Potential Cyber-Attack Detection and Mitigation Techniques for MTDC VSC HVDC Systems

A Thesis

Presented in Partial Fulfilment 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

Jessica Hatton

Major Professor: Brian K. Johnson, Ph.D.

Committee Members: Herbert L. Hess, Ph.D.; Dakota Roberson, Ph.D.

Department Administrator: Joseph D. Law, Ph.D.

August 2018

Authorization to Submit Thesis

This thesis of Jessica Hatton, submitted for the degree of Master of Science with a major in Electrical Engineering and titled "Potential Cyber-Attack Detection and Mitigation Techniques for MTDC VSC HVDC Systems," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____Date_____
Brian K. Johnson, Ph.D.

Committee Members: _____Date_____
Herbert L. Hess, Ph.D.

_____Date_____
Dakota Roberson, Ph.D.

Department Administrator: _____Date_____
Joseph D. Law, Ph.D.

Abstract

In this thesis, point-to-point VSC HVDC transmission system and multiterminal VSC HVDC transmission system simulation models are developed in an electromagnetic transients program. This thesis explains the controls for the system and the calculations necessary to build a simulation model for each type of system.

This thesis also discusses potential cyber-attack detection strategies and develops potential responses to detected cyber-attacks on multiterminal VSC HVDC transmisison systems. The cyber-attacks that are discussed are combinations of spoofed AC voltage, AC current, AC real power, DC power, and DC voltage measurements. The detection of these spoofed signals is achieved by comparing calculations using other measured signals for the system.

A possible alternative method for detecting types of cyber-attacks that were performed is also discussed. This method involves using the saturation of the modulating functions of the controllers and unexpected values for the measurement signals from the system. Possible control actions to take when an attack is detected are also introduced and discussed.

Acknowledgements

I would like to thank my adviser, Dr. Johnson, for his commitment to the instruction of his students, me in particular. Due to his dedication to his students, I was able to receive the education needed for a large majority of the courses for my master's degree. My thesis would also not be possible without his advice and direction during my research.

I would like to thank Dr. Hess for the time and input given on my thesis. I would like to thank Dr. Roberson for his help with my research and well as the contribution given on my thesis. I would also like to thank Dr. Nuqui at ABB Inc. for his feedback throughout this research.

I would like to thank my parents for their advice and encouragement that they have given me throughout my education. Finally I would like to thank and my husband, Trey, for his constant support and encouragement. I would not have been able to complete my degree without him.

Table of Contents

List of Tables

List of Figures

Acronyms

AC Alternating Current

DC Direct Current

HVDC High Voltage Direct Current

LLC Line Commutated Converter

MMC Modular Multilevel Converter

MTDC Multiterminal Direct Current

NPC Neutral Point Converter

PWM Pulse-Width Modulation

VSC Voltage Source Converter

CHAPTER 1

Introduction

While most power transmission lines are AC, there are applications where it is cost effective to use DC. These lines are called High Voltage Direct Current (HVDC) lines for transmission applications. These lines are able to transmit power longer distances or connect AC systems that are out of synchronization. HVDC controls are able to quickly regulate power. They give the benefit of being able to supply a commanded amount of power, unlike AC transmission lines which depend upon the voltage magnitudes and phase angle differences between surrounding buses. While HVDC systems have benefits, they operate based off of measurements and communication which can be vulnerable to cyber-attacks. This thesis will discuss the design of the simulation models, develop and test methods to detect the cyber-attacks on multiterminal HVDC transmission systems, along with potential responses to cyber-attacks.

1.1 Background Information

The vast majority of transmission lines in the world are AC transmission lines [1]. The main reason for this is the transformer. Transformers are devices used to change the voltage and current levels by a turns ratio. If the voltage is stepped up (increased by the turns ratio), then the current would be stepped down (decreased by the turns ratio). An ideal transformer has equal real and reactive power on both sides. While ideal transformers do not exist in real life, the power losses resulting from the transformer are small when compared to power transmission losses when voltages are not stepped up to high levels for transmission. As previously stated, when the voltage is stepped up, the current is stepped down, which results in lower transmission power losses because power losses follow (1.1).

$$P = |I|^2 R \tag{1.1}$$

Due to the fact that transformers require a time varying magnetic field, almost all transmission lines are AC. In order for DC transmission lines to be efficient, a transformer is first used to step the AC voltage up. The AC is then converted to DC using a power converter and transmitted along the dc line and converted back to ac at the other end.

There are two main types of DC to AC converters used for high voltage power transmission. One uses thyristor based line commutated current source converters (LCC) and the other is based on self commutated voltage source converters, which is called VSC HVDC transmission. This research will focus on the latter converter technology.

One of the applications of HVDC transmission is that it can be used to transmit power over longer distances. HVDC transmission lines are able to transmit more power over longer distances than AC lines because the electric and magnetic fields for DC lines only need to be charged once while AC lines charge twice every cycle. The charging current for these lines increase as line length increases. The charging current can be so large for underground cables, for example, that it is almost at the current limit of the line, which severely limits the amount of power that can be transferred. For DC lines, a capacitance behaves as an open circuit in steady-state. This allows a DC line to operate in steady-state without a charging current once the line is charged to operational level, allowing the DC line to transmit current up to the thermal rating of the line. Long overhead AC transmission lines can have voltage stability issues and require dynamic reactive compensation. Dynamic reactive compensators can be expensive and HVDC becomes more cost effective than the dynamic reactive compensators after about 600-800 km [2].

Another reason that HVDC lines are able to transfer more power is DC lines

don't have skin effect like AC lines. The higher the frequency, the more skin effect there is, and since DC lines have a frequency of zero, the current is evenly distributed throughout the entire cable [3]. So for a given cable thickness, DC lines would be able to transfer somewhat more power with lower losses than would be the case for a 60 Hz cable. DC transmission lines also only transmit real power while AC transmission lines transmit real and reactive power. So for the same real power transmitted, DC transmission lines would need smaller cables. DC lines also need less right of way because they require two cables as opposed to the three required for AC systems. Since AC systems consist of three phases, at least three conductors are needed, while DC transmission lines only need two. Since DC transmission needs two conductors and AC transmission needs three, DC transmission systems require less right of way. This makes them less expensive, while more power is also able to be transferred on fewer number of cables due to a combination of the effects discussed here.

1.2 HVDC Technology Applications

HVDC technology can be used in many different situations, where it is cost effective. The main applications of this technology are:

- "long distance, large-scale power transfer;
- subsea and long-distance [underground] cable-power transmission;
- interconnecting asynchronous AC systems or systems with different frequencies;
- controllable power transfer between different nodes in an electricity market or markets;
- AC grid stability support, ancillary service provision and resilience to blackouts;
- Connecting isolated systems like offshore windfarms or oil platforms." [2]

As previously stated, HVDC transmission can be used when longer lines are needed, which is approximately longer than 40-70 km for underwater cables and 600-800 km for overhead lines [4]. Underwater cables have a larger capacitance and less inductance than overhead AC cables, making the distance that AC power can be transmitted without compensation very limited. DC is competitive over AC for undersea cables when the cable length is between 40-70 km and longer [2]. At this distance the cost of the HVDC converters can be justified since the cost for compensation for AC cables is very expensive. An example of this is a 580 km HVDC cable between Norway and the Netherlands [2].

For overhead lines the distance where the cost of the converter is justified is much longer. There are many cases where a shorter HVDC line can be justified for cases such as right of way limitations, stability issues, and for connection of asynchronous systems, to name a few.

Overhead lines have a smaller capacitance and more inductance than underground or underwater lines making the charging current smaller and the distance where DC lines are typically used are between 600-800 km or longer [2]. A good example of this type of HVDC line is a "1360 km, 3.1 GW, +/- 500 kV Pacific DC intertie along the west coast of the United States" [2].

1.3 Voltage Sourced Converters

VSCs represent a class of topologies for AC to DC power conversion. The type of VSC that was modeled in the electromagnetic transients program for the HVDC systems simulated in this thesis was a two-level VSC, which is shown in Figure 1.1 [5]. The basic results developed here will apply for other VSC topologies too, such as the modular multilevel converter (MMC) and the neutral point clamped converter (NPC) [4]. The MMC is a converter where each transitor in the two level VSC shown in Figure 1.1 is replaced with a large number of single phase converter modules connected

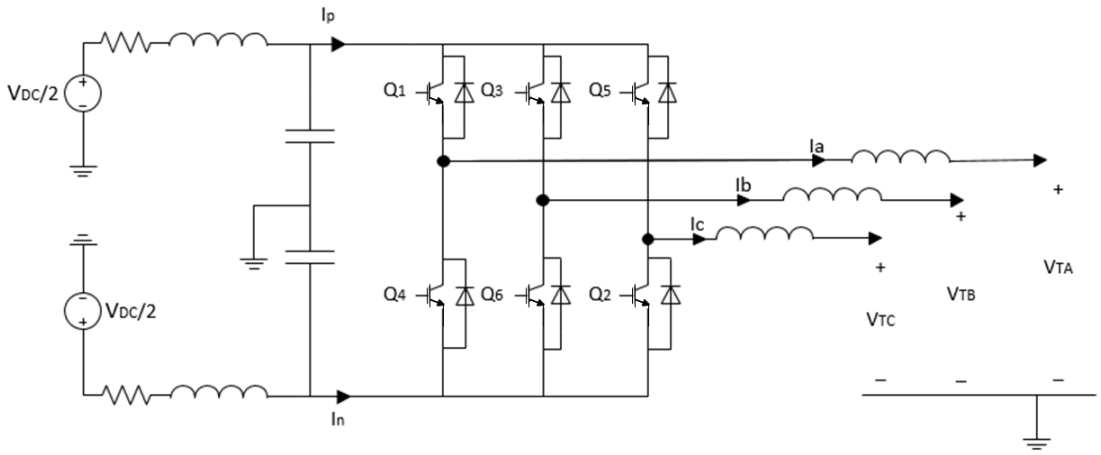

Figure 1.1: Two Level VSC

in series with the voltage divided between the series modules, reducing switching losses. This type of converter is often used when a single switch cannot handle the voltage or current requirements [4]. The NPC is a three level converter where each cell shown in Figure 1.1 is a group of switches simpler than in the MMC, and the DC voltage is divided across two capacitors that have a 0 V potential difference between them, which results in each cell only needing to be rated for half of the DC voltage [5].

A VSC supports bidirectional power flow between the AC and DC systems. The direction of power flow on the DC side is controlled by reversing direction of the DC current while maintaining the polarity of the DC voltage [5]. This is achieved by modulating functions that control the operation of the switches. A pulse-width modulation (PWM) scheme is used in a two-level VSC, but the modulation function can also control the timing of switching in a MMC as well.

The simulation cases in this thesis use state-space averaged models for the VSC because the results of interest for this project are steady-state results and cases with slow dynamic responses. The state space averaged model is shown in Figure 1.2 [5].

