{dt^2} = P_m - P_e \quad (2.15)$$

To simplify mathematical analysis, it is better to express the above equation in normalized per unit using a new inertia-related parameter H_{gen} which is defined as the ratio of the kinetic energy of the rotating mass at the rated synchronous speed $\omega_{syn,m}$ in mechanical radians per second to the three-phase apparent power rating $S_{rated,gen}$ of the generator:

$$H = \frac{\frac{1}{2} J_m \omega_{syn,m}^2}{S_{rated,gen}} \quad (2.16)$$

Using equation (2.16) in equation (2.15), one obtains

$$\left(\frac{\omega_m}{\omega_{syn,m}} \right) \frac{2H}{\omega_{syn,m}} \frac{d^2 \delta_m}{dt^2} = P_{m,pu} - P_{e,pu} \quad (2.17)$$

Without any loss of generality, one can assume that the generator base power is same as the system base power. Furthermore under transient conditions, it is reasonable to assume that the rotor mechanical speed ω_m is approximately equal

to the synchronous speed $\omega_{syn,m}$ corresponding to the frequency of the infinite bus. Thus Equation (2.17) can be simplified as

$$\frac{2H}{\omega_{syn,m}} \frac{d^2\delta_m}{dt^2} = P_{m,pu} - P_{e,pu} \quad (2.18)$$

In Equation (2.18), the angle deviation and the synchronous speed can be expressed in terms of electrical radians to obtain

$$\frac{2H}{\omega_{syn}} \frac{d^2\delta}{dt^2} = P_{m,pu} - P_{e,pu} \quad (2.19)$$

Equation (2.19) is called the *swing equation* which describes how the angle δ swings due to an imbalance between the mechanical input power and the electrical output power of the generator. The swing equation is most useful for determining the stability of a generator in the presence of transient disturbances or for determining if the generator will be capable of recovering after a fault has cleared.

Chapter 3

HIL CYBER PHYSICAL SYSTEM

The purpose of this chapter is to provide the details behind the development of the HIL system discussed in this thesis. The technology presented in chapter 3 is implemented specifically for the purpose of developing an HIL system and experimentally determining a generator's physical constants. There is a top level overview of the HIL system described in this thesis followed by a detailed explanation for determining a generator's physical parameters for the purpose of developing a generator excitation control system.

3.1 HIL Overview

The HIL simulation is based on a hybrid configuration of a cyber system and a physical system that interact with each other through digital and analog input/output (I/O) signals. The cyber system uses the computing power and flexibility of a real time digital simulator, such as Opal-RT or RTDS, that receives

feedback signals from the connected physical system. Figure 3.1 shows the high-level view of the HIL testbed for closed-loop control of a three-bus electrical grid which consists of two generator buses and a load bus. The load is shared by the two synchronous generators, and as the load changes, the terminal voltage of the generators change accordingly. The generator terminal voltages are controlled by adjusting the field current using a controller. The feedback loop is made through the OP8660 for data transmission between the generator terminals to the controller on the Opal-RT, and between the controller and the field coil of the generator. This makes the closed loop system vulnerable to cyberattacks since a cyber intruder can initiate a data attack or a denial-of-service (DoS) attack in the generator control system.

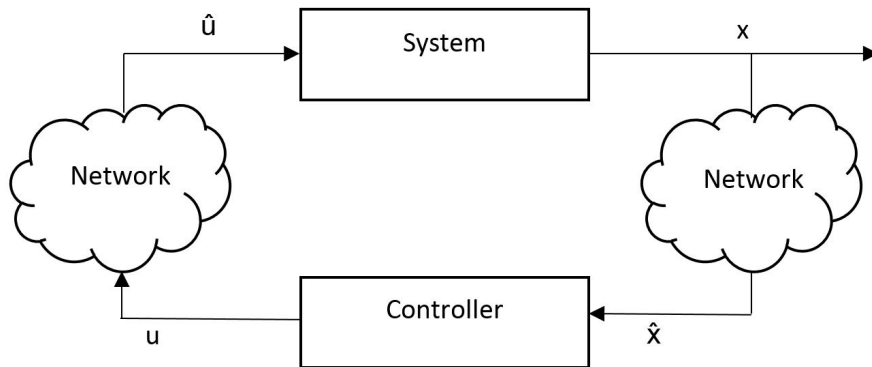


FIGURE 3.1: Schematic of Closed Loop NCS

3.2 Opal-RT Simulator

The developed HIL system uses an Opal-RT real-time processor for implementation of the controller for the two generators. Opal-RT is a PC/FPGA-based real-time simulator for the HIL experimental platform presented in this paper. The specific Opal-RT hardware platform in the experiments shown in Figure 3.2 is an OP5600 in conjunction with an OP8660 HIL controller and data acquisition interface. The OP5600 is equipped an Intel Xeon CPU and

a Xilinx Spartan-3 FPGA. The simulations are executed on the CPU and the FPGA handles the hardware interface and is reconfigurable to suit the individual users specifications. The OP8660 is a user-friendly interface meant to ease the integration process as the I/O connection options are commonly used banana cables or DB9 cables. The OP8660 is especially good for interfacing with the LabVolt series of equipment as it was specifically made for it, but not exclusively so.



FIGURE 3.2: OP5600 and OP8660 from left to right

The process of utilizing the Opal-RT platform consists of first creating a Matlab/Simulink model to meet the users goals (in this a case a controller and data acquisition system). The model is then configured to communicate with the specific hardware needed to properly execute the HIL setup. Once the hardware is connected to the Opal-RT platform and the system is properly configured, the user can run the model on the Opal-RT and gather data for analyzing and controlling the HIL experimental setup.

The setup specific to this application as shown in figure 3.3 portrays how the overall HIL creation, setup, and operation is accomplished. The initial step in the process is to create and build the Matlab/Simulink model on the host computer and then send the built model to the Opal to be executed. Another aspect of the host computer in the HIL setup is to act as the user interface console for the Opal whilst the model is running. The host computer console displays information such as voltages, currents, control signals, and send commands such as turn the

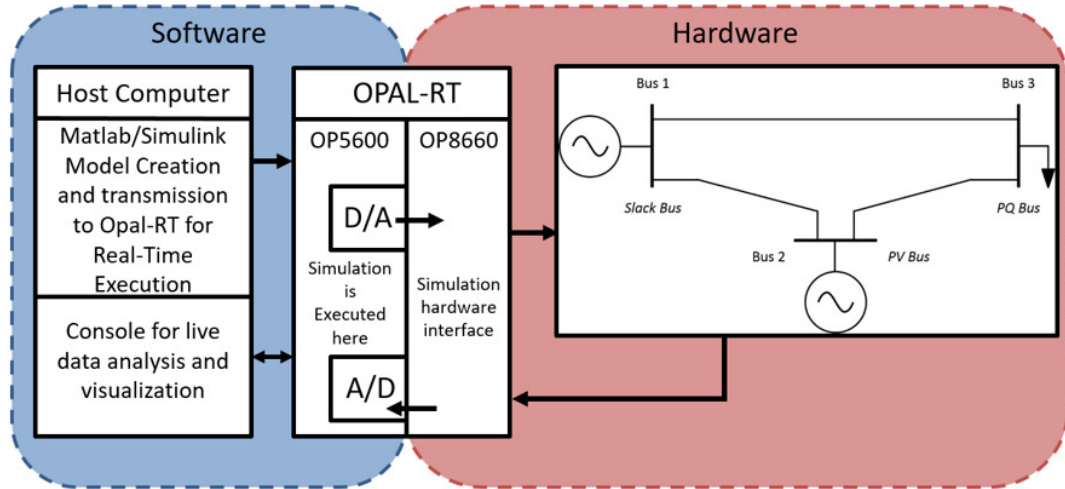


FIGURE 3.3: Opal-RT High Level Control Loop

controllers on/off or change control gains. The model is executed in real-time on the OP5600. The communication between the OP5600 and the hardware is accomplished with the OP8660 HIL controller and data acquisition interface which transmits the control signals to the hardware and receives the voltage and current measurements and conditions the signals to the proper voltage levels accepted by the analog to digital converter on the OP5600.

3.3 The Physical System - Three Bus Grid

The proposed experimental physical system is a three-bus electric network as shown in Figure 3.4. The developed three-bus system consists of two LabVolt EMS8000 series synchronous generators driven by dynamometers acting as the prime movers. The dynamometers were configured so that the slack bus generator runs at constant speed of 1800 rpm, and the PV bus generator supplies constant power using built-in fast-acting dynamometer control systems, however the speed can vary during transients. The load bus consists of switchable RLC loads through three transmission lines as shown. The actual hardware used in the testbed is shown in Figure 3.5.

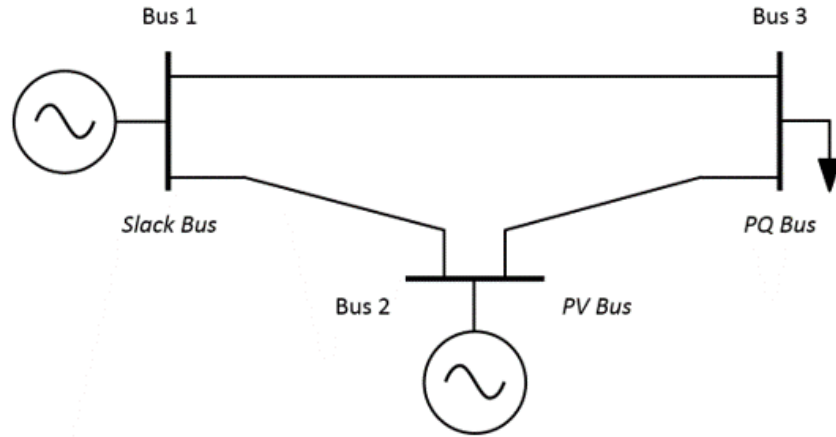


FIGURE 3.4: Three-Bus Electrical Network

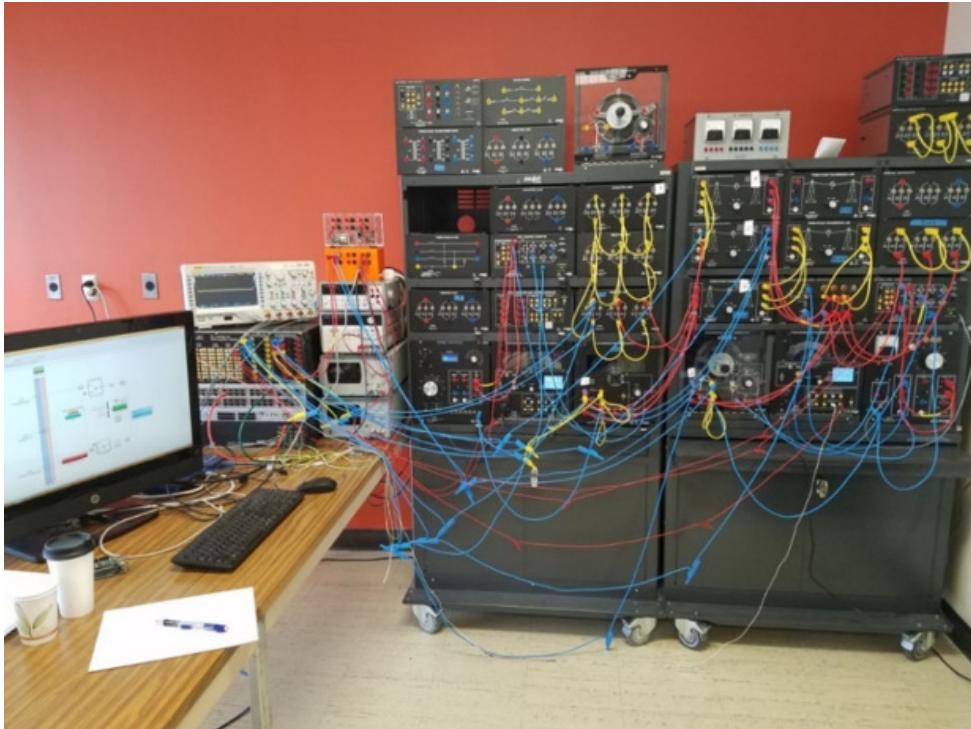


FIGURE 3.5: Experimental Setup

3.3.1 Generator Excitation System

The schematic of the generator field excitation system is shown in Figure 3.6, which consists of a PI (proportional-integral) controller and an IGBT supplying

the generator field coil. The IGBT regulates its DC output voltage based on gate pulse supplied by the PI controller, and the corresponding field current is nearly constant because of high inductance of the field winding. The induced electromotive force (EMF) of the generator is proportional to the duty ratio of the IGBT.