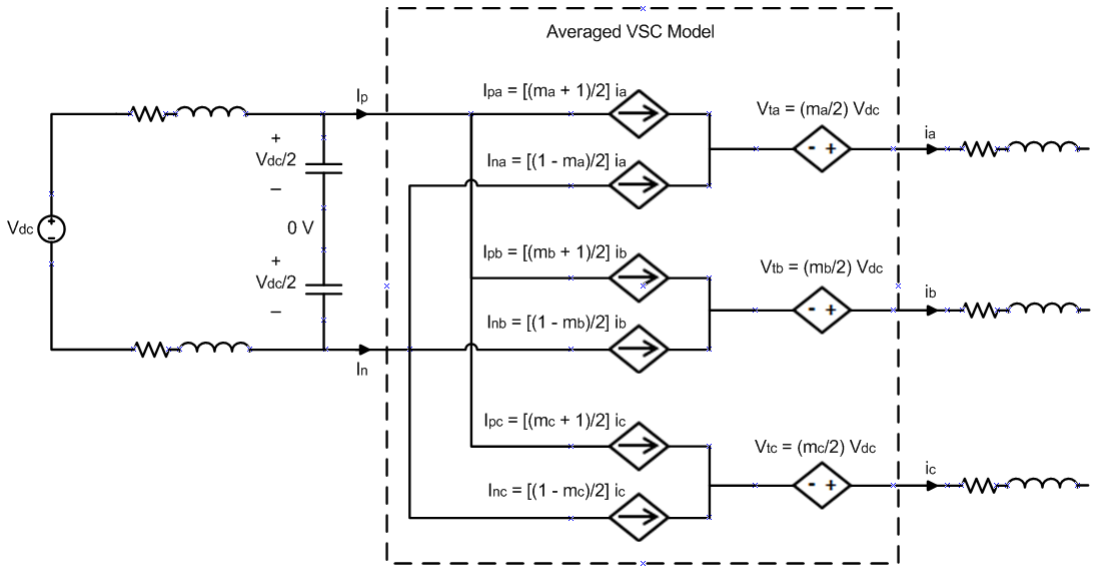

Figure 1.2: Averaged Model of VSC

The averaged model exhibits the same steady-state behavior and low frequency dynamic response that the switching model would produce. The averaged model does not produce the high frequency components that are in the actual converter and represented in the switching model. In addition, the averaged model does not implement the details of the PWM. Instead, the AC and DC outputs of the converter are low frequency dynamic functions of the modulating signals [4].

1.4 Cyber-Attacks on Power Systems

While there has not been much research into the detection of cyber-attacks on HVDC systems, there has been research done on cyber-attacks of AC systems through the supervisory control and data acquisition (SCADA) system [6] [7]. A paper titled *SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy* provides an introduction and discusses abnormalities in signals received [8]. A specific class of intrusion method discussed in the paper is called "anomaly detection." This

method discusses using anomalies in the observed data to detect if something unusual is happening on the system in order to detect an attack [8]. This thesis uses detection methods very similar to the detection methods introduced in [8].

The second chapter in this thesis will focus on the construction of a simplified simulation model for point-to-point VSC HVDC transmission systems. The design of the system and normal operation with be discussed. The third chapter will discuss multiterminal VSC HVDC transmission systems. The model used for this system will be introduced as well as results for normal operation for the system. The fourth chapter will discuss the detection of cyber-attacks on the multiterminal VSC HVDC transmission system introduced in Chapter 3. The fifth chapter will show preliminary results for applying the detection methods of Chapter 4 to a CIGRE benchmark DC system. Chapter 6 introduces detection methods based on monitoring control signals. That chapter will discuss how the modulating signals and other measurement signals can be used to detect attacks. Chapter 7 will introduce potential responses to the detection of a cyber-attack. It is important to note that the environment in which the simulations are performed has no significant measurement noise. In a practical system noise will provide additional challenges for detecting cyber-attacks.

CHAPTER 2

Development and Testing of a Point-to-Point VSC HVDC Transmission Model

2.1 Control of Point-to-Point VSC Transmission System

The end goal for this project is to test schemes to detect and mitigate against cyber-attacks on multiterminal VSC HVDC transmission systems. As a step toward achieving that goal, a point-to-point VSC HVDC transmission system is developed to help solidify modeling and control concepts.

A point-to-point VSC HVDC transmission system has two VSCs connected by a HVDC line. A diagram of a point-to-point VSC HVDC transmission system connecting two AC grids is shown in Figure 2.1. A DC circuit model using a state space averaged model appropriate for this simulation model for the system is shown in Figure 2.2. For this simulation model, the capacitors have been set at an initial charge of $V_{dcref} = 4500$ V.

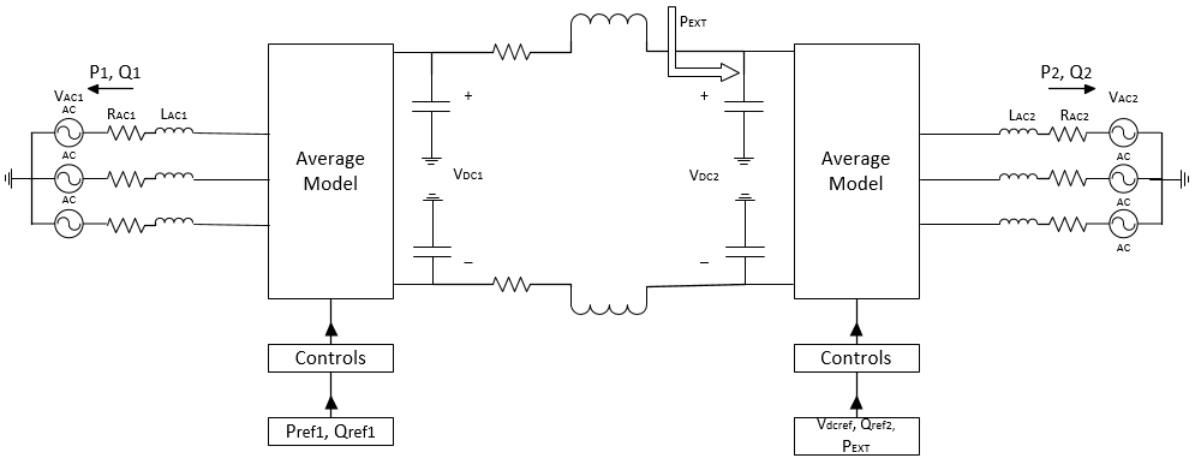

Figure 2.1: Point-to-Point VSC HVDC Transmission System [9]

The outer level control inputs for a point-to-point VSC HVDC system are P_{ref1}, Q_{ref1}, Q_{ref2}, and V_{dcref}. The other references needed for control of the system are cal-

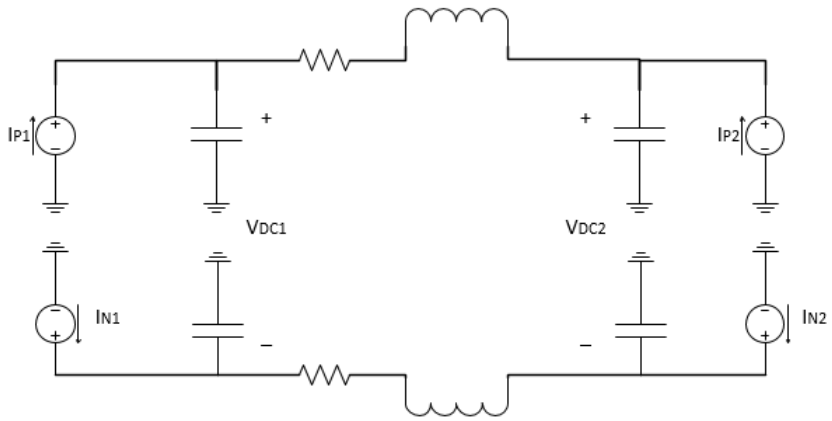

Figure 2.2: System Modeled in ATPdraw

culated from these four inputs and/or from system parameters such as AC impedance or DC capacitance.

For the case in Figure 2.1, the power on the DC system is flowing from converter one to converter two. Based on Figure 2.1, the power flowing into AC grid 1 is P_1, would be a negative number, and P_2, the power flowing into AC grid 2 is a positive number. The VSC inner control loops use measurements and set points transformed using the Parks transformation in (2.1) to operate in a two-axis synchronous reference frame [5]. The real power reference is used to determine I_{dref}, the d axis component of I_{abc} in the synchronous reference frame, and the reactive power reference is used to determine I_{qref}, the q axis component of I_{abc} in the synchronous reference frame. The power reference for converter two must be calculated based on system quantities to avoid an overdetermined system. P_{ref2} is calculated by a loop that regulates V_{dc2}, which is measured on the system, and compared to V_{dcref}, which is an input to the system. When $V_{dc2} = V_{dcref}$, converter two is equal to the power injection from converter one minus DC losses. If $V_{dc2} > V_{dcref}$ then converter two is transferring less power than converter one is injecting with the excess energy charging the capacitor and increasing the voltage. The error between V_{dc2} and V_{dcref} is put through a transfer function to compute P_{ref2} [9]. The transfer function used in this simulation is based

on the equation for energy stored in a capacitor since the error between V_{dc}^2 and V_{dcref}^2 was used. The error signal input to the PI controller can either be the error between V_{dc} and V_{dcref} or it can be the error between V_{dc}^2 and V_{dcref}^2 depending on design preference, however using the squared terms gives linearity with the power input commands. P_{ref2} should be equal to the negative of P_{ref1} minus the losses in the line. In this simulation, the error between V_{dc}^2 and V_{dcref}^2 is used in the DC bus voltage regulator and is shown in Figure 2.3. The transfer function used in Figure 2.3 is derived in Yazdani [9].

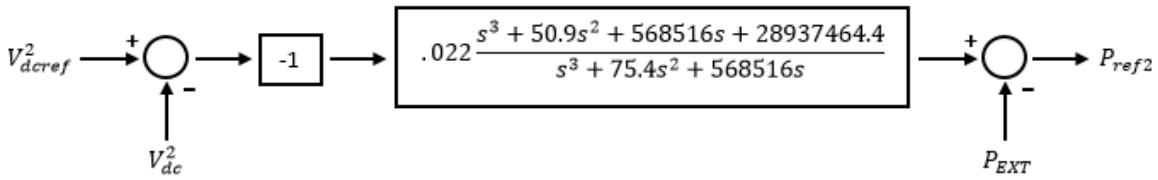

Figure 2.3: P_{ref2} Calculation from V_{dc}^2 and V_{dcref}^2

After P_{ref2} is computed, I_{d1ref}, I_{q1ref}, I_{d2ref}, and I_{q2ref} are computed from P_{ref1}, P_{ref2}, Q_{ref1}, and Q_{ref2}. I_{dref} and I_{qref} are computed in the synchronous reference frame instead of the stationary I_{abc} is because signals in the dq frame are constant values in steady-state, making it easier to design a control system based on PI controllers. Equations (2.2) and (2.3) are used to calculate I_{dref} and I_{qref} [9]. These equations are derived from the equations for real and reactive power shown in (2.4) and (2.5). The synchronizing reference is chosen such that V_q is equal to 0. The transformation to determine elements in the dq frame from the abc frame is shown in (2.1) [5]. Once that is substituted and the equations are rearranged, the result is (2.2) and (2.3) [9].

$$\begin{bmatrix} x_d \\ x_q \\ x_0 \end{bmatrix} = \frac{2}{3} \begin{bmatrix} cos(\omega_r t) & cos(\omega_r t - \frac{2\pi}{3}) & cos(\omega_r t - \frac{4\pi}{3}) \\ -sin(\omega_r t) & -sin(\omega_r t - \frac{2\pi}{3}) & -sin(\omega_r t - \frac{4\pi}{3}) \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \times \begin{bmatrix} x_a \\ x_b \\ x_c \end{bmatrix} \tag{2.1}$$

$$I_{dref} = \frac{2}{3V_d} P_{ref} \tag{2.2}$$

$$I_{qref} = \frac{-2}{3V_d} Q_{ref} \tag{2.3}$$

$$P = \frac{3}{2}(V_d I_d + V_q I_q) \tag{2.4}$$

$$Q = \frac{3}{2}(-V_d I_q + V_q I_d) \tag{2.5}$$

Equation (2.2) is implemented as part of Figure 2.4, which is the current regulator for I_d. After the reference value for I_d is calculated from (2.2), a PI regulator determines a d-axis modulating function, M_d, to provide control of I_d. The PI constants, k_p and k_i, are calculated based upon (2.6) and (2.7) respectively. One approach for determining the control gains for the PI regulator is to cancel the open loop pole at $\frac{-R_{AC}}{L_{AC}}$ associated with the circuit impedance between the converter terminal and the point of interconnect [4]. Equations (2.6) and (2.7) account for the resistance and inductance as well as setting a desired time constant for the current regulator response. The current regulator time constant, τ_i, is typically in the range of 0.5-5 ms [4] [10]. The regulator time constant was set at 5 ms since a faster response is not necessary for this application. The impedance of both of the AC systems was .0096 Ω and .384 mH in this example. The output of the PI controller is then summed

with a feed forward component. In the same junction, a component used to cancel the cross-coupling between the d an q axes is subtracted from that summation. The output of that junction is then divided by $\frac{V_{dc}}{2}$ to put the signal into per unit, thus limiting M_d between positive and negative one.

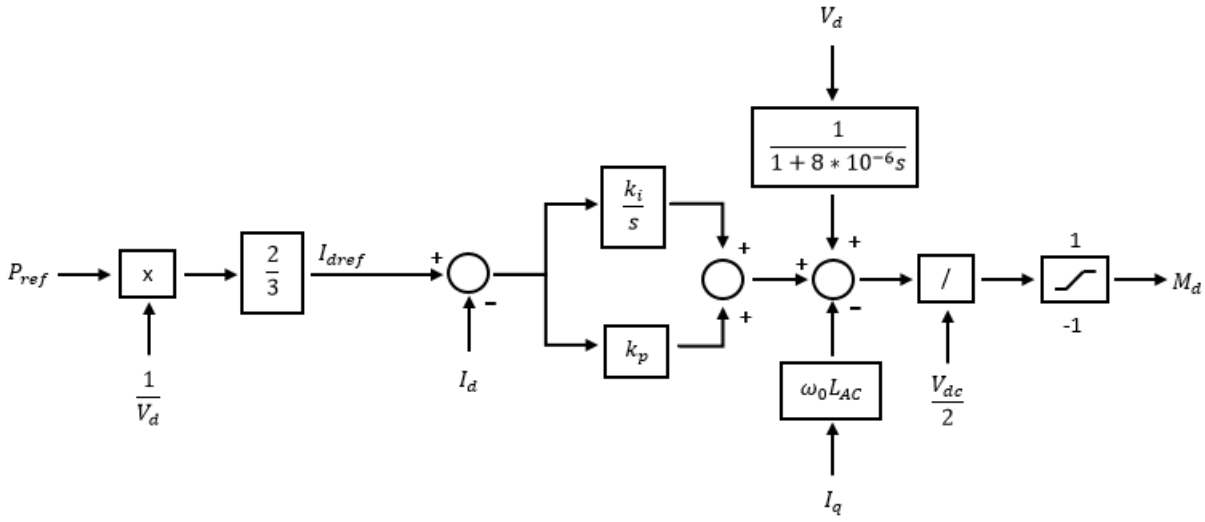

Figure 2.4: Current Regulator for I_d

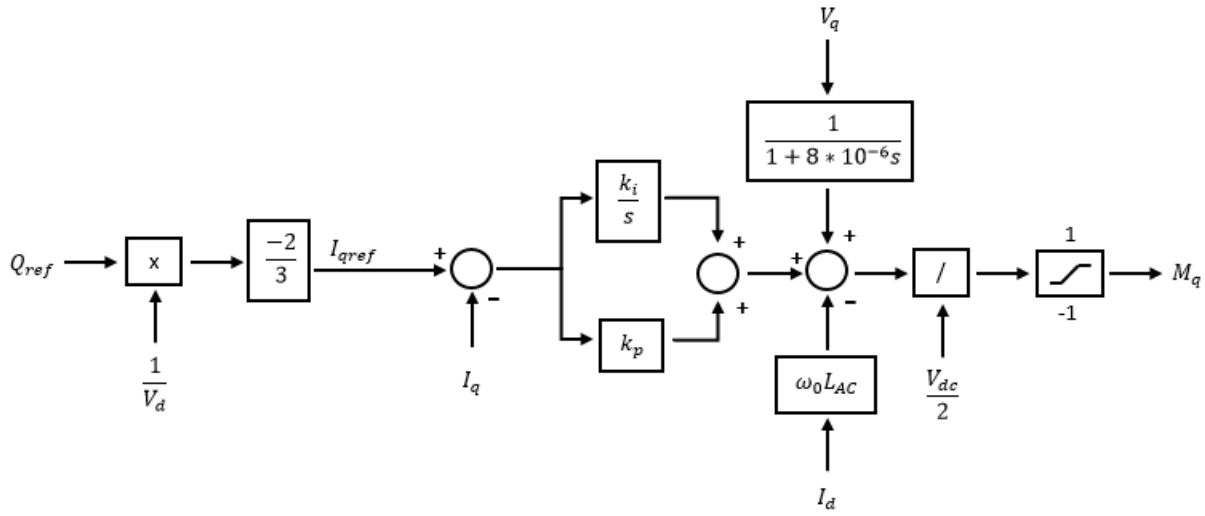

Figure 2.5: Current Regulator for I_q

$$k_p = \frac{L_{AC}}{\tau_i} \tag{2.6}$$

$$k_i = \frac{R_{AC}}{\tau_i} \tag{2.7}$$

The current regulator for I_q looks very similar to the current regulator for I_d, and is shown in Figure 2.5. The current regulator for I_q has the same PI constants as the the current regulator for I_d. The current regulator for I_q also contains a feed forward component and a decoupling term. However, in this case the feed forward component is in the q axis and the decoupling term is in the d axis. The current regulation for I_d and I_q for each converter would use each system's individual inputs. Converter one would have inputs of P_{ref} and Q_{ref}. It would also have its own measurements for V_d, V_q, I_d, I_q, and V_{dc}. The PI constants for converter one, k_p and k_i, would be based off of the impedance to the point of interconnect for converter one. Converter two would have the inputs V_{dcref} and Q_{ref}. Converter two would also have its own measurements for V_d, V_q, I_d, I_q, and V_{dc}. The PI constants for converter two, k_p and k_i, would be based on the impedance that is between the point of interconnect and the converter terminals for converter two.

The outputs for the controllers are the modulating functions, M_d and M_q, which are limited to between positive and negative one. M_d and M_q are then transformed back into the stationary abc frame. For simulation purposes, they are used to calculate the current injected on the DC system and the voltage on the AC side of the VSC using the state-space modeling approach. In the process of transforming M_d and M_q, they are first transformed into the stationary $\alpha\beta$ reference frame using (2.8) and (2.9). Then the α and β components are converted to the abc frame using (2.10) through (2.12) which are Blondel's transformation. While this can be done in one step, two steps were used in the simulation.

$$M_{alpha} = M_d cos(\omega_r t) - M_q sin(\omega_r t) \tag{2.8}$$

$$M_{beta} = M_q cos(\omega_r t) + M_d sin(\omega_r t) \tag{2.9}$$

$$M_a = M_{alpha} \tag{2.10}$$

$$M_b = \frac{\sqrt{3}M_{beta} - M_{alpha}}{2} \tag{2.11}$$

$$M_c = \frac{\sqrt{3}M_{beta} + M_{alpha}}{2} \tag{2.12}$$

Once the modulating functions are put into the abc reference frame, they are then used to determine state-space averaged converter model parameters. The values directly impacted by M_d and M_q are the converter terminal AC voltage and the DC current injected into the DC system from the converter. The DC currents injected into the DC system, as shown in Figure 2.2, are I_P and I_N for the positive and negative poles respectively. Equations (2.13) through (2.23) show how $V_{T_{ABC}}$, I_P, and I_N are related to by M_{abc}.

$$V_{T_A}(t) = \frac{M_a V_{dc}}{2} \tag{2.13}$$

$$V_{T_B}(t) = \frac{M_b V_{dc}}{2} \tag{2.14}$$

$$V_{T_C}(t) = \frac{M_c V_{dc}}{2} \tag{2.15}$$

$$I_{P_A} = \frac{1 + M_a}{2} I_{AC_a}(t) \tag{2.16}$$

$$I_{P_B} = \frac{1 + M_b}{2} I_{AC_b}(t) \tag{2.17}$$

$$I_{P_C} = \frac{1 + M_c}{2} I_{AC_c}(t) \tag{2.18}$$

$$I_P = I_{P_A} + I_{P_B} + I_{P_C} \tag{2.19}$$

$$I_{N_A} = \frac{1 - M_a}{2} I_{AC_A} \tag{2.20}$$

$$I_{N_B} = \frac{1 - M_b}{2} I_{AC_B} \tag{2.21}$$

$$I_{N_C} = \frac{1 - M_c}{2} I_{AC_C} \tag{2.22}$$

$$I_N = I_{N_A} + I_{N_B} + I_{N_C} \tag{2.23}$$

The currents I_P and I_N are the same currents that are shown in the average model that are flowing on the DC lines in Figure 2.2. I_{P1}, the positive pole DC current from converter one, would be the sum of I_{P1_A}, I_{P1_B}, and I_{P1_C}. I_{N1} is the sum of I_{N1_A}, I_{N1_B}, and I_{N1_C}, where I_{N1_A}, I_{N1_B}, and I_{N1_C} are all instantaneous currents. I_{P1} and I_{N1} are the current injections from the averaged model of converter one. I_{P2} and I_{N2} are the current injections from the averaged model of converter two. This is shown in Figure 2.2. The calculation of I_{P2} and I_{N2}, which is similar to the calculation of I_{P1} and I_{N1}, is shown in (2.19) and (2.23).

This section has outlined equations behind the basic operation of a point-to-point VSC HVDC transmission system model. To gain a better understanding of the actual operation of the system and to demonstrate that the equations stated sufficiently capture the dynamics of interest, a model of a point-to-point VSC HVDC system was built in an electromagnetic transients program and the reference tracking of the current regulators are shown in the next section of this thesis.