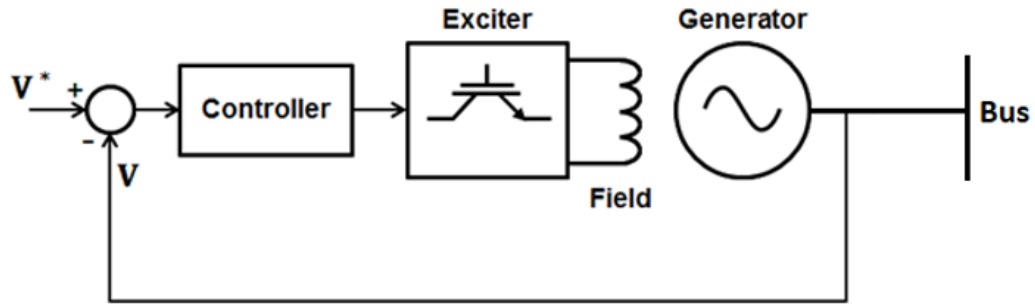


FIGURE 3.6: Generator Excitation System

3.4 Generator Parameters

3.4.1 Synchronous Generator Constants

The generators used in the experiments are the $0.2kW$ LabVolt 8241-2 synchronous machine modules. The generators used are 4 pole synchronous machines, which means the peaks of the generated voltages correlate directly to a physical position of the rotor. Therefore, the synchronous speed of the prime mover is governed by:

$$N_s = \frac{120f}{p} \quad (3.1)$$

where N_s is the synchronous speed of the generator in revolutions per minute (RPM), f is the frequency produced by the rotational speed of the generator, and p is the number poles on the rotor. Therefore, the prime mover must rotate at $1800RPM$ to produce a $60Hz$ three phase voltage. Since LabVolt does not offer

the information necessary to develop a control model that involves the physical characteristics of their synchronous machines, it was necessary to determine them through experimentation. The evaluation of these constants will provide the information necessary in the development of the excitation controller for the generators.

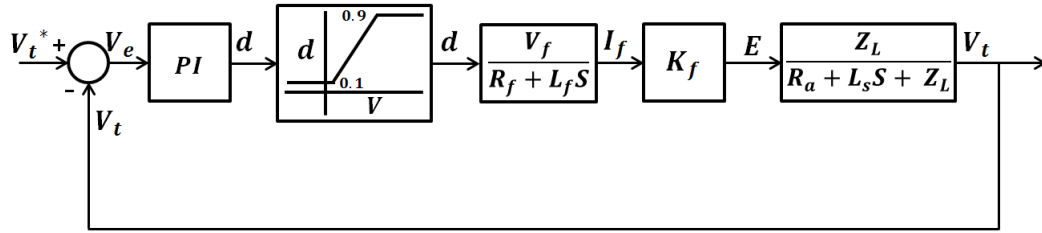


FIGURE 3.7: Complete Excitation Control System

Figure 3.7 is the complete excitation control system with both the generator physical characteristics and equivalent circuit parameters [34] included in the system. The constants to be determined are as follows:

Synchronous Generator Constants	
R_a	Armature Resistance
R_f	Field Resistance
L_f	Field Inductance
L_s	Stator Inductance
K_f	Magnetization Constant

TABLE 3.1: A List of Synchronous Generator Constants

3.4.2 Determination of Armature Resistance R_a and Field Resistance R_f

Of the constant values that are needed in the Control system model in table 3.1, R_a and R_f are the simplest to measure and determine. The measurements were obtained with the TPI 192 II Digital Multimeter. The armature resistance is the DC resistance of the stator coil of the synchronous generator and R_a was measured

to be 12Ω . The measurement of the field resistance was done in the same way, but instead it was the resistance of the rotor winding (R_f) and the experimentally observed value is 188.8Ω .

3.4.3 Evaluation of the Field Inductance L_f

The procedure to determine the inductance of the field coil starts with the KVL that relates the field current to the applied field voltage given below:

$$V_f(t) = R_f i_f(t) + L_f \frac{di_f(t)}{dt} \quad (3.2)$$

The Laplace transform is then applied to equation (3.2),

$$I_f(s) = V_f \left(\frac{1}{s(R_f + L_f s)} \right) \quad (3.3)$$

Applying the inverse the Laplace transform to equation (3.3) yields the solution to equation (3.2).

$$i_f(t) = \frac{V_f}{R_f} - \frac{V_f}{R_f} e^{-\frac{R_f}{L_f} t} \quad (3.4)$$

The transient response of equation (3.4) is used to determine L_f . A new $y(t)$ is defined to remove the steady state response of the solution:

$$y(t) = i_{f_{ss}}(t) - i_f(t) \quad (3.5)$$

The natural logarithm is then applied to equation (3.5),

$$\log (y(t)) = \log \left(\frac{V_f}{R_f} \right) - \frac{R_f}{L_f} t \quad (3.6)$$

Equation (3.6) is now linear with a slope that relates L_f and R_f .

A step response of the experimental setup was recorded and the data of the transient was isolated. Once isolated, the natural logarithm was applied to the data set and a best fit line approximation was used to obtain a slope in Figure 3.8.

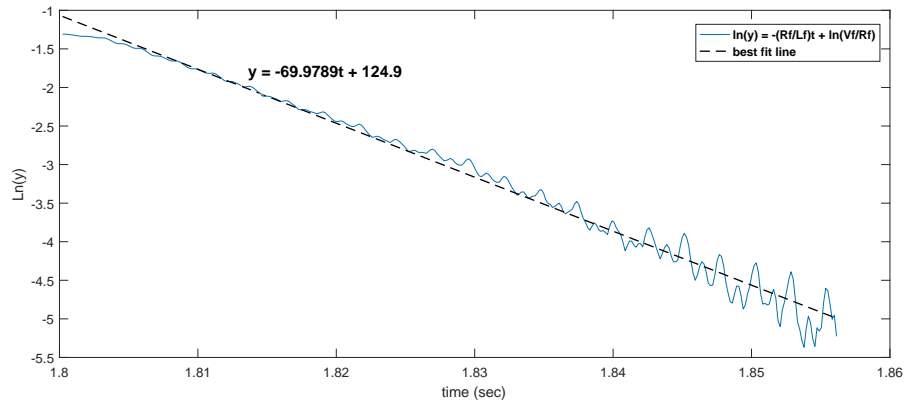


FIGURE 3.8: Experimental Evaluation of L_f

By combining the $slope = \frac{R_f}{L_f}$ from equation 3.6 with the results from Figure 3.8, an approximate value for L_f was determined to be approximately $2.7H$.

3.4.4 Determination of the Stator Inductance L_s

The inductance of the stator winding in the generator is determined using both the short-circuit and open-circuit tests. Details of both of these tests can be found in [34]. With the data collected from the two tests, a plot is created to determine an approximate value of L_s based on the short circuit current, the open circuit phase voltage, and the operating field current of the rotor.

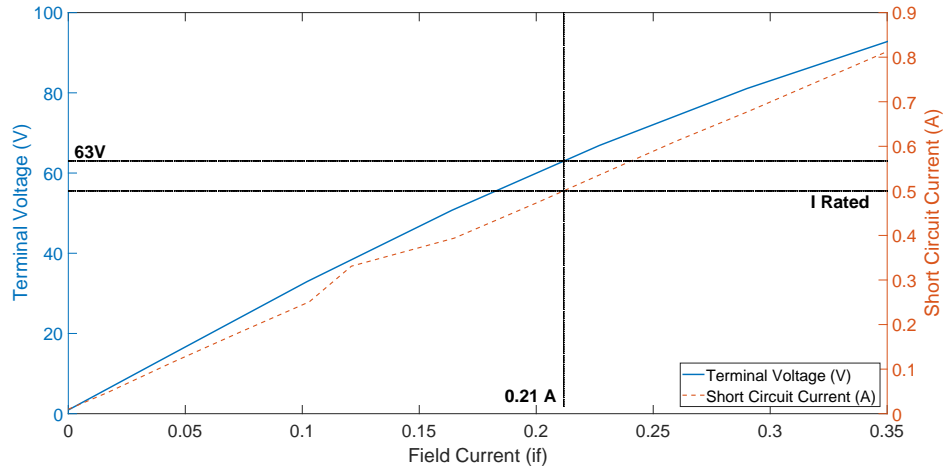


FIGURE 3.9: Plot to find L_s

The inductance of the stator winding is evaluated using:

$$\frac{V_{oc}}{I_f} = X_s = \omega L_s \quad (3.7)$$

where I_f is the field current at which the short circuit current is equal to the rated current of the machine. The open circuit voltage is selected as well based on that rated current. From Figure 3.9, assuming the machine is rotating at $1800RPM$, equation is evaluated from

$$L_s = \frac{\left(\frac{63}{0.21}\right)}{2\pi 60} = 0.7958H \quad (3.8)$$

3.4.5 Evaluation of the Magnetization Constant K_f

The evaluation of K_f , the magnetization constant, is done by measuring both the generator's induced EMF and the field current. The experiment is performed with the prime mover rotating at $1800RPM$ to produce the $60Hz$ electrical frequency of the generator to simulate proper working conditions. To measure the induced EMF, the generator terminals were measured directly with a voltage meter and no load was attached. The field current was measured with an ammeter. Plotting

the induced EMF against the field current supplied yielded the results in Figure 3.10.

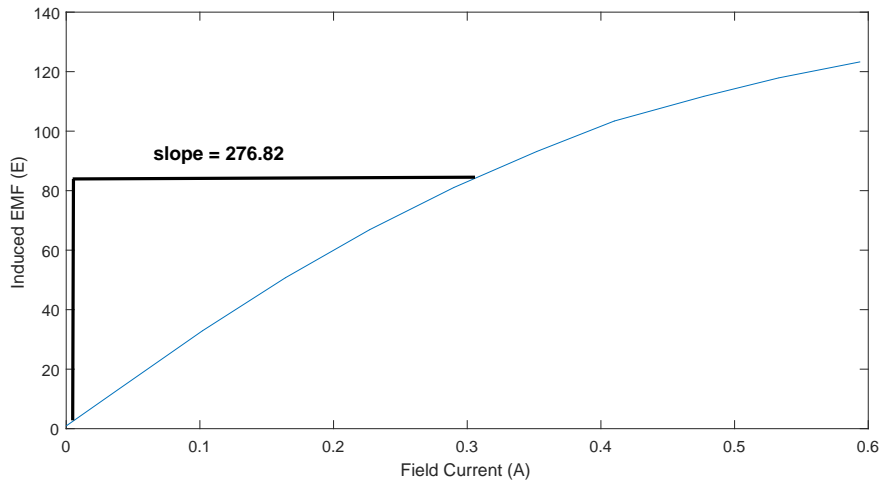


FIGURE 3.10: Plot to find K_f

Neglecting saturation, the generator induced EMF is proportional to the field current given by

$$E_a = K_f i_f \quad (3.9)$$

Notice the induced EMF eventually saturates as the field current is increased. For this reason, the generator's operational voltage was set to 75V to remain in a linear operating region, keeping K_f constant. Equation (3.9) shows that K_f relates the induced EMF to the field current and as long as it remains in the linear operating region, K_f is approximately 276.82 Ω .

This completes determination of physical parameters of the generator.

Chapter 4

MULTIBUS SYSTEM

This chapter reviews the basic mathematical framework for modeling and control of multibus power systems. A multibus power system consists of a) transmission system consisting of transmission lines that are connected to various buses in the network, and b) power generators connected to some of the buses, and c) loads also connected to some of the buses. In a commercial power grid, there are typically thousands of transmission lines, hundreds of buses and generators. System loads supplied by distribution network are aggregated at the buses. This chapter presents the methodology for developing a complete dynamic mathematical model of the multibus system that could be used for analysis and control design.

In large scale power system analysis, transmission lines are represented as a π section model with line resistance and inductance in series and line conductance and capacitance to ground as shunt branches. For simplicity, transmission lines are represented by algebraic equations resulting from KVL and KCL. Power generators are represented by the classical model as a voltage source with a series impedance. Also system load at the buses are represented as constant impedances although this assumption may not be always valid, especially for power electronic loads. Thus the multibus system could be represented as a set of algebraic equations

that are then coupled with prime mover model represented as the swing equation. The next few sections provide the details.