2.2 Electromagnetic Transients Program Simulation Results of Point-to-Point VSC Transmission System

To demonstrate that the controls perform as expected, a simulation model is built in an electromagnetic transients program. To demonstrate expected performance the plots of the currents for each converter in the dq frame, I_d and I_q, will be shown tracking their reference. The nominal DC voltage for this system is 4500 V. The DC voltage setting is low due to the fact that the AC voltage at the point of interconnect in this initial model is 1.8 kV_{LL}. P_{ref1} is a step function set to an initial value of -100 W to a final value of -50 W. P_{ref2} was calculated from the difference between V_{dc}^2 and V_{dcref}^2. Q_{ref1} and Q_{ref2} were also varied. Q_{ref1} is a step function from an initial value of 50 VARs to a value of 250 VARS after 0.8 seconds have elapsed in the simulation. Then at 0.9 seconds, the reference is changed by a negative 200 VARs. Q_{ref2} is a step function from an initial value of 25 VARs to a value of -175 VARs after 0.9 seconds have elapsed in the simulation. Since P_{ref} is used to calculate I_{dref} and Q_{ref} is used to calculated I_{qref}, only the plots showing the actual values and references for I_{d1ref}, I_{q1ref}, I_{d2ref}, and I_{q2ref} will be shown in Figures 2.6 through 2.9.

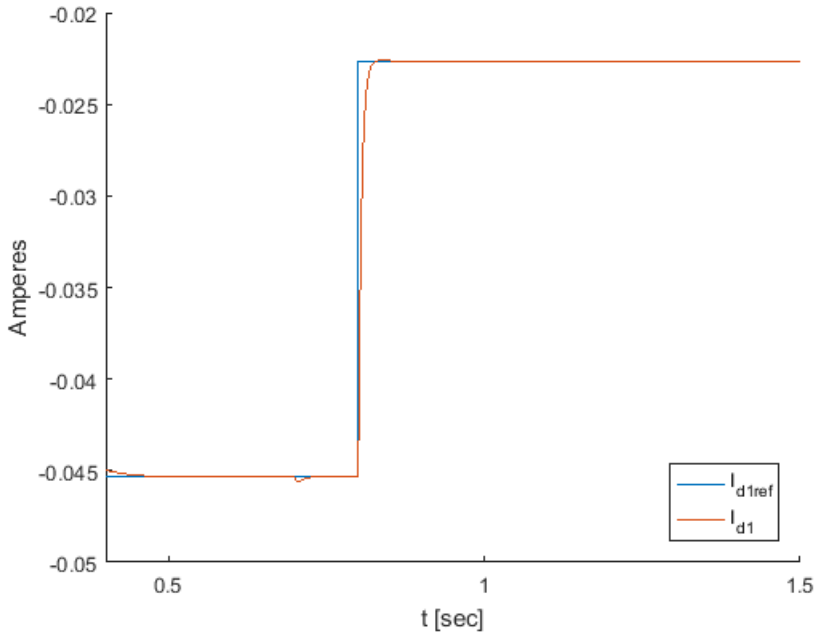

Figure 2.6: I_{d1ref} and I_{d1}

The simulation has a large start up transient at the beginning. Since the start up behavior is not of interest in this work, the time scale in Figure 2.6 starts after the start up transient has largely died down. When I_{d1ref} steps up, it can be seen that I_{d1} has a very good response because it is tracking the reference very closely. The values are very close, showing the effectiveness of the control loop. As shown, the change in Q_{ref} for converter one has no effect on P_{ref1}, which means there is not an effect on I_{d1ref}. There is a small amount of coupling between the d and q axes which can be seen in the I_d1 measurement in Figure 2.6 between 0.5 and 1 second.

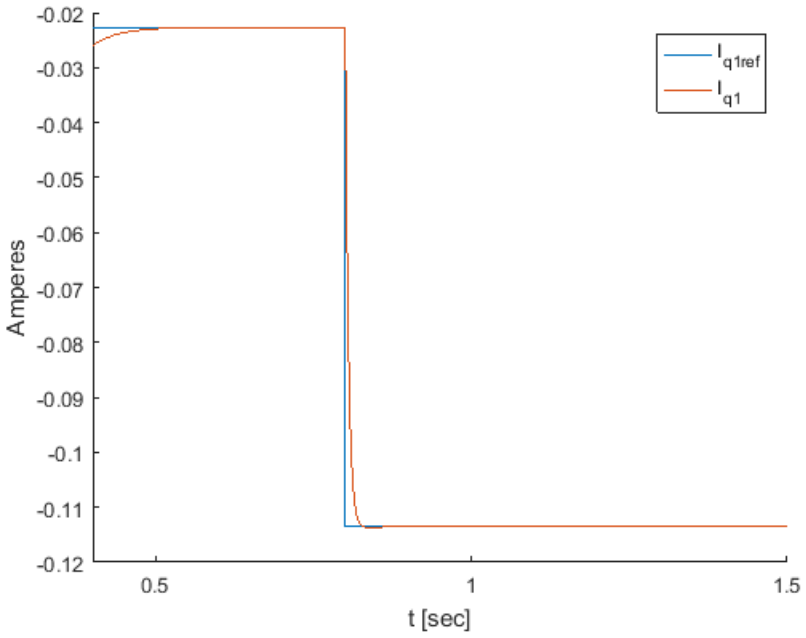

Figure 2.7: I_{q1ref} and I_{q1}

Similar to the plot in Figure 2.6, the time window in Figure 2.7 was shifted to not show the start up transient. The change in I_{q1ref} that can be seen is a result from the change in Q_{ref1}. The measurements show that the values for I_{q1} and I_{q1ref} are very close, which means that the control loop is operating as expected. There is also no visible response between changes in I_{q1} from changes in I_{q2ref}, showing that the reactive power response of the two converters are independent of each other. This figure also shows that there is no change in I_{q1} when I_{d1} responds to a change in reference.

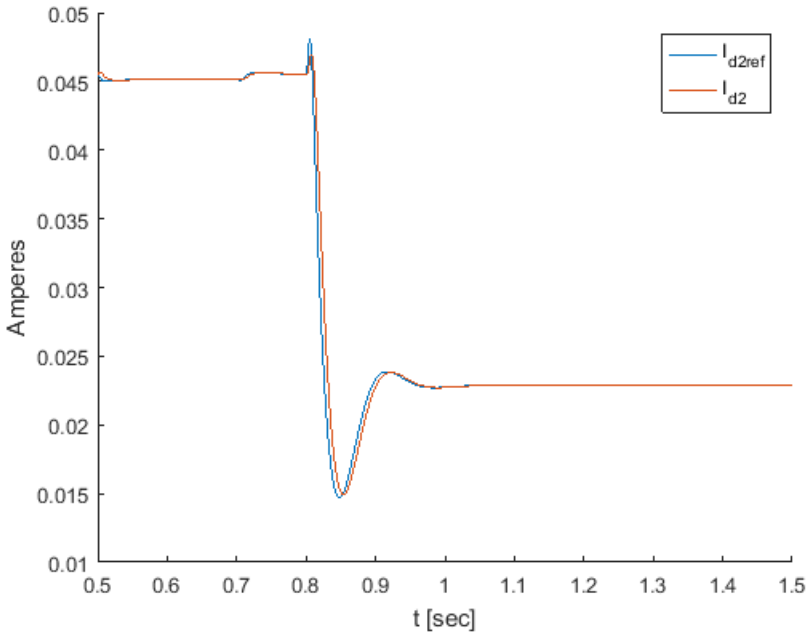

Figure 2.8: I_{d2ref} and I_{d2}

Similar to the plots in Figures 2.6 and 2.7, the time window in Figure 2.8 is shifted to not show the start up transient. The change in I_{d2ref} that can be seen is a result from the change in P_{ref2}. It can be seen from the figure that I_{d2} and I_{d2ref} are very close, which means that the control loop is operating as expected.

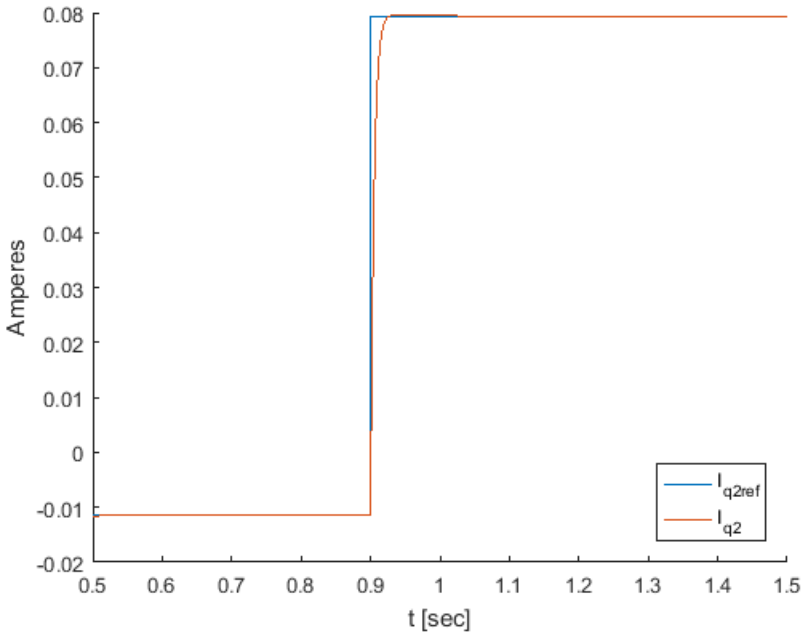

Figure 2.9: I_{q2ref} and I_{q2}

Similar to the plots in Figures 2.6, the time window in Figure 2.9 is shifted to not show the start up transient. The change in I_{q2ref} that can be seen is a result from the change in Q_{ref2}. The measurements show that the values for I_{q2} and I_{q2ref} are very close, which means that the control loop is operating as expected. As with Figure 2.7, there is no visible response between changes in I_{q2} from changes in I_{q1ref}. This indicates that I_{q1} and I_{q2} for the two converters are independent of each other.

Figures 2.6 through 2.9 demonstrate that the simulation is working as expected and has a response that is sufficiently fast and appropriately free of significant steady-state error for the system response to changes in real and reactive power. In practice, the AC system may not be able to respond to sudden changes in the power references and the commands may need to be ramped up or down instead of the step functions that were demonstrated.

CHAPTER 3

Multiterminal HVDC VSC Transmission Model

A multiterminal VSC HVDC transmission system is designed as a testbed for cyber-attack studies and modeled in ATP using the control schemes in *Voltage-Sourced Converters in Power Systems: Modeling, Control, and Applications* by Yazdani and Iravani and *High Voltage Direct Current Transmission: Converters, System and DC Grids* by Jovcic and Kahled [2] [5].

The multiterminal VSC HVDC transmission system, which was modeled in an electromagnetic transients program, has four VSCs connected by HVDC lines. Each VSC is connected to an isolated AC grid. A diagram of the transmission system modeled is shown in Figure 3.1.

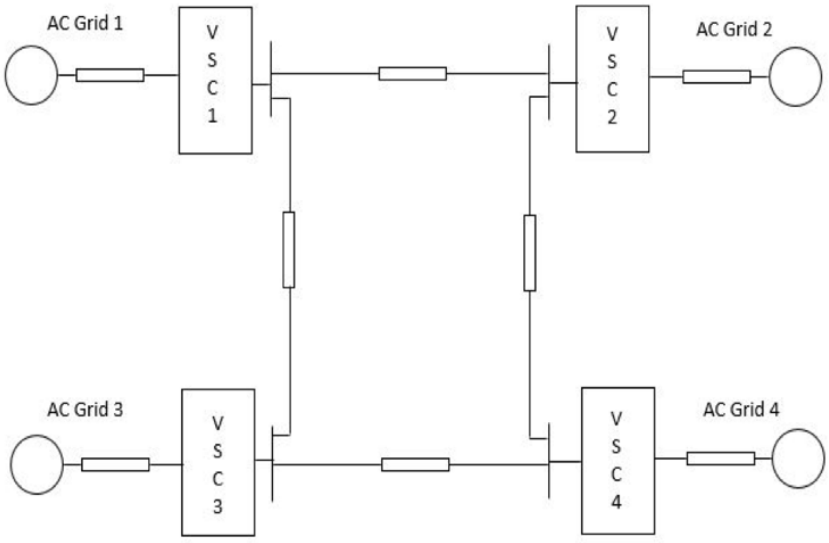

Figure 3.1: Diagram of modeled multiterminal VSC HVDC transmission system

The parameters for the system are chosen starting from desired voltage and power ratings. The power limits for each converter were chosen first. The power rating chosen for each converter was set at 900 MW. The nominal AC voltage for each converter was chosen to be 180 kV line-to-line. Equation (3.1) was used to determine the AC

equivalent impedance, where the short circuit MVA, MVA_{SC}, of each converter was set at five times its rating, and that the X over R ratio for each AC system is set at 10. This resulted in $Z_{pu} = \frac{1}{45}$, $R_{AC} = 0.716\ \Omega$, and $L_{AC} \approx 19$ mH for each converter with $V_{pu} = 1.0$ for rated operation.

$$MVA_{SC} = \frac{V_{pu}^2}{Z_{pu}} \tag{3.1}$$

Using an AC voltage of 180 kV line-to-line as the voltage base and 100 MVA as the power base, the impedance base was approximately 324 Ω. Then the AC system impedance is calculated using the X over R ratio. Since the power limit and AC voltage are the same for each converter and AC system, all of the AC impedances were the same. The impedance for the DC system was chosen arbitrarily as this would be determined by the type of conductor and the length of the line. The DC impedance of the system affects the power losses of the DC system. If the power losses on the DC system plus the power demanded from the converters that are acting as inverters is greater than the power that rectifiers are supplying, the DC voltage at the converters that are acting as rectifiers will drop. To account for these losses, the voltage of each converter is monitored. Since the DC voltage is monitored for those converters, the DC voltage controllers at those converters will cause them to supply more power to the DC system to bring the DC voltage back up to an acceptable level. The resistances chosen for the DC lines for each pole are either 7 Ω or 10 Ω. The DC resistances are shown in Table 3.1 where R_{12} is the DC resistance between the positive poles of converters one and two and between the negative poles of converters one and two. It is similar for the other DC resistances and inductances listed.

DC Resistance and Inductance Label	Resistance or Inductance
R_{12}	7 Ω
R_{13}	10 Ω
R_{24}	10 Ω
R_{34}	10 Ω
L_{12}	5 mH
L_{13}	5 mH
L_{24}	5 mH
L_{34}	5 mH

Table 3.1: Table of DC Resistances and Inductance between each pole of the VSC

3.1 Multiterminal VSC HVDC Transmission System Control

The inputs for each converter in the multiterminal VSC HVDC system are P_{ref}, Q_{ref}, and V_{dcref}. The other references needed for control of the system are calculated from these three inputs or from system parameters and measurements such as impedance or current measurements.

The power on the system is capable of flowing bidirectionally between each of the converters as each converter can be set up to receive or transmit power. The references needed to control the DC power are scheduled in advance and are set from the control center. In this case the control center is emulated with fixed commands. In this simulation a positive power command means that the power is flowing into the AC grid and is acting as an inverter. The power reference determines how I_{dref} is controlled, which ultimately controls the real power flow between the AC and DC systems at that converter.

If the converter is acting as a rectifier, it is controlled using DC voltage. If the converter is acting as an inverter, its primary form of control is via a power reference.

The inverter control changes such that the I_{dref} control for an inverter is switched to be controlled a voltage reference if the voltage goes outside of a set threshold, which is between 0.9 pu and 1.1 pu. The controls circuits determine whether the real power is controlled via a voltage reference or power reference are shown in Figures 3.2 and 3.3. If $I_{d_{voltage}} = 1$, then the converter is controlled using a voltage reference. If $I_{d_{power}} = 1$, then the converter is controlled using a power reference. If both are the unit value one at the same time, an error is thrown.

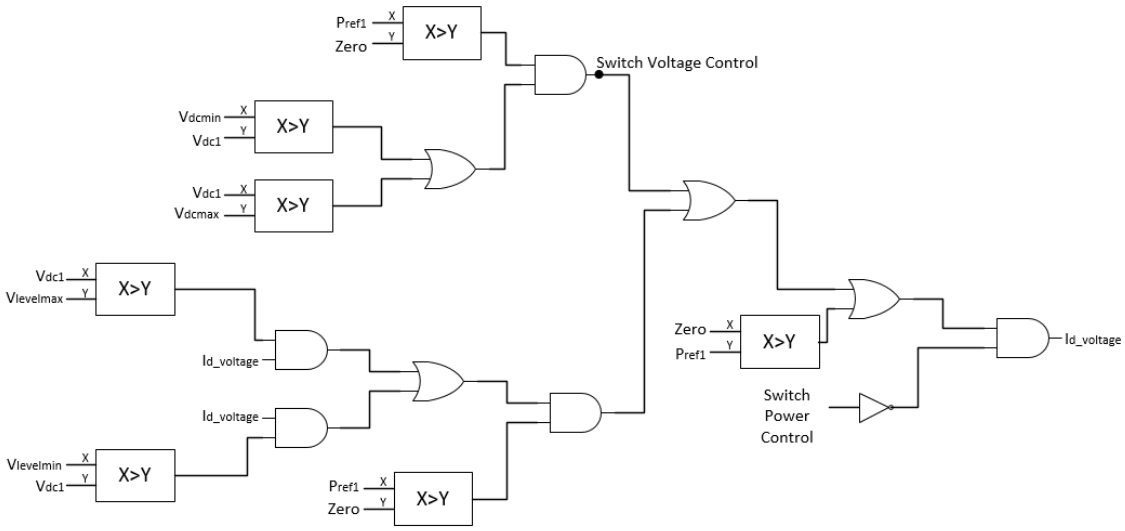

Figure 3.2: Logic to Determine if I_{dref} is to Be Controlled Using a Voltage Reference

The controllers shown in Figures 3.2 and 3.3 are designed such that the inverter will be controlled using the power reference unless the DC voltage goes above the maximum voltage, 1.1 times the nominal V_{dc}, or below the minimum voltage, 0.9 times the nominal V_{dc}. When the voltage is out of tolerance the controller determines I_{dref} using a DC voltage control loop as shown in Figure 3.5. When the voltage falls below 1.05 times the nominal V_{dc} or above 0.95 times the nominal V_{dc} the control reverts back to control based on a power reference.

The power reference calculation contains a voltage droop gain to alter the original desired power reference to attempt to keep the voltage from getting out of range and to allow multiple converters to be regulated voltage in parallel. The calculation for

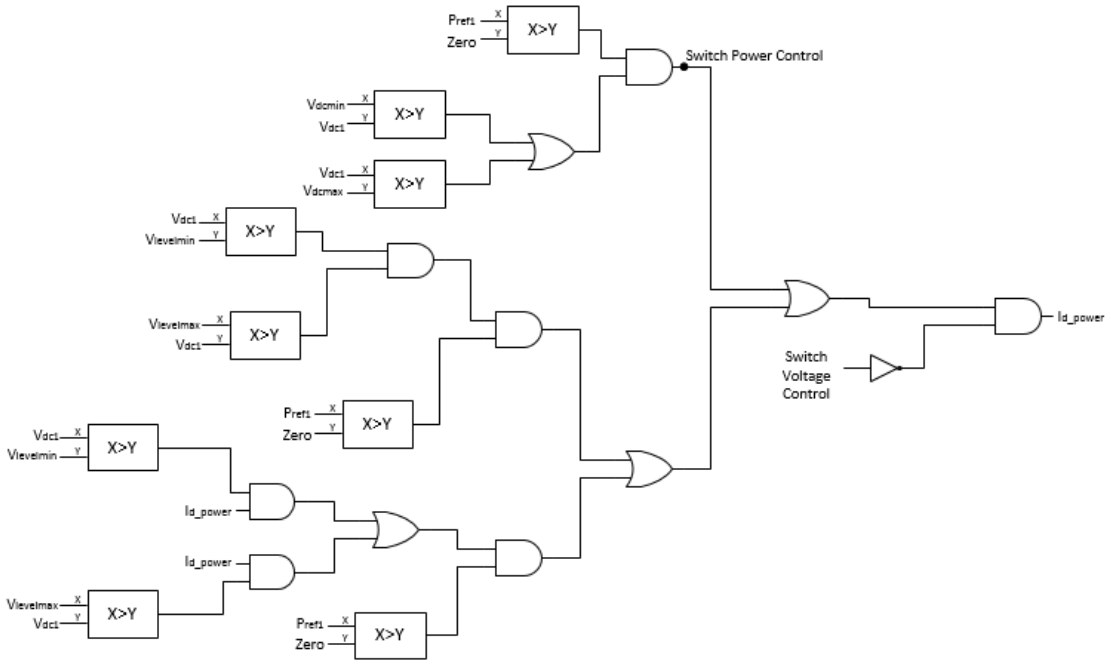

Figure 3.3: Logic to Determine if I_{dref} is to Be Controlled Using a Power Reference

P_{ref} using a voltage droop gain constant is shown in Figure 3.4 [11]. The droop gain is calculated using (3.2) and is set to 10,000 for this study system based on the nominal power rating and the voltage range.

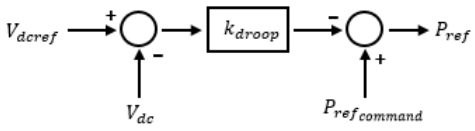

Figure 3.4: Power Reference Calculation Using Voltage Droop Gain

$$k_{droop} = \frac{2P_{dc_{max}}}{V_{dc_{max}} - V_{dc_{min}}} \tag{3.2}$$

After P_{ref} is computed for each converter, I_{dref} and I_{qref} need to be computed for each converter as well. The reason I_{dref} and I_{qref} are computed instead of $I_{abc_{ref}}$ is because signals in the dq frame are slowly varying and are not sinusoidal values, which makes it easier to design because for signals that are not sinusoidal, there is

no steady-state error due to the integrating term in the PI controller. Effectively modulating I_{dref} and I_{qref} yields no stead-state error.