4.0.1 Load Model

Consider a power grid consisting of N generator buses and M load buses which are numbered sequentially. The first step in the analysis is to represent the load at each bus as a constant impedance. This is done using a load flow analysis under normal operating conditions. Dividing the bus voltage by bus current injection, one obtains the load impedance. For each bus, denote

$$V_i \angle \theta_i = \text{bus voltage}$$

$$I_i \angle \phi_i = \text{current injection}$$

$$E_i \angle \delta_i = \text{Excitation voltage for generators}$$

The loads must be represented as equivalent admittances based on load flow analysis. For each load, denote V_ℓ , P_ℓ , Q_ℓ , and I_ℓ as load voltage, real and reactive power, and load current, respectively. Also let the load admittance be denoted as $Y_\ell = G_\ell + jB_\ell$. Then we have $I_\ell = Y_\ell V_\ell$, and

$$\begin{aligned} P_\ell + jQ_\ell &= V_\ell I_\ell^* \\ &= V_\ell V_\ell^* (G_\ell - jB_\ell) \\ &= V_\ell^2 (G_\ell - jB_\ell) \end{aligned} \tag{4.1}$$

This gives the load admittance

$$Y_\ell = \frac{P_\ell}{V_\ell^2} - j \frac{Q_\ell}{V_\ell^2} \tag{4.2}$$

Using the above equation, one represents all loads by corresponding admittances. As discussed earlier, a constant admittance representation of a load is not always a valid assumption, nevertheless for the sake of simplicity, we will use it here.

4.0.2 Grid Model

Starting with the Kirchoff's current law, the transmission grid can be represented in the matrix form as $I = YV$, where I is the bus current injection, V is the bus voltage, and Y is the admittance matrix of the network. Partitioning this equation, we have

$$\begin{bmatrix} I_G \\ 0 \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix} \begin{bmatrix} V_G \\ V_L \end{bmatrix} \quad (4.3)$$

Here I_G and V_G are generator current injection and generator bus voltages respectively, and V_L is the load bus voltage, all represented as vectors. Note that loads are represented as admittances so that there are no current injections at the load buses. Rewrite the above equation as

$$\begin{aligned} I_G &= Y_{11}V_G + Y_{12}V_L \\ 0 &= Y_{21}V_G + Y_{22}V_L \end{aligned} \quad (4.4)$$

Simplifying these equations, we obtain

$$\begin{aligned} I_G &= [Y_{11} - Y_{12}Y_{22}^{-1}Y_{21}]V_G \\ &= Y_R V_G \end{aligned} \quad (4.5)$$

Here Y_R is the reduced bus admittance matrix with all load buses removed. This is the complete network model in terms of voltages and currents at the generator buses.

4.0.3 Combined Generator and Grid Model

Generator excitation control directly affects the generator excitation voltage. Thus it is necessary that the above equation be further simplified to express the network in terms of the excitation voltages rather than the generator bus voltages. This could be done by expressing the generator bus voltage in terms of excitation voltage and the generator impedance. Considering the classical model of the generator, assume $z_i = r_i + jX_{d_i}$ as the impedance of the generator. Then the generator current is given by

$$I_i = \frac{E_i - V_i}{r_i + jX_{d_i}}, \quad i = 1, 2, \dots, N$$

Writing the above equation for all generator buses, we obtain

$$\begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_N \end{bmatrix} = \begin{bmatrix} \frac{1}{r_1 + jX_{d_1}} & 0 & \cdots & 0 \\ 0 & \frac{1}{r_2 + jX_{d_2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{r_N + jX_{d_N}} \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_N \end{bmatrix} - \begin{bmatrix} \frac{1}{r_1 + jX_{d_1}} & 0 & \cdots & 0 \\ 0 & \frac{1}{r_2 + jX_{d_2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{r_N + jX_{d_N}} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_N \end{bmatrix}$$

which is symbolically expressed as

$$I_G = Y_G E_G - Y_G V_G \tag{4.6}$$

which is combined with equation (4.5)

$$I_G = Y_G E_G - Y_G V_G = Y_R V_G$$

from which we obtain

$$(Y_R + Y_G)V_G = Y_G E_G \quad (4.7)$$

and hence

$$V_G = [Y_R + Y_G]^{-1} Y_G E_G$$

Substituting the above equation into equation (4.6), we obtain

$$\begin{aligned} I_G &= [Y_G - Y_G(Y_R + Y_G)^{-1}Y_G] E_G \\ &= Y_R(Y_R + Y_G)^{-1}Y_G E_G \\ &= Y E_G \end{aligned} \quad (4.8)$$

This completes the grid model in terms of generator current injection and the generator excitation voltages. This is very significant since it describes the grid in terms of generator currents and generator excitation voltages. The network topology is embedded in the admittance matrix of the above equation. Also note that once I_G and E_G are known, we can always revert the process to obtain all bus voltages using equation (4.3).

4.0.4 Swing Equation

Synchronous generators enter into swinging oscillations when there is an imbalance between prime mover input and generator electrical output, which can be described by the swing equation. First we calculate the power supplied by each generator. As is well known, real power supplied by the generator is given by

$$P_i = \text{real}\{E_i I_i^*\}$$

Also from equation (4.8),

$$I_i = \sum_{j=1}^N Y_{ij} E_j = \sum_{j=1}^N (G_{ij} + jB_{ij}) E_j$$

so that combining the above two equations, we have

$$\begin{aligned} P_i &= \text{real} \left[\sum_{j=1}^N E_i E_j^* Y_{ij}^* \right] \\ &= \text{real} \sum_{j=1}^N \left[E_i \angle \delta_i E_j^* \angle \delta_j (G_{ij} - jB_{ij}) \right] \\ &= \text{real} \sum_{j=1}^N \left[E_i E_j \cos(\delta_i - \delta_j) + j E_i E_j \sin(\delta_i - \delta_j) (G_{ij} - jB_{ij}) \right] \\ &= \sum_{j=1}^N \left[E_i E_j G_{ij} \cos(\delta_i - \delta_j) + E_i E_j B_{ij} \sin(\delta_i - \delta_j) \right] \end{aligned} \tag{4.9}$$

The generator dynamics can be described by the swing equation

$$\begin{aligned} \dot{\delta}_i &= \omega_i - \omega_0 \\ \dot{\omega}_i &= \frac{\omega_0}{2H_i} \{ P_{m_i} - P_{e_i} \} \end{aligned} \tag{4.10}$$

where H_i is the generator inertia constant, P_m is the mechanical power input and P_e is the electrical power output of the generator. Substituting the generated power P_i from equation (4.9), we obtain

$$\begin{aligned} \dot{\delta}_i &= \omega_i - \omega_0 \\ \dot{\omega}_i &= \frac{\omega_0}{2H_i} \left\{ P_{m_i} - \sum_{j=1}^N [E_i E_j G_{ij} \cos(\delta_i - \delta_j) + E_i E_j B_{ij} \sin(\delta_i - \delta_j)] \right\} \end{aligned} \tag{4.11}$$

4.0.5 Excitation System

For most applications, the excitation voltage E_i is controlled by a local feedback loop using the terminal voltage and the frequency error. The schematic is shown

in Figure 4.1 below.

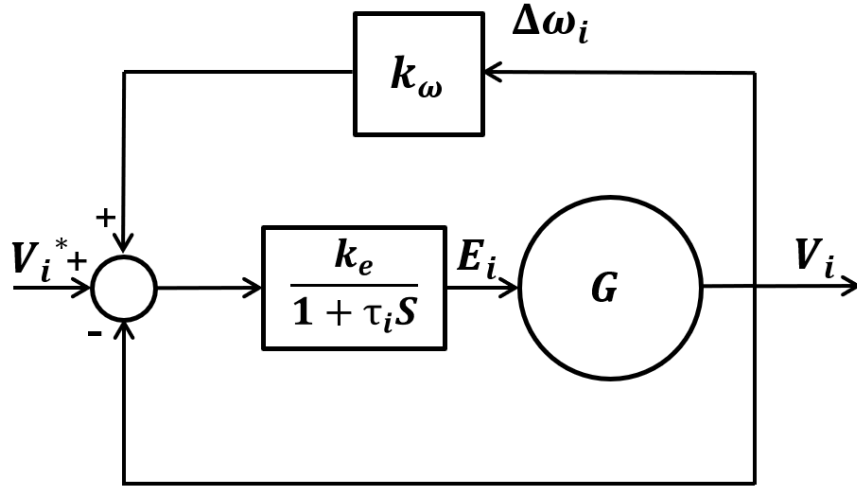


FIGURE 4.1: Excitation System

Here the exciter is represented as a first order system with τ_e and k_e as the time constant and gain, respectively. Modern power generators are usually fitted with a power system stabilizer based on frequency error. Using the above block diagram, we obtain the following equation for the excitation system:

$$\dot{E}_i = \frac{k_e(V_i^* - V_i + k_\omega \Delta\omega) - E_i}{\tau_i} \quad (4.12)$$

4.0.6 Prime Mover

The prime mover converts the energy from natural sources to rotational energy that drives the generator, which is then converted to electrical energy by the generator. The prime mover dynamics are complex depending on the fuel source and the design. Here we will consider a simple first order transfer function for the prime mover with a standard droop (proportional-integral) feedback based on frequency deviation. The block diagram of the prime mover is shown in Figure 4.2.

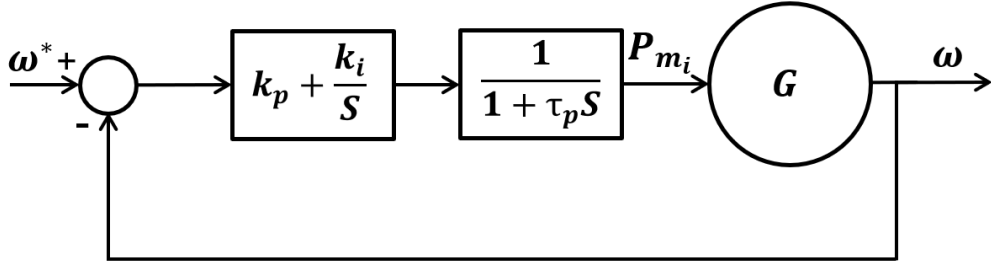


FIGURE 4.2: Excitation System

which gives

$$P_{m_i} = \frac{1}{1 + \tau_p s} \cdot \left(k_p + \frac{k_i}{s}\right) \Delta\omega \quad (4.13)$$

4.0.7 Complete System Model and Control Design

The complete dynamic model of the system is given by the coupled set of differential equations (4.11), (4.12), and (4.13). This completes the modeling of the multibus power grid that can be used for transient analysis and control design.

Clearly this is a nonlinear model consisting of many differential equations. For the design of a controller, one can linearize the system model and then use standard root locus or frequency domain tools to design the controller for the desired performance. Note that there are two controllers in the closed loop system: 1) the power system stabilizer in the feedback loop of the exciter, gain k_ω , and 2) the droop control in the prime mover that has the proportional gain k_p and the integral gain k_i . We shall not pursue the details of state space control design in this thesis.

4.1 Simulation Results

This section simulates transients in a three bus system following a 5-cycle short circuit. The 3-bus system in Figure 4.3 consists of a slack bus 1, a PV bus at Bus 2,

and a load bus at Bus 3 [33]. Assume that a 5-cycle short circuit to ground occurred on the transmission line between buses 1 and 2. The fault location is at 1/3rd distance from Bus 1 and 2/3rd distance from Bus 2. The fault is automatically cleared after 5 cycles.

It is assumed that there is no excitation control system for the two generators, in other words, the generator excitation voltages remain constant during transients. Also, we assume that there is no prime mover control for this system so that the prime mover input is constant. The following figures show the transients.

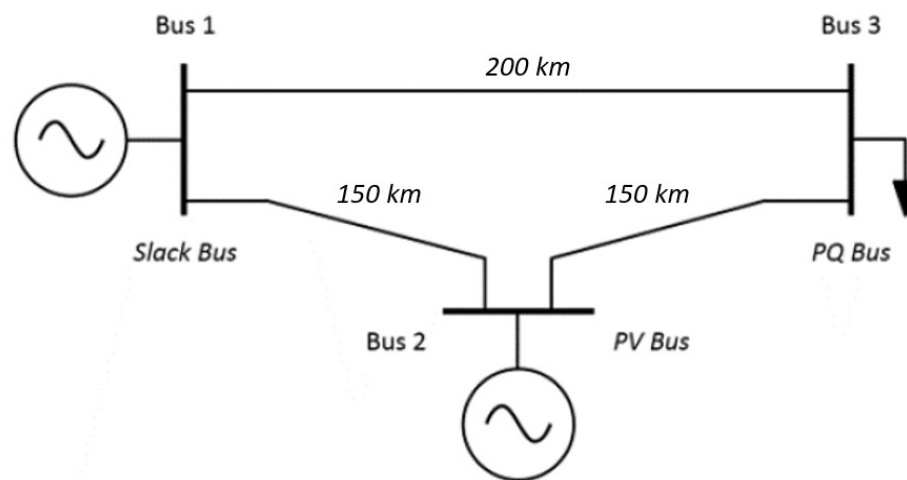


FIGURE 4.3: 3-Bus System

The frequency swing of the individual generators in Figure 4.4 shows that the two generators were attempting to return to the nominal frequency of $60Hz$ by compensating for one another as they settled out. Because of the initial short circuit, the total prime mover input is more than the load power so that both generators accelerated which accounts for the initial higher frequency swings right after the short circuit. The two generators slowly returned to the normal frequency state after some time due to natural friction losses of the generators.