To calculate I_{dref} from the power reference and I_{qref} from a reactive power reference equations (2.4) and (2.5) are used as discussed in Chapter 2 [9]. The values for the current regulator PI control loops, k_i and k_p, are chosen based upon the respective Thevenin AC grid impedances and the time constants. A typical time constant, τ_i, is between 0.5-5 ms [4]. For the AC systems that were used in this model, τ_i was chosen to be 5 ms. The resistance of each of the AC systems was 0.71287 Ω and the inductance was 0.01891 mH which were calculated from the desired short circuit ratio (SCR) using (3.1). The k_p and k_i for the current PI controllers are calculated using (2.6) and (2.7).

As mentioned in Chapter 2, the reference for I_d can be calculated using two different methods in this control loop. When P_{ref} is used to calculate I_{dref}, it is a direct calculation using (2.4). When DC voltage regulation is used, it requires another PI controller. When cascaded PI loops are used, the inner loop must operate faster than the outer loop. To achieve this, equations (3.3) and (3.4) are used. Dividing the constants by 7 makes the outer control loop approximately 7 times slower than the inner control loop. The controller for the d-axis current is shown in Figure 3.5. The controller for the q-axis current is the same as was used for the point-to-point system and is shown in Figure 2.5.

$$k_{pv} = \frac{k_p}{7} \tag{3.3}$$

$$k_{iv} = \frac{k_i}{7} \tag{3.4}$$

The modulating functions, M_d and M_q, are limited to vary between positive and negative one. They are transformed into the abc frame to control the converter output

voltage to regulate AC current. This simulation uses averaged converter models, so M_{ABC} are used to calculate the applied AC voltage and injected DC current at described in Chapter 2. Equations (2.8) through (2.12) are used to put M_d and M_q into the abc reference frame. The currents $I_{P_{abc}}$ and $I_{N_{abc}}$ are the DC current injections to the positive and negative poles for the averaged model as shown in Figure 1.2. The calculation of the DC currents and AC voltages for the converter models using M_{abc} are shown in (2.13) through (2.23).

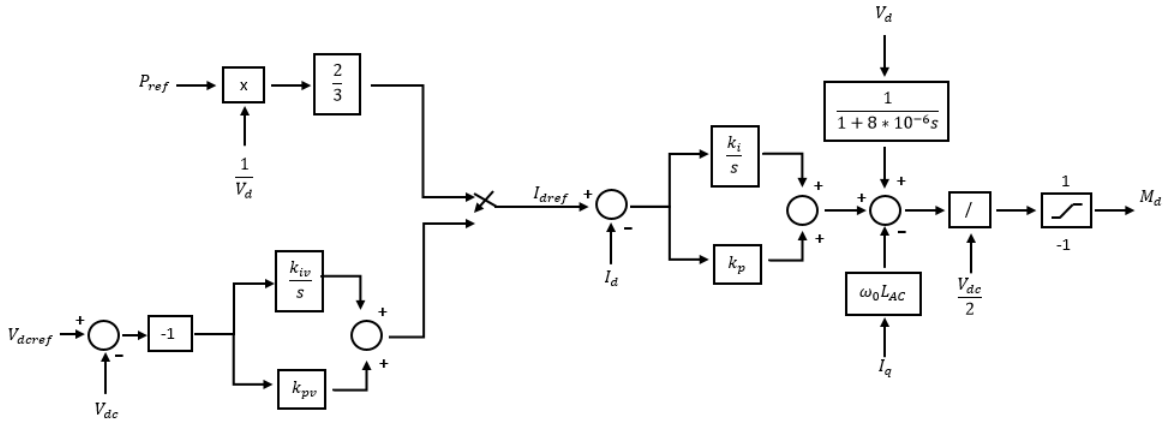

Figure 3.5: D axis Control Loop for Each Converter in a Multiterminal VSC HVDC transmission system

3.2 Simulation Cases Demonstrating Routine Operation of the Multiterminal VSC HVDC System

To demonstrate that the control scheme is working properly, P_{ref}, V_{dcref}, and Q_{ref} are set in the simulation for each converter. The control logic then determined whether I_d should be controlled based on the power or DC voltage reference for each converter. If the power reference is used to calculate I_{dref}, the reference is offset from the desired power reference based on the voltage droop gain and the voltage error. These settings are calculated and set for each converter. The nominal V_{dcref} was set to 450 kV. A 20 second simulation is used to test the controls to ensure expected

operation. In this simulation converters one and three act as inverters and converters two and four act as rectifiers. The first part of the simulation results are start-up transients and don't represent normal operation and that time period is not included in the figures shown here. The simulations do not use start up sequences that would be used in the field.

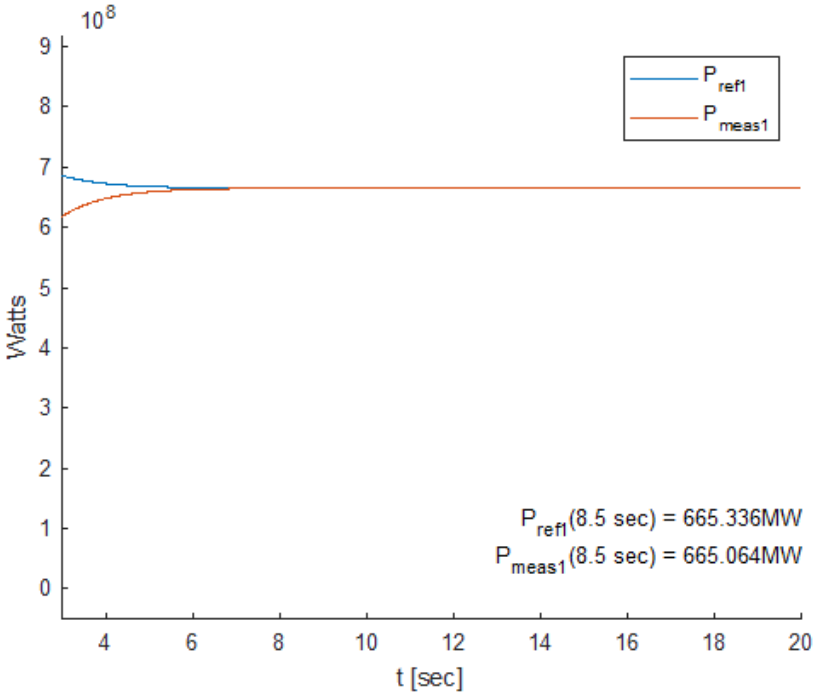

Figure 3.6: Power reference for Converter One (P_{ref1}), and the Measured Power for Converter One (P_{meas1}) in Response to a Step Change in Power Reference for Converter One

Figures 3.6 and 3.7 show simulation results for converter one, where the converter is acting as an inverter. Since the voltage is within normal limits shown in Figure 3.7, I_{dref1} is calculated from the power reference. Figure 3.6 also shows that the power reference is tracking properly.

Figures 3.8 and 3.9 show the behavior of converter three. Figure 3.8 shows that the power reference is the same as the power measured. This means that the control logic that determines what I_{dref3} is creating a reference such that the real power

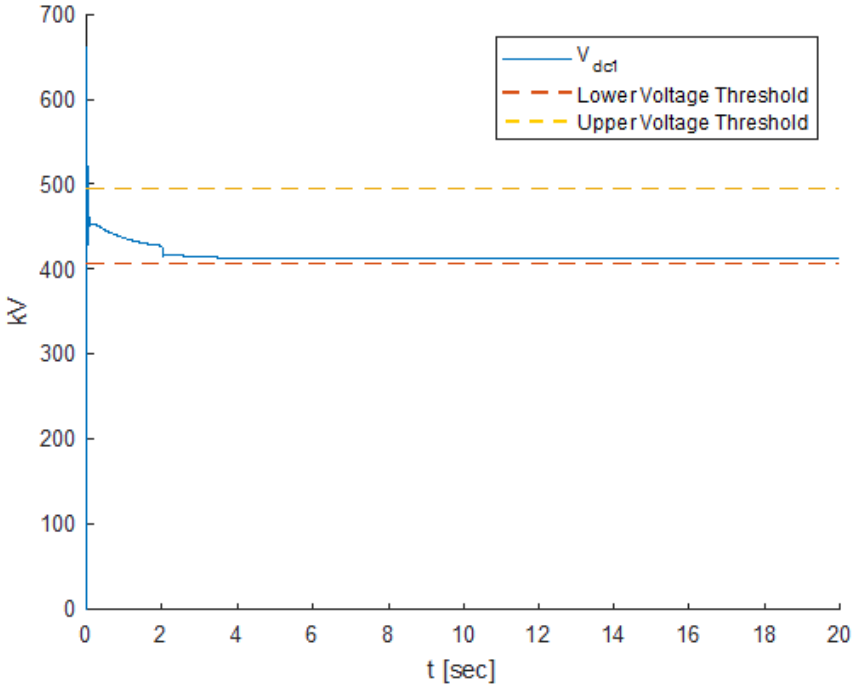

Figure 3.7: V_{dc1} in Response to a Step Change in Power Reference for Converter One

reference is being tracked. This could also be deduced since the voltage stays above $V_{dc_{min}}$ shown in Figure 3.9. Figure 3.8 also shows that converter 3 is operating as an inverter because the power is positive and that the PI loop is working properly.

Figures 3.10 and 3.11 show that the voltage references for converters two and four are being tracked and within the voltage thresholds. If the voltage reference is being tracked this means that the controller in Figure 3.5 is basing the calculation for I_{dref} on the DC voltage for converters two and four. Both of these converters are acting as rectifiers. Since the voltage levels remain within an acceptable level for each converter, this indicates that the power is balanced on the DC grid, since the voltage level is an indicator of the power balance.

Figures 3.6 through 3.11 use another senario to demonstrate that the control scheme is working as designed and has a stable response to changes in desired real and reactive power. It is important to note that the AC system may not be able to respond to large rapid changes in the power references and in practice power is ramped

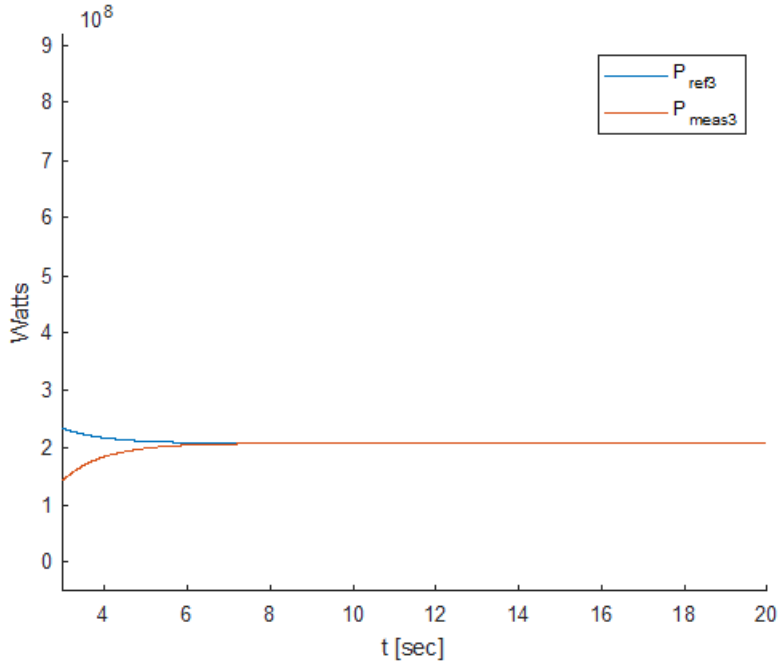

Figure 3.8: Power Reference for Converter Three (P_{ref3}), and the Measured Power for Converter Three (P_{meas3}) in Response to a Step Change in Power Reference at Converter One

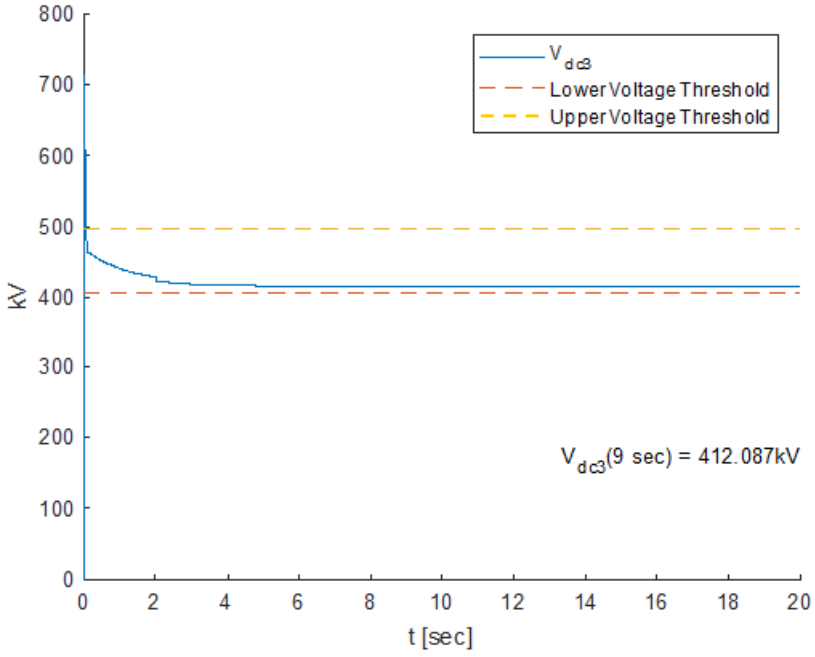

Figure 3.9: V_{dc3} in Response to a Step Change in Power Reference at Converter One

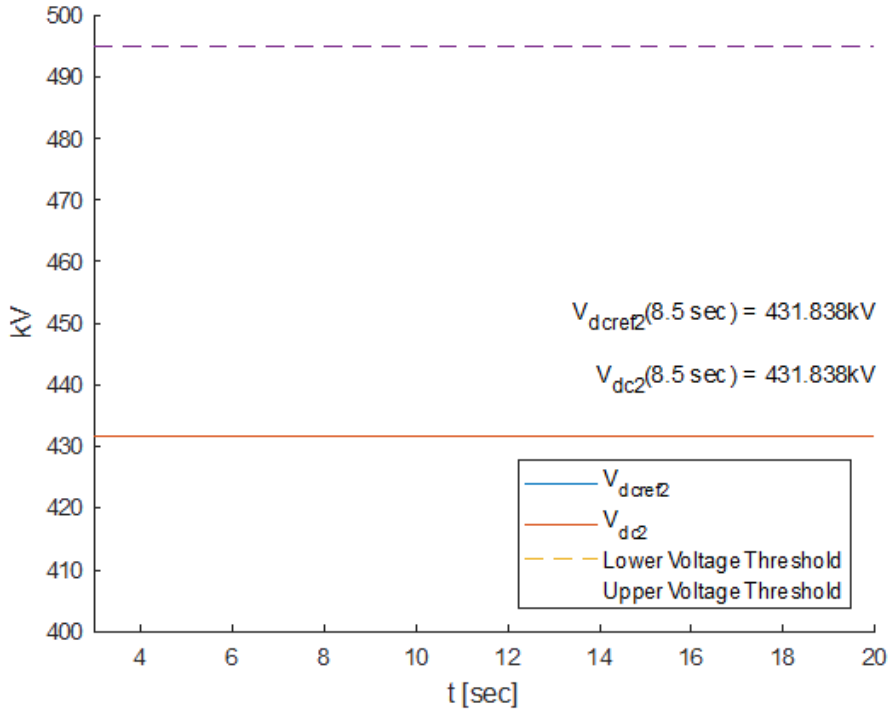

Figure 3.10: V_{dcref2} and V_{dc2} in Response to a Step Change in Power Reference at Converter One

more slowly. A step change is shown here to evaluate converter control response to an extreme condition.

This chapter discussed the control and normal operation of a multiterminal VSC HVDC transmission system. This chapter also discussed the reasoning behind the values that were chosen and calculated for the different components of the system. The results of the simulation were shown to demonstrate that the references are being tracked and that the system is operating as expected.

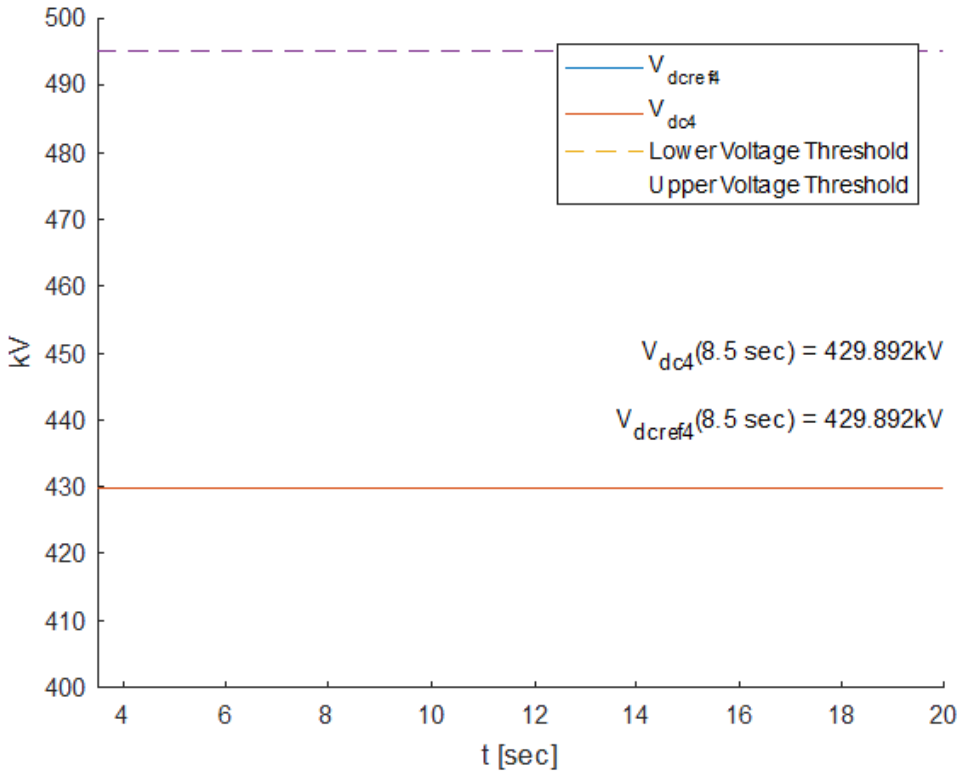

Figure 3.11: V_{dcref4} and V_{dc4} in Response to a Step Change in Power Reference at Converter One

CHAPTER 4

Multiterminal VSC HVDC Transmission System Cyber-Attacks

There are many potential cyber-attacks vectors. This chapter will look at attacks modifying communicated measurement signals. To simulate the attack, certain measurements are changed to a spoofed value. The number of signals that are changed at one time are limited to either one or two. The attacks that have one signal spoofed are referred to here as single attacks and the attacks with two signals spoofed are called double attacks. To detect these cyber-attacks, the spoofed signals or calculations from these spoofed signals are compared with expected values calculated based on physical relationships with other measurements.

4.1 Single Attacks

Four different types of single attacks were performed on this system. These attacks spoofed the AC voltage amplitude, AC current amplitude, AC real power, and DC voltage measurements.

4.1.1 AC Voltage Measurement Attack

To detect an AC voltage spoof cyber-attack, the measured AC voltage magnitude can be compared to a voltage calculated from the three phase power magnitude and measured current. This calculation shown in (4.1). Where $|I_{AC_{expected}}|$ can then be compared to the magnitude of the AC current for that converter. If the system is not under attack, this value should be close or equal to zero.

$$|I_{AC_{expected}}| = \frac{|S_{3phase}|}{3|V_{spoof}|} \tag{4.1}$$

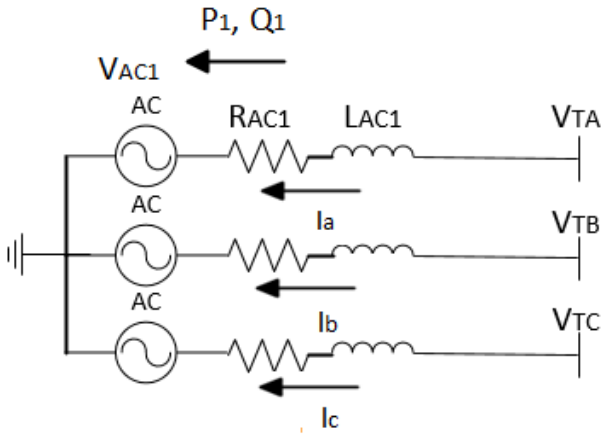

Figure 4.1: AC system connected to converter 1

For this spoof attack $|V_{AC}|$, shown in 4.1, was set to 115 kV_{LN} RMS and the normal voltage is about 104 kV_{LN} RMS. Figure 4.2 shows the difference between $|I_{AC_{expected}}|$ and the measured $|I_{AC}|$ during and attack, $|I_{error_{attack}}|$, and during no attack, $|I_{error_{noattack}}|$.

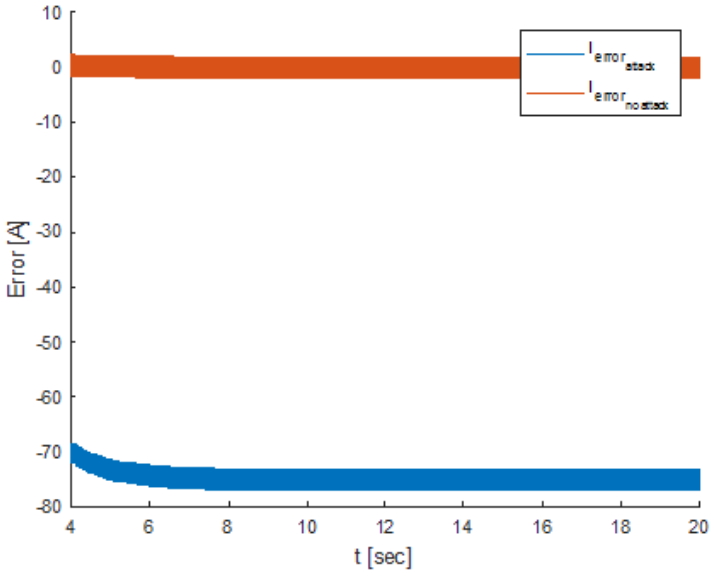

Figure 4.2: Error between $|I_{AC_{expected}}|$ and the actual $|I_{AC}|$ for the system under an AC voltage spoof cyber-attack and under normal operation

Figure 4.2 shows that when there is no attack, the detector sees a value at or very close to zero. The figure also shows that when there is an attack, $I_{error_{attack}}$ is below

zero.