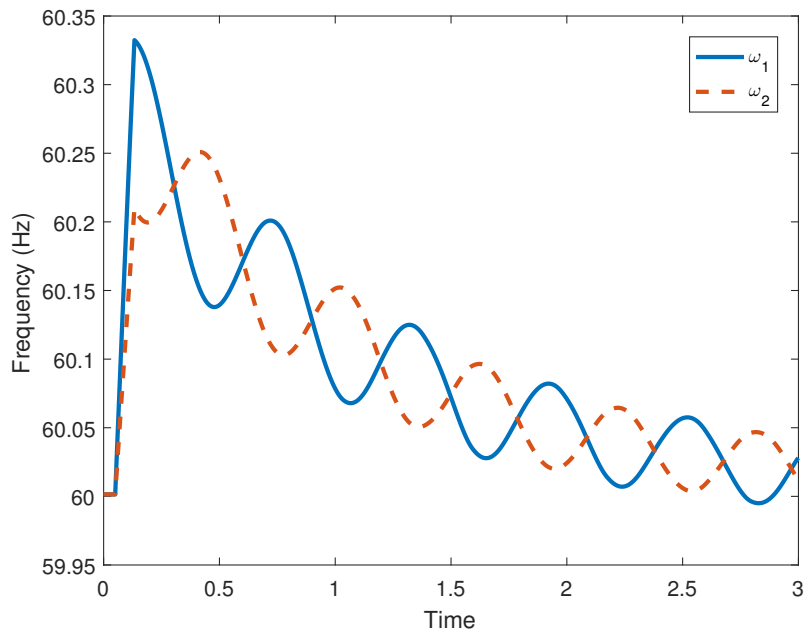


FIGURE 4.4: Frequency Swing

The bus voltage from Figure 4.5 at the load returned to the appropriate value as soon as the short was over, but there was larger difference between the slack bus and PV bus voltages because of the change in the individual rotor angle δ of the generators due to the fault.

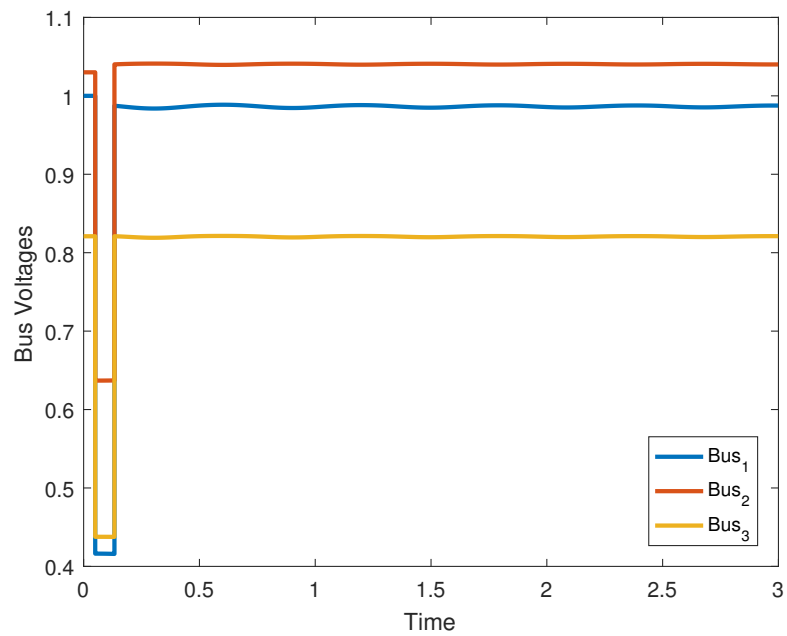


FIGURE 4.5: Bus Voltages

The fluctuating and increasing distance of the individual bus voltage angles w.r.t. the slack bus in Figure 4.6 indicate that fault caused PV bus to produce more reactive power and that effect can be observed on the load bus as well.

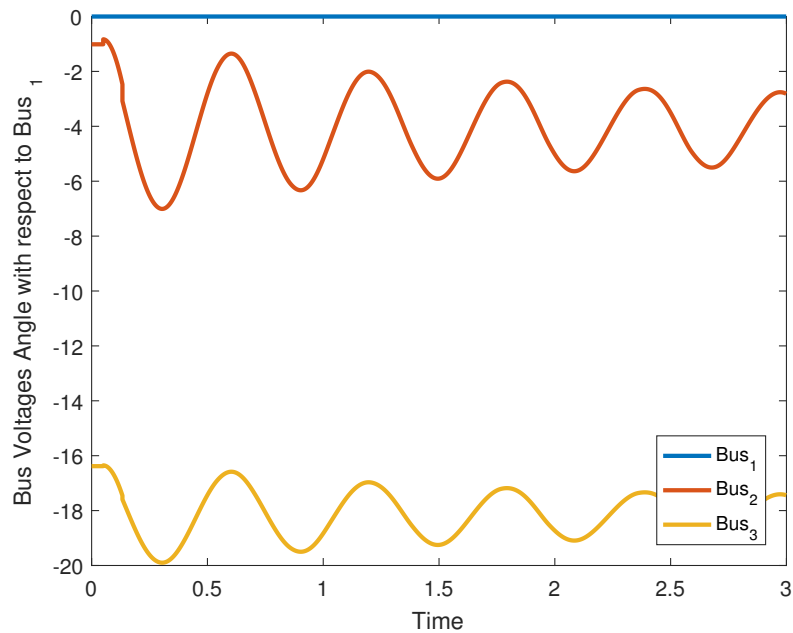


FIGURE 4.6: Bus Voltage Angles with respect to Bus 1

Since the fault occurred between the two generators, the Rotor angle swing varied wildly for the PV bus as shown in Figure 4.7 because PV generator could not compensate for the loss of power along that transmission line. Another reason is because the generators almost fell out of synchronism due to the fault which caused the big oscillations in the rotor angle of the PV bus with respect to the slack bus.

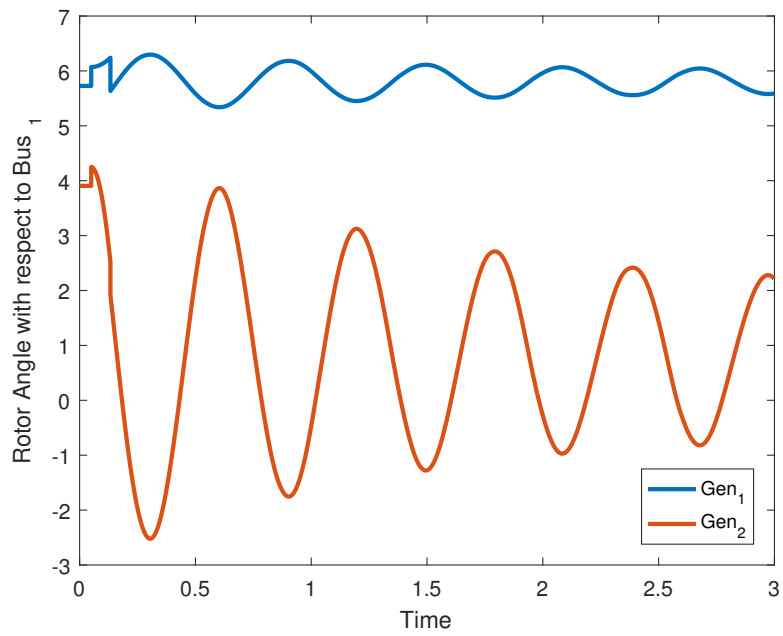


FIGURE 4.7: Rotor Angles with respect to Bus 1

The power supplied by both the generators in Figure 4.8 is oscillating, but will be settling out back at the prefault value if given sufficient time. The graph is showing on 3 seconds of simulation time to focus on the before during and after effects of the short circuit.

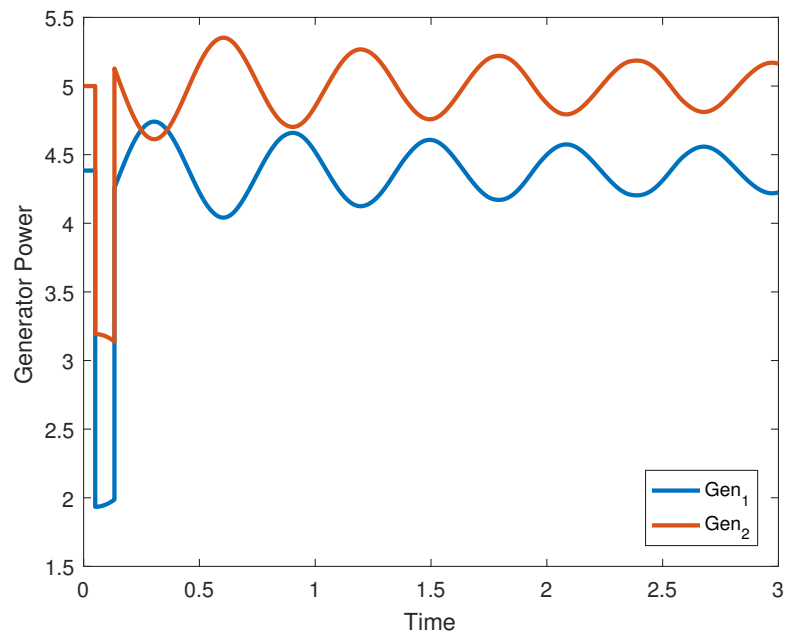


FIGURE 4.8: Power Supplied by the Generators

The reactive power of the two generators in Figure 4.9 has changed from pre-fault to post-fault due to a change in the rotor angles and the effective power being produced by the individual generators as a result of the fault. The sudden increase in reactive power supplied during the fault is a result of the voltage drop which causes the current to increase to maintain power supplied, causing system to consume more reactive power and the voltage drops further. If the current increase too much, transmission lines go off line, overloading other lines and potentially causing cascading failures.

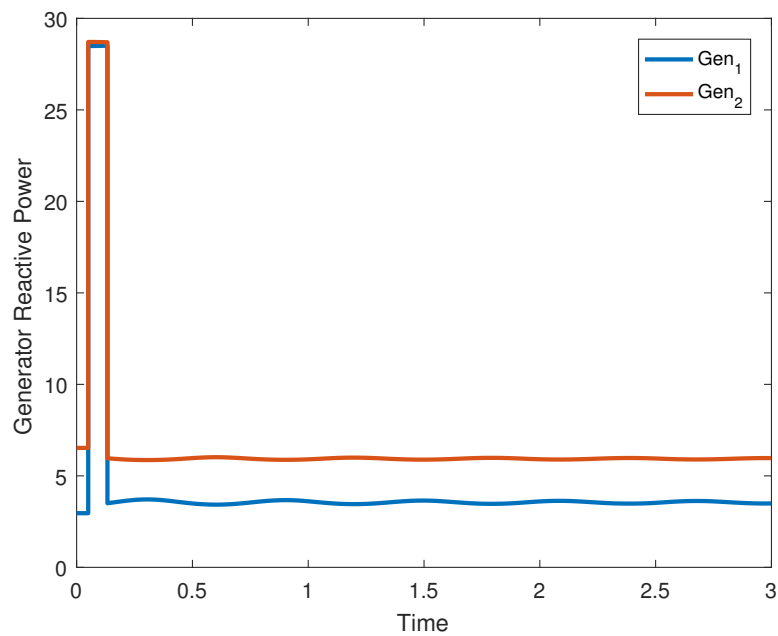


FIGURE 4.9: Reactive Power Supplied by the Generators

The excitation voltages in Figure 4.10 remained the same during the fault because the fault duration occurred over a such period of time (5 cycles) and it is being supplied by a separate DC source.

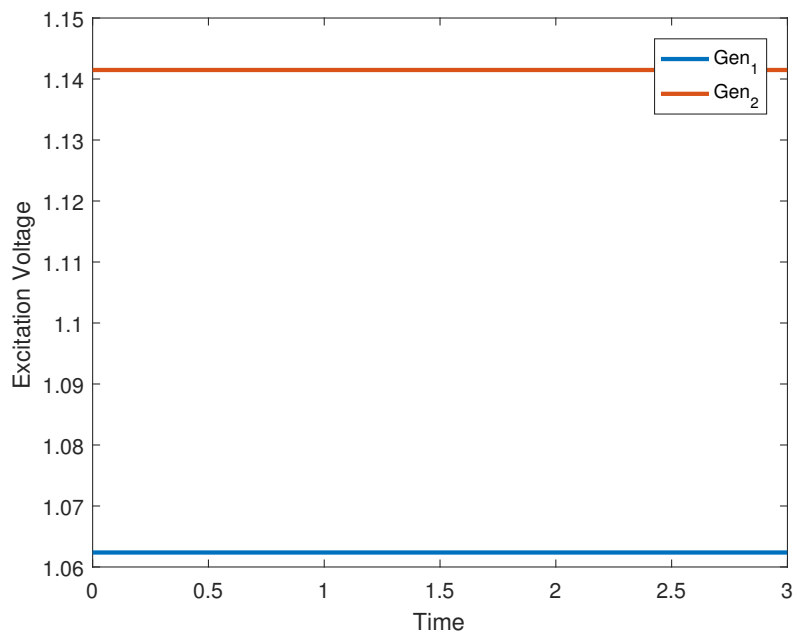


FIGURE 4.10: Excitation Voltage of the Generators

This chapter provides the basic understanding of transients in the power system following a disturbance. Most often power system transients occur due to short circuits, however transients could also start due to a cyberattack in the system. Most vulnerable element of the power grid is the control loop that include sensor network, feedback loop, and the controller. The dynamic model given above could be used for simulating such cyberattacks.

Chapter 5

EXPERIMENTAL RESULTS

In this section, we present the results of cyberattacks on the PV bus generator control system, however, no cyberattacks were considered on the slack bus generator. Cyberattacks were implemented in the simulation on the Opal-RT and were targeted specifically at the generator voltage sensor data and the controller. As the (simulated) intruder intercepts the voltage sensor data, the actual data received by the controller is modified according to the attack process.

The first step of experimentation is to synchronize the two generators. The slack bus generator was first configured to run at 1800 rpm. Then the PV bus generator controller was adjusted to generate 9.375W at 75V and 1800 rpm and the dynamometer was set to run at constant torque. A LabVolt synchronizing module was then used to synchronize the two generators. For this three-bus system, the PV bus generator output remained constant (except during transients), while the balance of PQ bus load and line losses are supplied by the slack bus generator.

5.1 Baseline Performance

To validate the performance of the excitation system controllers, first, we show the closed-loop system performance running under various load conditions. After the generators were synchronized, the PQ bus loads were turned ON and OFF at various time points as marked in Figures 5.1-5.4. Figure 5.1 clearly shows that the controller maintained the terminal voltage of the slack bus generator (middle window) and the PV bus generator (top window) constant as the PQ bus load was varied. Transients in the terminal voltage are however expected during the load switching as seen in Figure 5.1. The load bus voltage (bottom window) drops when load demand increases due to higher line voltage drop, increases when capacitive load is switched ON, which easily follows from simple circuit concepts. An opposite effect on terminal voltage at the load bus is observed when the inductive load is switched ON. Changes in load bus voltage were due to changes in the line voltage drop between the load bus and the other buses.

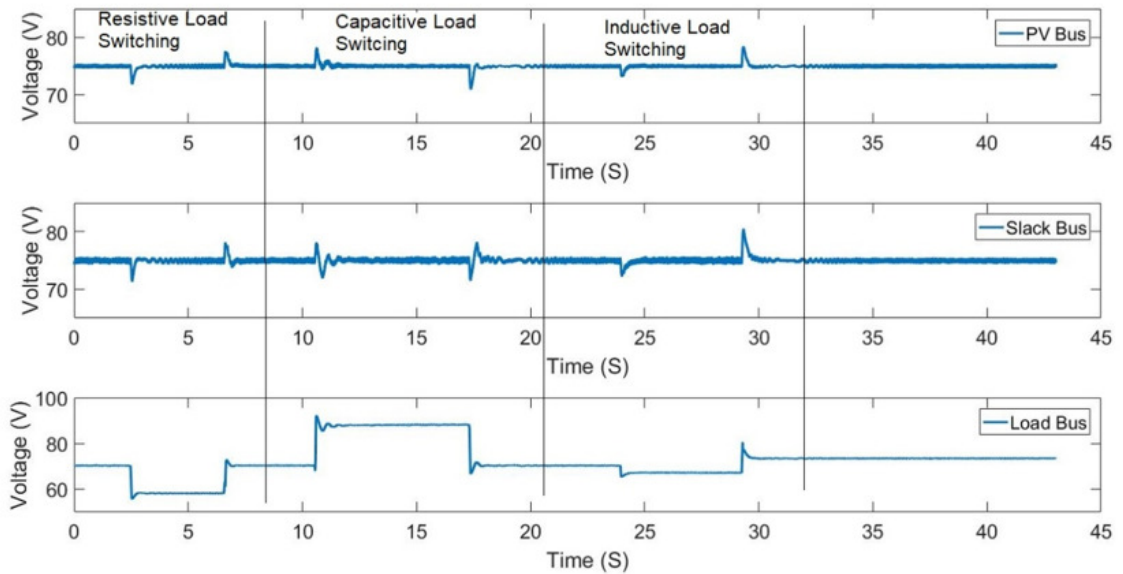


FIGURE 5.1: Bus Voltages for Load Switching

Figure 5.2 shows that the load current (bottom window) varies significantly with changes in load, however the current supplied by PV bus generator (top window) remained relatively constant which is expected since the PV bus generator operates as a constant torque generator producing constant output power. The slack bus generator (middle window) supplies the additional current required by the load and changes in line losses.

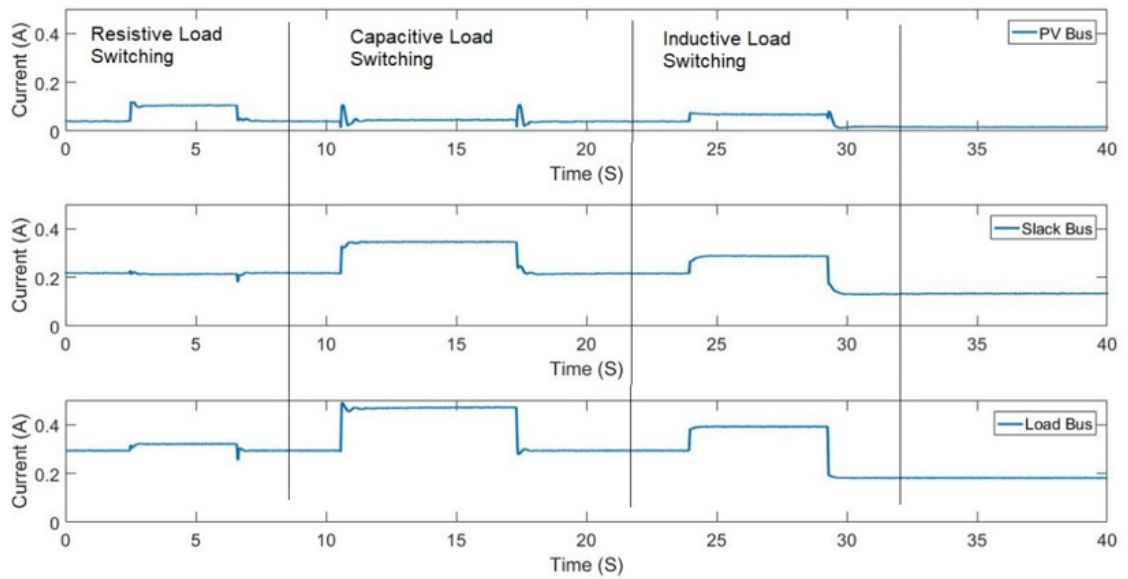


FIGURE 5.2: Bus Currents for Load Switching

Figure 5.3 shows the duty cycle ratio of the IGBT controller to the slack bus exciter. As the generator supplies more resistive current, its generated voltage must be increased so that the terminal voltage remains constant as signified by a higher duty cycle of the IGBT controller. Recall that the induced EMF is proportional to the IGBT duty cycle. For capacitive current loads, as expected the induced EMF must be decreased as seen from Figure 5.3 and corresponding lower duty cycle of the IGBT controller. For inductive loads, a higher duty cycle of the IGBT controller is required since induced EMF is expected to be higher. The duty cycle ratio of the PV bus IGBT controller remained relatively constant (not

shown in the figure) except during transients because the output current of the generator remained relatively constant. Here, we recall that the PV bus generator is expected to supply constant power output irrespective of variations in load.

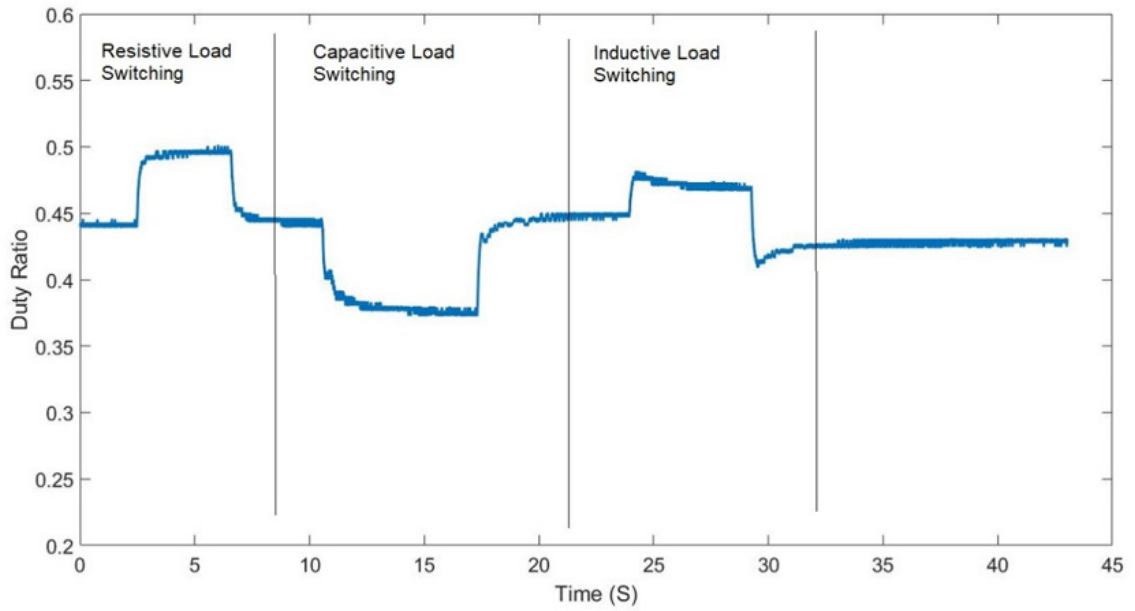


FIGURE 5.3: Duty Cycle Ratio of Slack Bus Generator for Load Switching

Figure 5.4 shows the speed of the PV bus generator which remained near 1800 rpm (except for a small bias in the measurement system). As expected, the speed varied during load switching, however returned to the normal speed within a few seconds. The speed of the slack bus generator was maintained constant by the dynamometer controller.

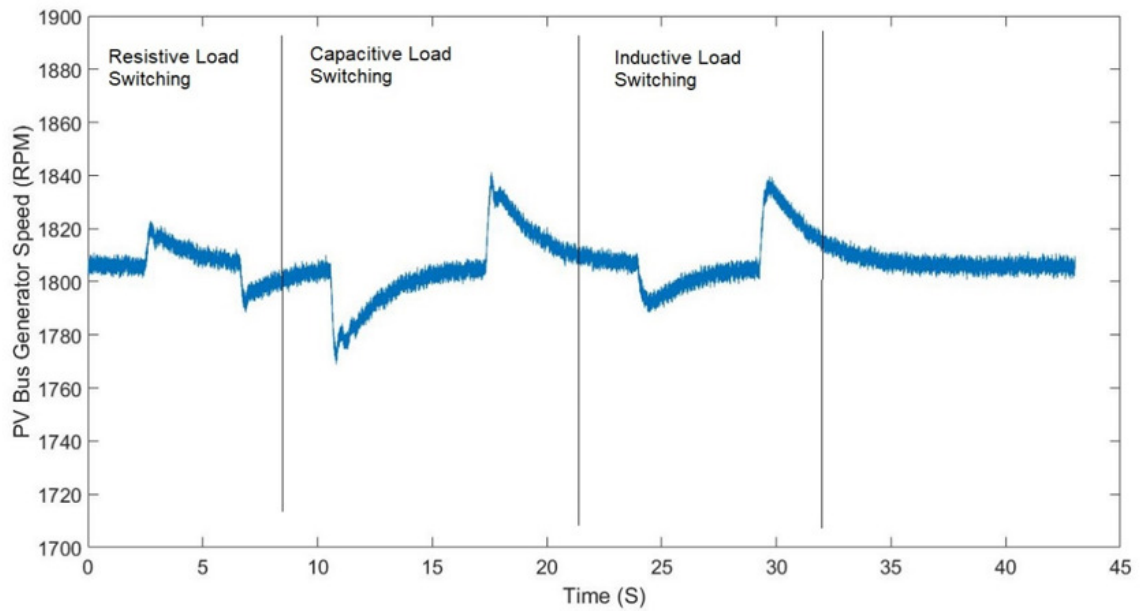


FIGURE 5.4: Generator Speed (PV Bus)

Overall, the baseline experimental data demonstrates that the controllers for both the slack bus and the PV bus generators were operating as expected. The gains of the PI controller were acceptable to maintain the terminal voltage of the two generators at the nominal value of 75V. Future experiments will include investigation of the effects of cyberattacks on the PV bus generator control system.

5.2 Cyberattack on a 2-Bus System

5.2.1 Constant Bias Attack

Figure 5.5 shows a constant bias attack in which the intruder injects a constant bias to the generator voltage data packets. The controller believes it is maintaining the desired terminal voltage, while the consumer is getting a voltage that is different from the expected voltage.

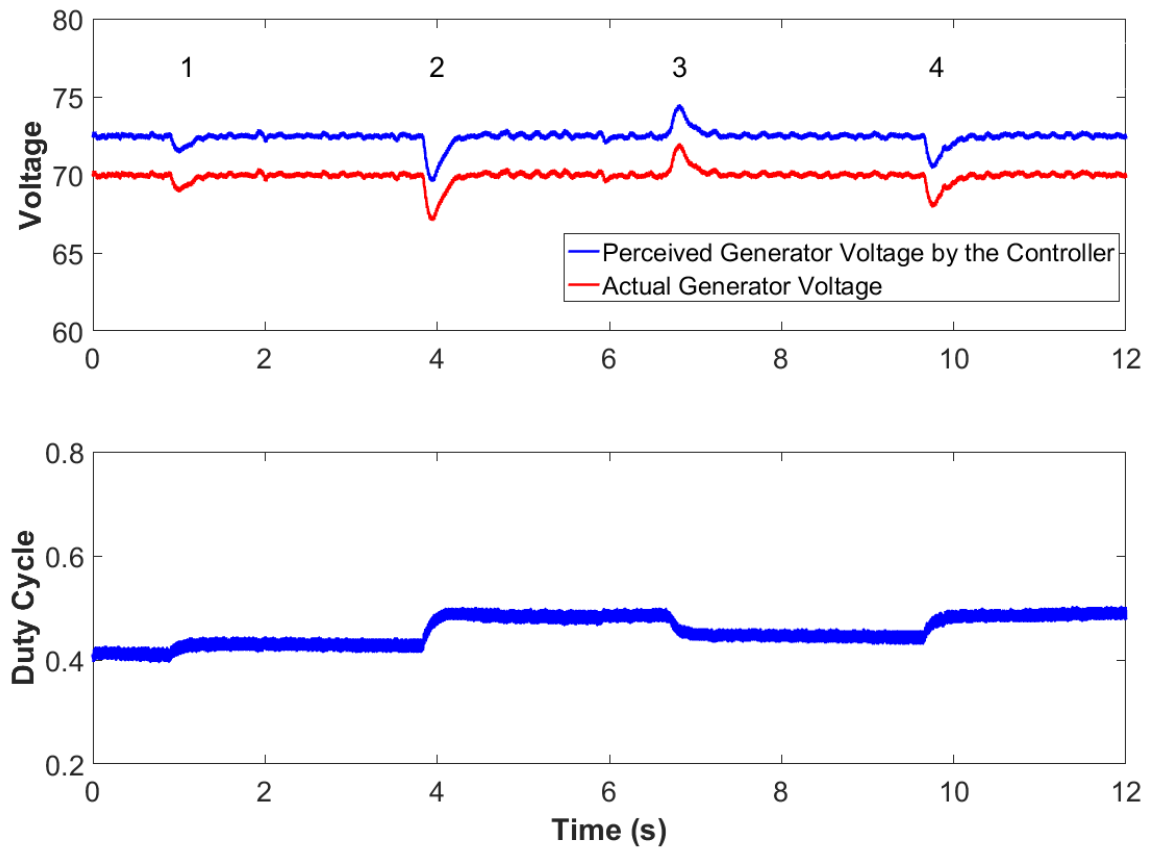


FIGURE 5.5: Constant Bias Attack

As the intruder injects a bias in the sensor data, the generator terminal voltage increases so that the PI controller reduces the IGBT duty cycle. The controller maintains the IGBT duty cycle based on the (false) sensor data it receives so that there is a difference between the actual generator voltage and the false generator voltage. The difference between the two voltages is exactly equal to the bias induced by the attacker. In an actual power system, if the load voltage drops below a certain threshold, the circuit breaker trips the load.

5.2.2 Ramp Bias Attack

In Figure 5.6, we consider a data attack in which the intruder injects a linearly increasing bias into the voltage data packets. For this experiment, it is assumed that the bias voltage increases according to the equation $V_{\text{bias}} = t$, i.e. 1 volt drop per second. Thus, as time increases, the bias data injected by the intruder also increases which leads the controller to correspondingly decrease the IGBT duty cycle. The controller falsely believes that the generator terminal voltage is being maintained at the desired constant level, while in fact it keeps decreasing. In an industrial setting, the generator will be shut down by the under voltage relay.

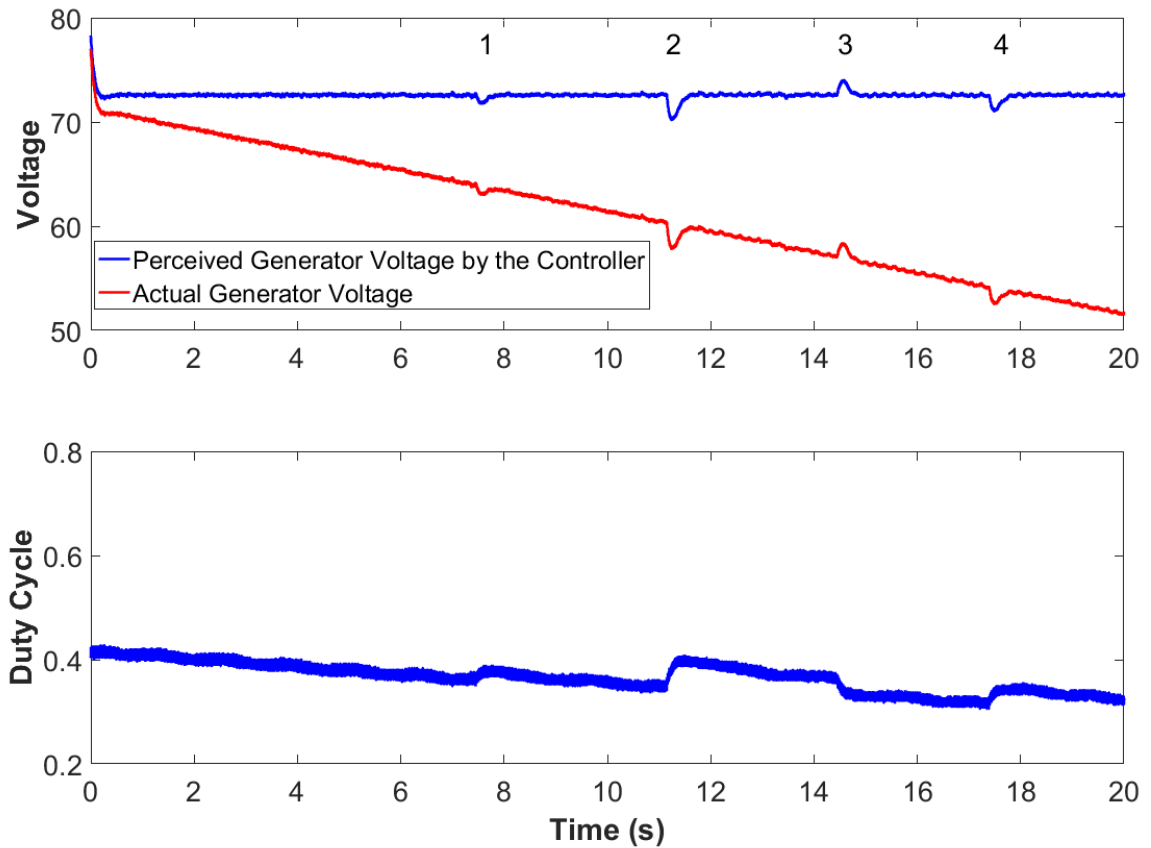


FIGURE 5.6: Ramp Bias Attack

5.2.3 Random Data Injection

Figure 5.7 shows a random data injection attack in which the intruder adds a random number to the sensor data packets. In this attack however, V_{bias} is a uniform random number between -10V and 10V. This sets the controls into large variations in the duty cycle and the corresponding changes in the generator terminal voltage. Note again that while actual terminal voltage of the generator varies randomly, the controller has no way of knowing the actual scenario as the controller receives sensor data that has been manipulated by the attacker.

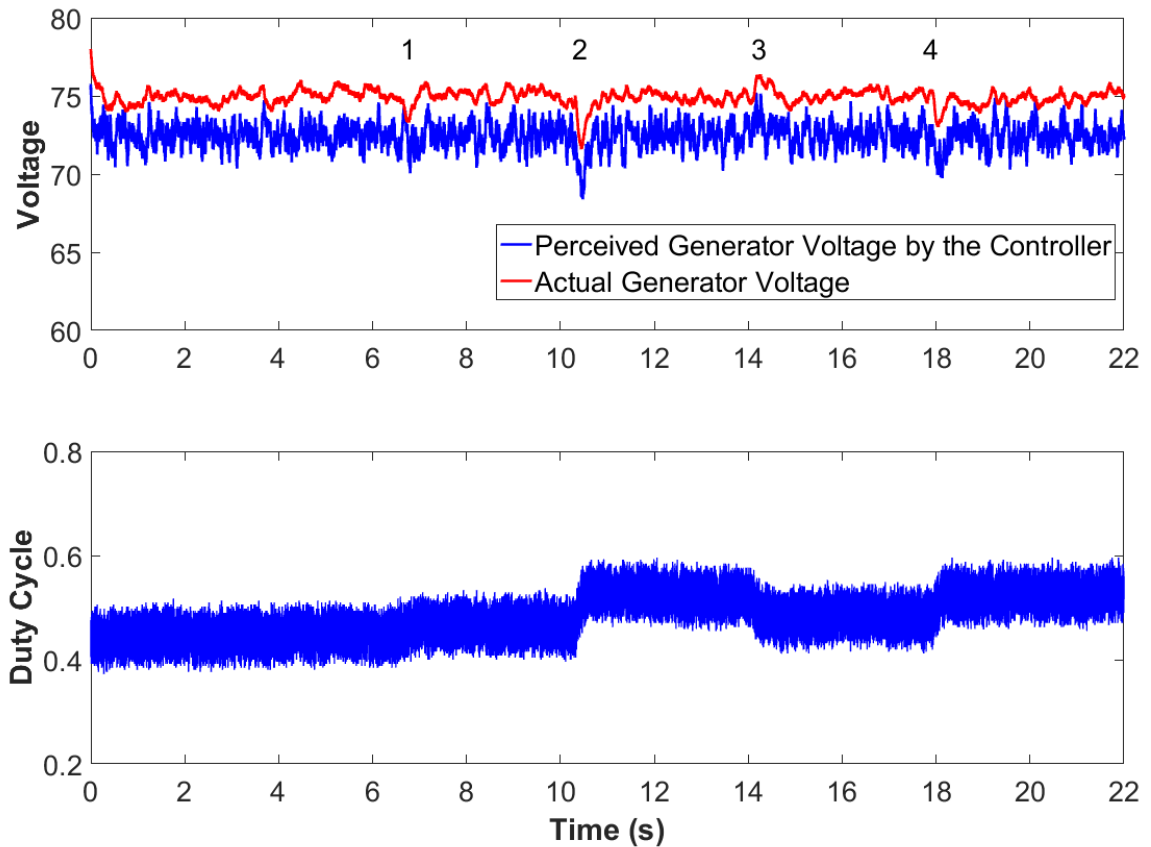


FIGURE 5.7: Random Bias Attack

5.2.4 DoS Attack

Next we investigate the effects of the denial-of-service attack in the sensor data transmission. Data packets in transition from the sensor to the controller were dropped according to an independent and identically distributed Bernoulli process [32, 35]; the packet dropout probability was assumed to be 0.98. This research uses UDP protocol for data transmission so that a lost data packet is not retransmitted. Instead it was assumed that the controller holds the last received sensor data and uses it to replace the lost packet. Figure 5.8 shows noisy response of the generator due to Bernoulli packet drops. It has been shown that the closed loop system maintains stability in the mean square sense if the packet drop probability is below a certain threshold.

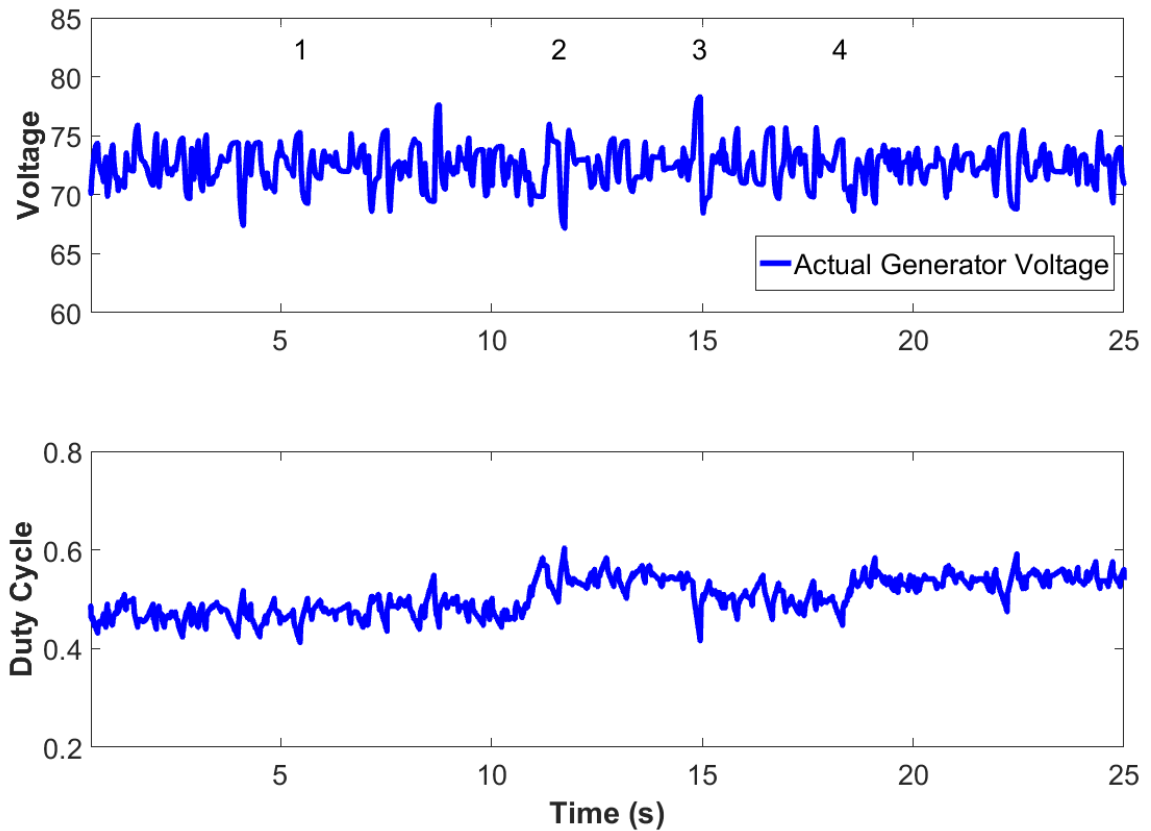


FIGURE 5.8: DoS Attack

5.3 DoS Attack on 3-Bus System

This section presents experimental results of a (simulated) DoS attack on the PV bus generator excitation control system. The Denial-of-service attack usually causes congestion in the network causing data packet drops, which affects the feedback control system. In this experiment, DoS attack was simulated at the software level; because of network security issues, an institutional permission was not feasible to allow actual DoS attacks on the excitation system. Data packets in transition from the sensor to the controller were dropped according to a Bernoulli process; the packet dropout probability was a variable parameter for experimentation. This research utilizes the idea behind the UDP protocol for data transmission so that the simulated lost data packet is not retransmitted. Instead it was assumed that the controller holds the last successfully received sensor data and uses it to replace the lost packet. Figures 5.9-5.12 show the response of the three-bus system due to five different values of packet drop probabilities of Bernoulli packet drops of PV bus generator control loop.

For each packet drop probability β , the PQ bus loads were switched sequentially, first switching ON/OFF of a resistive load, then an inductive load followed by a capacitive load. As expected, switching of a resistive load causes a drop in load bus voltage, an inductive load causes a larger drop, and capacitive load causes an increase of voltage as shown in Figure 5.9. Note also that the slack bus voltage (middle window) and the PV bus voltage (top window) are held relatively constant by the excitation system controller except for short switching event transients. The top window of Figure 5.9 shows the effects of packet drop on the PV bus voltage; the PV bus voltage becomes noisier with increasing levels of packet drop. Overall, the system remained stable for packet drop probabilities below a certain threshold.

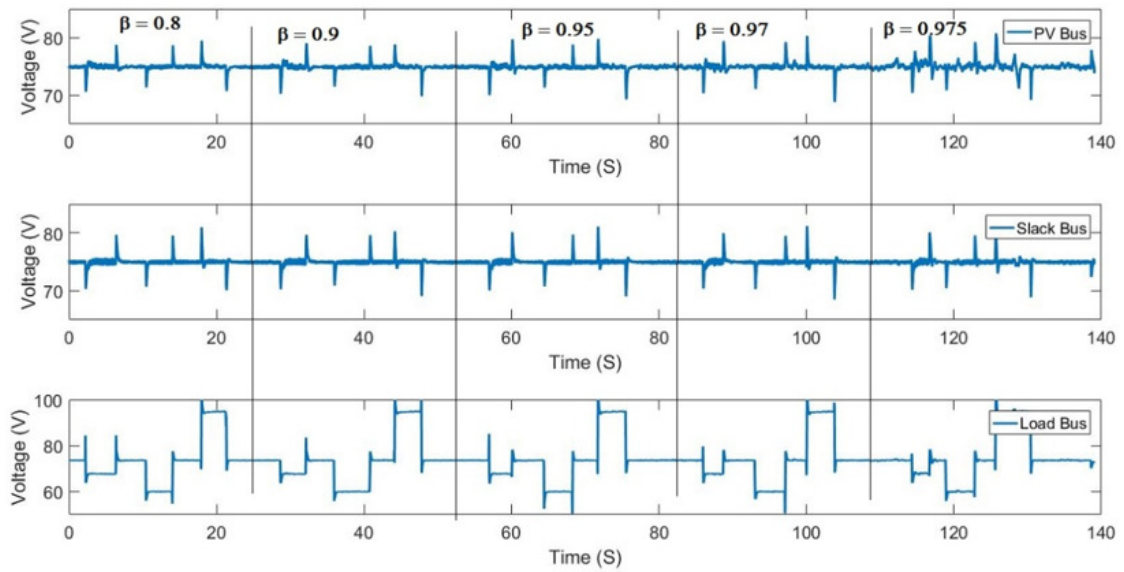


FIGURE 5.9: Bus Voltages (DoS Attack on PV Bus Generator)

Figure 5.10 shows the corresponding current injections at the various buses. The load bus current varies with load as seen from the bottom window of Figure 5.10. Clearly, current injection at the PV bus (top window) is expected to remain constant since this generator supplies a constant power; transient variations are however observed during load switching. The slack bus generator supplies additional current as the load changes as shown in the middle window. Figure 5.11 shows the duty cycle ratio for different values of packet drop probability, which also shows increased sharp variations in duty ratio when the packet drop probability is high.

Variations in PV bus generator current also imply an imbalance between its prime mover input and electrical output which sets the generator into oscillations. This can be observed in Figure 5.12. Because of the fast sampling rate of the system, overall the system remained stable even when the packet drop probability was 0.975, which depends on the sampling time of the controller.

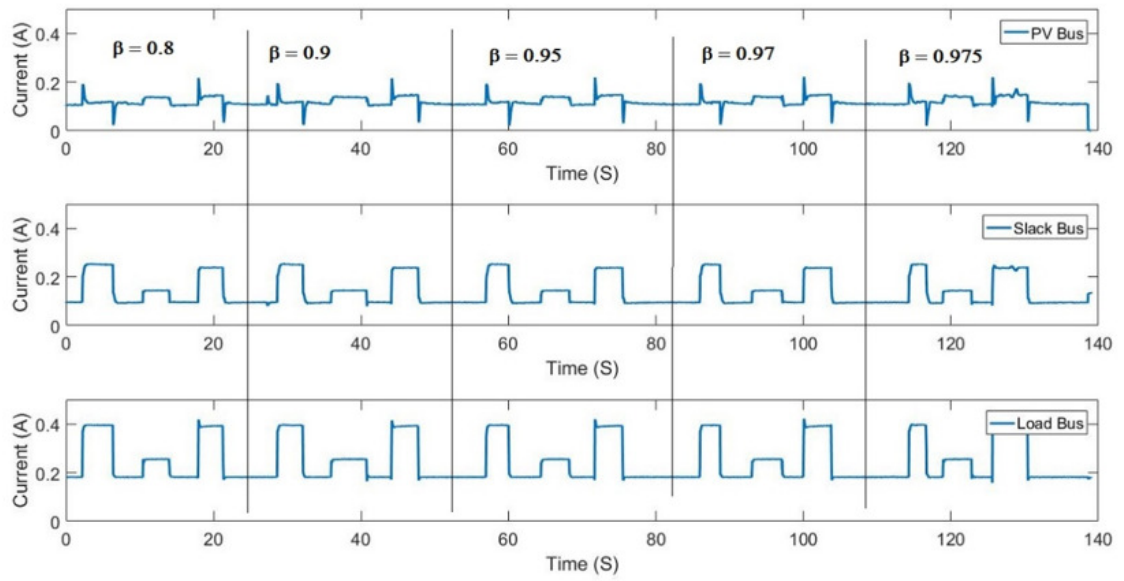


FIGURE 5.10: Bus Current (PV Bus)(DoS Attack)

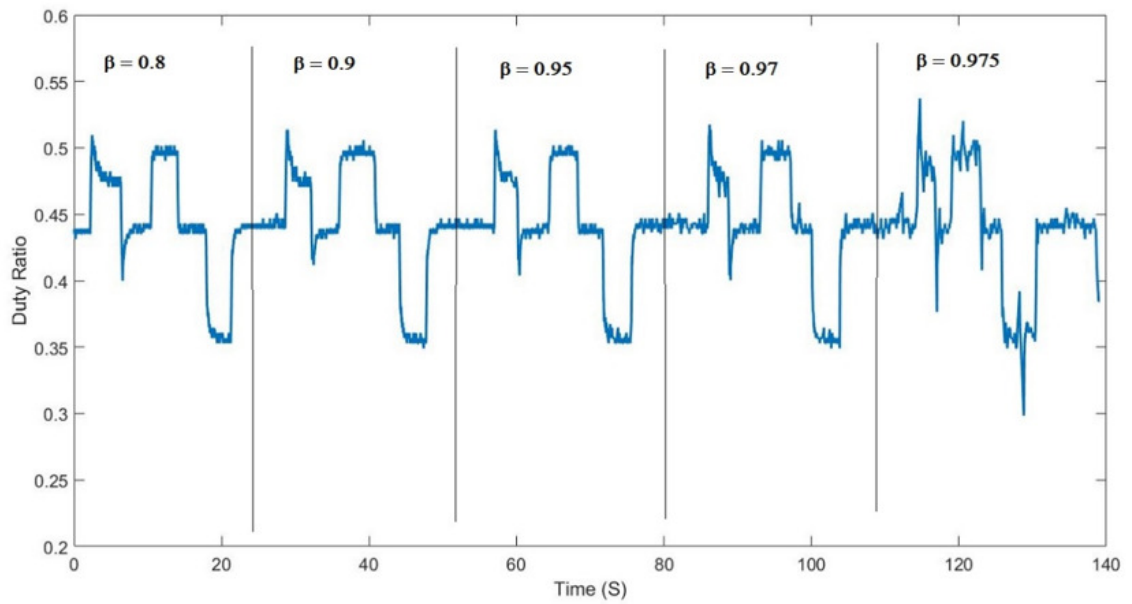


FIGURE 5.11: Duty Cycle Ratio (DoS Attack)

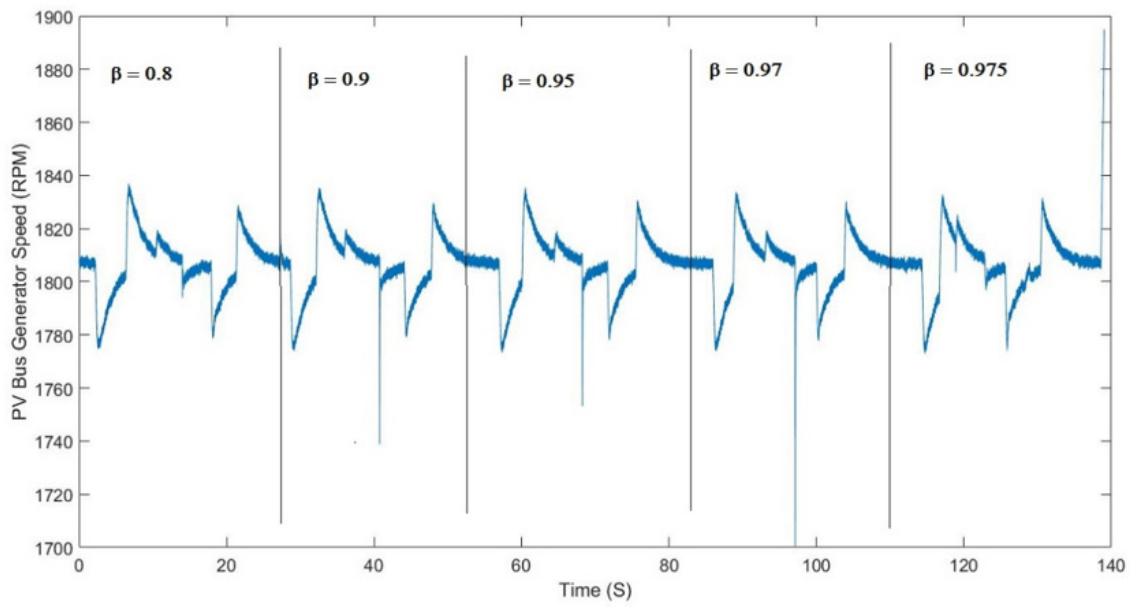


FIGURE 5.12: Generator Speed (PV Bus)(DoS Attack)

This chapter considered cyberattacks only on the sensor network. The developed HIL network could also be used to apply other types of cyberattacks, such as attacks on the generator control system that change gains in the controller.

Chapter 6

CONCLUSION

6.1 Summary

In this research, we have developed a novel HIL experimental platform of a 3-bus power system consisting of two generators and a load. Cyberattacks, specifically DoS attacks and false data injection attacks, were successfully simulated at the software level on the HIL platform to show the degradation in performance of the system.

The fundamentals of power system stability theory were discussed. First, the single machine infinite bus was described. The basics of the prime mover dynamics of the synchronous generator were described. The design and methodology of the synchronous generator excitation circuit were outlined. Ultimately, this led to the swing equation which was also described in detail w.r.t. how it pertains to determining the stability of a generator.

The background for the HIL 3-bus system that can be used for observing and evaluating cyberattacks on a real physical microgrid was outlined. The specific hardware used and implemented were mentioned. The generator's physical

parameters that were utilized in the experimental setup were found experimentally and the process of which was described in detail.

The basic mathematical framework for the modeling and control of multibus power systems was reviewed. With the aforementioned mathematical framework, the 3-bus system of the interest was simulated. A simulated fault was administered on the system to demonstrate the transient response of the system with the controller and the potential implications of it.

On the experimental side, first baseline experiments were conducted to validate functionality of the controllers and the entire system under normal operating conditions. The load switching caused the terminal voltage of the two generators to change which was corrected by the IGBT duty cycle computed by their individual controllers.

Four experiments were done on a 2-bus generator system. First, a constant bias attack in which the intruder injects a constant bias to the generator voltage data packets was administered. The results showed that the attack was successful and in a real life condition the generator would have had an undervoltage trip. Second experiment was a ramp bias attack in which the intruder injects a linearly increasing bias into the voltage data packets and thus decreasing the actual output voltage of the generator. This, too, would result in an undervoltage trip under real life operating conditions. Third experiment, a random data injection attack in which the intruder adds a random number to the sensor data packets was administered. This resulted in unpredictable fluctuations in the generator's output voltage. Fourth experiment, The DoS attack in which data packets in transition from the sensor to the controller were dropped according to an independent and identically distributed Bernoulli process with a packet dropout probability of 0.98 was done. With the packet loss of 0.98, the generator voltage varied, but maintained stability.

A final (simulated) DoS attack experiment was investigated on the HIL 3-bus system. The setup was a slack bus, PV bus, and a load bus with a controller and data acquisition system. The attack was performed on the PV bus controller's received sensor data. The system was tested with the same load switching profile over the course of the experiment. The probability β of packet loss was 0.8, 0.9, 0.95, 0.97, and 0.975 respectively for each of the load switching events. The system random stable throughout and only really getting somewhat garbled at the probability of 0.975, but still remained in an acceptable limit.

Denial-of-service attacks were launched on the defenseless system to prove the functionality of the controller and the ability to successfully maintain stability of the system under cyberattacks. The results demonstrate the impacts of cyberattacks on the microgrid and its stability. The platform can be used in senior level courses on power systems as a laboratory demonstration tool to show the impacts of cyberattacks, albeit simulated, on a real physical microgrid. This HIL setup could also be used as an experimental platform for research to evaluate cyber countermeasures capable of defending or preventing harm to the power grid.

6.2 Future Research

Future research could be conducted by extending the HIL platform to a WCCC 9-bus system. The extension to a 9-bus system will allow one to further analyze the effects cyberattacks on a larger networked power system. This research was only concerned with the effects cyberattacks had on one generator and how that affected the rest of the 3-bus system. Experiments on the 9-bus system will allow one to examine how cyberattacks on multiple generator control systems affect the overall system as well as other generators in the same grid. This research involving the design and analysis of the 3-bus NCS due to packet drop could also be extended in other directions, such as packet delays, loss of transmission line

or a large load center, controller alterations by changing gains, etc. Research on cyberattacks that include both packet drop and delays would also be important. This research was concerned with only a PI controller and a state space controller based on the linearized system model. Future research could include other types of controllers including controllers based on actual nonlinear system dynamics. In addition, this research uses manually switched loads and could be improved by creating an automatic controller to improve switching event accuracy as well as providing different avenues for cyberattacks or by producing physical faults in the system.

Bibliography

- [1] E. J. Markey and Henry A. Waxman. *Electric Grid Vulnerability: Industry Responses Reveal Security Gaps*. U.S. House of Representatives, Washington, DC, 2013.
- [2] B. Wingfield. Power-grid cyber attack seen leaving millions in dark for months, 2012. <http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html>.
- [3] R. Rantala. *Cybercrimes Against Businesses*. Bureau of Justice Statistics, 2008.
- [4] S. Baker, S. Waterman, and G. Ivanov. *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. McAfee, Santa Clara, California, 2009.
- [5] A. Lipovsky and A. Cherepanov. Blackenergy trojan strikes again: Attacks ukrainian electric power industry. 2016. <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry>.
- [6] Wall Street Journal. U.S. risks national blackout from small-scale attack. 2014.
- [7] US General Accounting Office. Critical infrastructure protection: Challenges in securing control systems. 2003. URL <http://www.gao.gov/new.items/d04140t.pdf>.
- [8] R. Nicholson. Critical infrastructure cybersecurity: Survey findings and analysis. *Energy Insights*, 2008.

- [9] L. Tinnel, O. Saydjari, and D. Farrell. Cyberwar strategy and tactics: An analysis of cyber goals, strategies, tactics and techniques. *Proceedings of the IEEE SMC Workshop on Information Assurance*, pages 228–234, 2002.
- [10] US Government Accountability Office. Protection of chemical and water infrastructure: Federal requirements, actions of selected facilities and remaining challenges. *Report No. GAO-05-327*, 2005.
- [11] A. Sanjab and W. Saad. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective. *IEEE Transactions on Smart Grid*, 7(4):2038–2049, July 2016. ISSN 1949-3061. doi: 10.1109/TSG.2016.2550218.
- [12] Liu Y., Ning P., and Reiter M. False data injection attacks against state estimation in electric power grids. In *ACM Trans on Information and System Security*, volume 14, 2011.
- [13] Sridhar S. and Manimaran G. Data integrity attacks and their impacts on scada control system. In *IEEE Power and Energy Society General Meeting*, 2010.
- [14] Giani A., Bitar E., Garcia M., McQueen M., Khargonekar P., and Poola K. Smart grid data integrity attacks. In *IEEE Trans on Smart Grid*, pages 1–11, 2012.
- [15] S. Biswas and A. Sarwat. Vulnerabilities in two-area automatic generation control systems under cyberattack. In *2016 Resilience Week (RWS)*, pages 40–45, Aug 2016. doi: 10.1109/RWEEK.2016.7573304.
- [16] Esfahani P.M., Vrakopoulou M, Margellos K., Lygeros J., and Goran Andersson. A robust policy for automatic generation control attack in two area power network. In *IEEE Conference on Decision and Control*, 2010.
- [17] Chabukswar R, Mo Y, and Sinopoli B. Detecting data integrity attacks on scada systems. In *18th IFAC World Congress*, Aug 2011.
- [18] A. Rege, F. Ferrese, S. Biswas, and L. Bai. Adversary dynamics and smart grid security: A multiagent system approach. In *2014 7th International Symposium on Resilient Control Systems (ISRCS)*, pages 1–7, Aug 2014. doi: 10.1109/ISRCS.2014.6900101.

- [19] Timothy R. McJunkin, Craig G. Rieger, Brian K. Johnson, D. Subbaram Naidu P. E., Lawrence H. Beaty, Indrajit Ray, Katya L. Le Blanc, and Michael Guryan. Interdisciplinary education through edutainment: Electric grid resilient control systems course, 6 2015.
- [20] M. Sloderbeck, C. Edrington, and M. Steurer. Hardware-in-the-loop experiments with a simulated electric ship power system utilizing a 5 mw variable voltage source converter amplifier. In *2009 IEEE International Electric Machines and Drives Conference*, pages 1167–1172, May 2009. doi: 10.1109/IEMDC.2009.5075351.
- [21] S-T. Cha, P. I. Kwon, Q. Wu, A. H. Nielsen, and J. stergaard. Real-time hardware-in-the-loop testing for digital controllers. In *IEEE PES Asia-Pacific Power and Energy Engineering Conference IEEE*, 2012. doi: <https://doi.org/10.1109/APPEEC.2012.6307219>.
- [22] M. S. Almas, L. Vanfretti, and L. Vanfretti. Experimental performance assessment of a generator’s excitation control system using real-time hardware-in-the-loop simulation. In *IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society*, pages 3756–3762, Oct 2014. doi: 10.1109/IECON.2014.7049059.
- [23] J. Jung. Power hardware-in-the-loop simulation (PHILS) of photovoltaic power generation using real-time simulation techniques and power interfaces. *J. Power Sour.*, 285(7/1):137145, 2015.
- [24] Y. Zhou, J. Lin, Y. Song, Y. Cai, and H. Liu. A power hardware-in-loop based testing bed for auxiliary active power control of wind power plants. *Electr. Power Syst. Res.*, 124(7):1017, 2015.
- [25] M. Milosevic, P. Prempraneerach, J.L. Kirtley, G. Karniadakis, and C. Chrysostomidis. An end-to-end simulator for the all-electric ship mvdc integrated power system. In *Proceedings of the Grand Challenges in Modeling and Simulation (GCMS10)*, 2010.
- [26] R. Brandl, M. Calin, and T. Degner. Power hardware-in-the-loop setup for power system stability analyses. *CIREN - Open Access Proceedings Journal*, 2017(1):387–390, 2017. ISSN 2515-0855. doi: 10.1049/oap-cired.2017.1100.
- [27] X. Wu, S. Lentijo, and A. Monti. A novel interface for power-hardware-in-the-loop simulation. In *2004 IEEE Workshop on*

- Computers in Power Electronics, 2004. Proceedings.*, pages 178–182, Aug 2004. doi: 10.1109/CIPE.2004.1428147.
- [28] G. F. Lauss, M. O. Faruque, K. Schoder, C. Dufour, A. Viehweider, and J. Langston. Characteristics and design of power hardware-in-the-loop simulations for electrical power systems. *IEEE Transactions on Industrial Electronics*, 63(1):406–417, Jan 2016. ISSN 1557-9948. doi: 10.1109/TIE.2015.2464308.
- [29] S. Paran, T. V. Vu, F. Franco, and C. S. Edrington. Evaluation of the interface accuracy for power hardware-in-the-loop experiments. *Journal of Electric Power Components and Systems*, 45:763–773, 2017.
- [30] James D Kollmer, Robert Irwin, Saroj Biswas, Walid Saad, Arif Sarwat, and Li Bai. Development of an experimental platform for analysis of cyberattacks on power grid. In *2017 ASEE Annual Conference and Exposition*, June 2017.
- [31] James D Kollmer, Saroj K Biswas, Li Bai, Arif I. Sarwat, and Walid Saad. A hardware-in-the-loop experimental platform for power grid security. In *2018 ASEE Annual Conference & Exposition*, Salt Lake City, Utah, June 2018. ASEE Conferences. <https://peer.asee.org/29689>.
- [32] Robert Irwin, James D Kollmer, Saroj Biswas, and Li Bai. An investigation of cyber attacks on a power system. In *2017 Intelligent Ships Symposium*, June 2017.
- [33] Ned Mohan. *Electric Power Systems: A first Course*. Wiley, first edition, 2012.
- [34] Turan Gonen. *Electrical Machines with MATLAB*. CRC Press, second edition, 2012.
- [35] B. Niemoczynski, S. Biswas, and J. Kollmer. Stability of discrete-time networked control systems under denial of service attacks. In *2016 Resilience Week (RWS)*, pages 119–124, 2016.