4.1.2 AC Current Measurement Attack

To detect an AC current spoof cyber-attack, the measured AC current magnitude can be compared to an expected AC current magnitude calculated from the three phase power magnitude and the measured AC voltage. This calculation shown in (4.2). $|I_{AC_{expected}}|$ can then be compared to the magnitude of the measured AC current for that converter. If the system is not under attack, this value should be close or equal to zero.

For this spoof attack $|I_{AC}|$ was set to have a peak of 1500 A where the set point AC current would be about 1200 A peak. Figure 4.3 shows the error between $|I_{AC_{expected}}|$ and the measured $|I_{AC}|$.

$$|I_{AC_{expected}}| = \frac{|S_{3phase}|}{3|V_{AC}|} \tag{4.2}$$

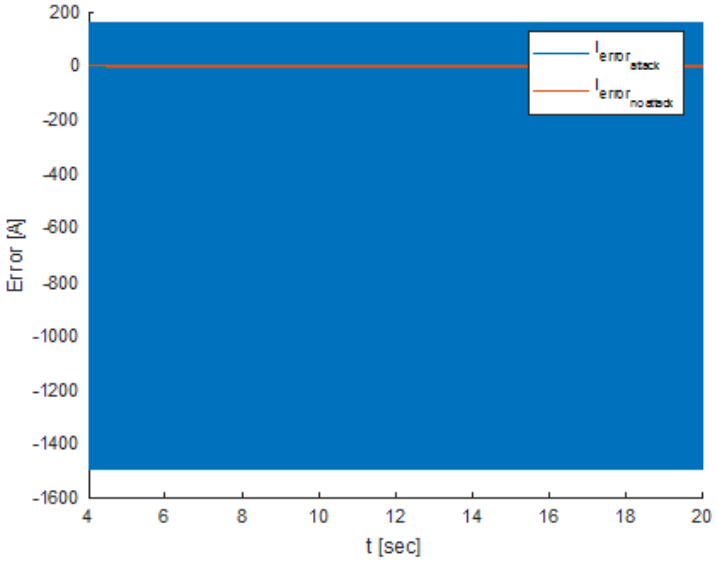

Figure 4.3: Error between $|I_{AC_{expected}}|$ and the actual $|I_{AC}|$ for the system under an AC current spoof cyber-attack and under normal operation

Figure 4.3 shows that when there is no attack, the detector outputs a value at or very close to zero. It also shows that when there is an attack, $I_{error_{attack}}$ is oscillating far above and below zero where the average value is a large negative number.

4.1.3 AC Real Power Measurement Attack

To detect an AC real power spoof cyber-attack, the measured AC real power spoofed magnitude can be used to calculate the magnitude of the three phase apparent power using the three phase reactive power measurement. This and the measured voltage then can be used to calculate the expected AC current magnitude. This expected AC current magnitude can then be compared to the measured AC current magnitude. This calculation is shown in (4.1). $|I_{AC_{expected}}|$ can then be compared to the magnitude of the measured AC current for that converter. If the system is not under attack, this value should be close or equal to zero.

$$|I_{AC_{expected}}| = \frac{|S_{3phase_{spoofed}}|}{3|V_{AC}|} \tag{4.3}$$

For this spoof attack, $|P_{3phase_{spoof}}|$ was set to 500 MW. As stated in Chapter 3, the power rating of the converter is 900 MW. The power set point before the droop control block is 544.43 MW, but with droop included the power set point is about 262 MW. Figure 4.4 shows the error between $|I_{AC_{expected}}|$ and the actual $|I_{AC}|$.

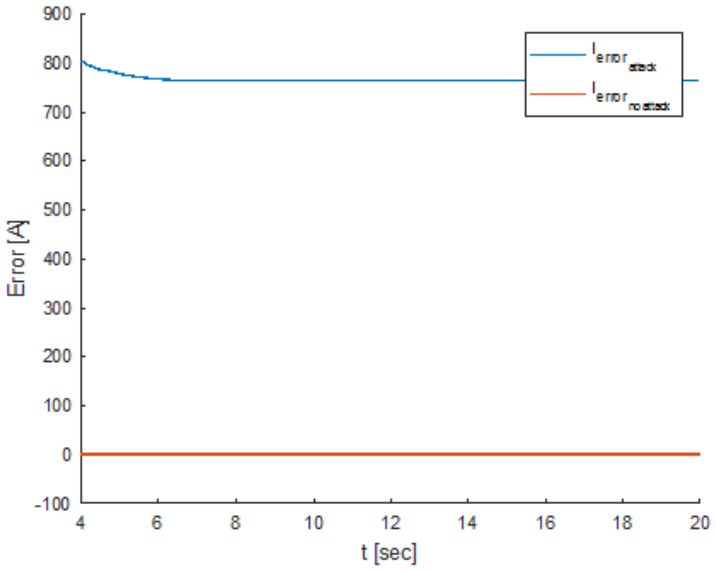

Figure 4.4: Comparison of Error between $|I_{AC_{expected}}|$ and the actual $|I_{AC}|$ for the system under an AC power measurement spoof cyber-attack and under normal operation

Figure 4.4 shows that when there is no attack, the detector sees a value at or very close to zero. It also shows that when there is an attack, it detects it since $I_{error_{attack}}$ is far above zero.

4.1.4 DC Voltage Measurement Spoof

To detect a DC voltage spoof cyber-attack, the measured DC power and the measured DC current can be used to calculate the expected DC voltage. This calculation shown in (4.4). The expected DC voltage can then be compared to the measured DC voltage for that converter. If the system is not under attack, this value should be close or equal to zero.

$$V_{DC_{expected}} = \frac{P_{DC}}{I_{DC}} \tag{4.4}$$

For this attack $V_{DC_{spoof}}$ was set to 0.7*$V_{DC_{meas}}$, where the nominal $V_{DC} = 450$ kV.

Figure 4.5 shows the error between $|V_{DC_{spoof}}|$ and the actual $|V_{DC_{meas}}|$.

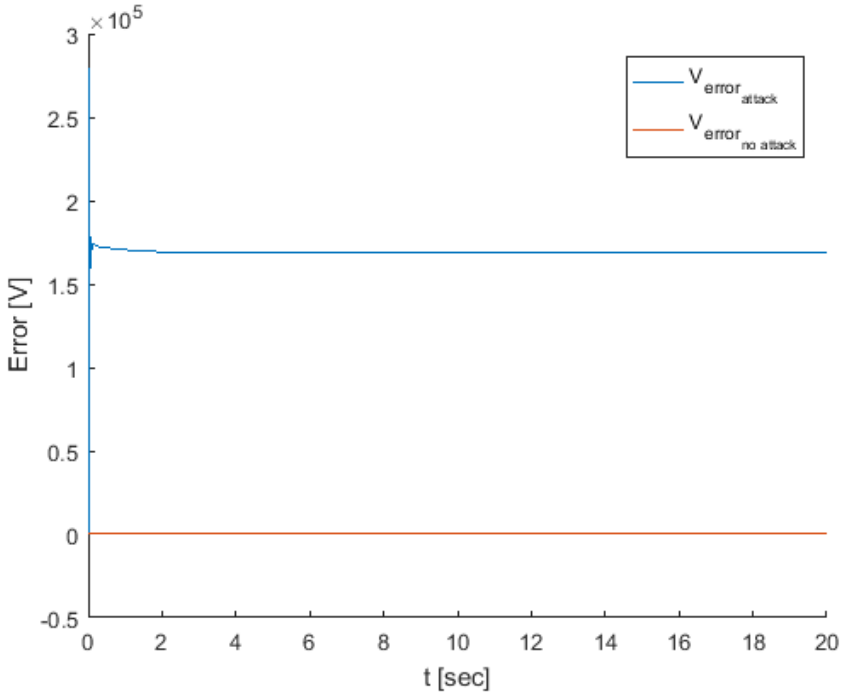

Figure 4.5: Error between $V_{DC_{expected}}$ and the actual $V_{DC_{meas}}$ for the system under a DC voltage spoof cyber-attack and under normal operation

Figure 4.5 shows that when there is no attack, the detector sees a value at or very close to zero. It also shows that when there is an attack, it detects it since $I_{error_{attack}}$ is far above zero.

4.2 Double Attacks

After completing the set of single attacks on the system, a set of simultaneous double attacks are developed that are crafted to be self consistent to thwart simple detection schemes. Additional detection methods are developed to address these potential cases. When there are two simultaneous attacks on the system, it will be referred to as a double attack in this thesis. The four double attacks that are performed on this system combine spoofed measurements for the AC voltage and AC current, AC current and AC real power, DC voltage and DC power, and AC real

power and AC voltage.

4.2.1 Combined Attack on AC Voltage and AC Current Measurements

For the double attack on AC voltage and AC current measurements, the spoofed AC Voltage is chosen to be a little above the expected AC voltage at 115 kV_{LN} RMS. The normal AC voltage is at about 104 kV_{LN} RMS. The AC current measurement is scaled such that the apparent power does not change. The calculation of this spoofed current measurement is shown (4.5). The value for $|I_{AC_{spoof}}|$ was chosen to fool the detector developed in section 4.1.1 into thinking that there was no attack.

$$|I_{AC_{spoof}}| = \frac{|S_{3phase}|}{3|V_{AC_{spoof}}|} \tag{4.5}$$

To detect the attacks, two methods were used. The $method_{AC_1}$ developed earlier to detect a single attack and a new method that could detect both single and double attacks. The first method calculated the expected current based on the measured three phase apparent power for the measured (spoofed) AC voltage. The current from the calculation is then compared to the measured AC current. Since the spoofed current in this case is calculated using the three phase power and the spoofed AC voltage, it is obvious that this method would not detect the attack. This method was chosen to demonstrate how the detector could be fooled if the correct two measurements were spoofed in a self consistent fashion.

The $method_{AC_2}$ calculates the AC current by subtracting the AC voltage, V_{AC}, and the AC voltage just outside the terminals, V_T, and then dividing by the impedance between these two measurement points. V_{AC1} and V_{TA} are shown in Figure 4.1. This calculated current is then compared to the measured AC current. This method is shown in (4.6).

$$|I_{AC_{expected}}| = \frac{|V_{AC_{terminals}} - V_{AC_{spoof}}|}{|Z_{AC}|} \tag{4.6}$$

Figure 4.7 compares the responses of $method_{AC_1}$ and $method_{AC_2}$ for a double attack on the measured AC voltage and AC current measurements. The signals plotted are the outputs of the error calculations that result from using $method_{AC_1}$ and $method_{AC_2}$ during normal operation in Figure 4.6 and during a double attack in Figure 4.7. $Method_{AC_1}$ determines the error between the measured AC current and the AC current that is calculated using the three phase power measurement shown in (4.1). $Method_{AC_2}$ determines the error between the measured AC current and the AC current calculated by calculating the difference between the two AC voltage phasors and dividing the difference by the impedance shown in (4.6).

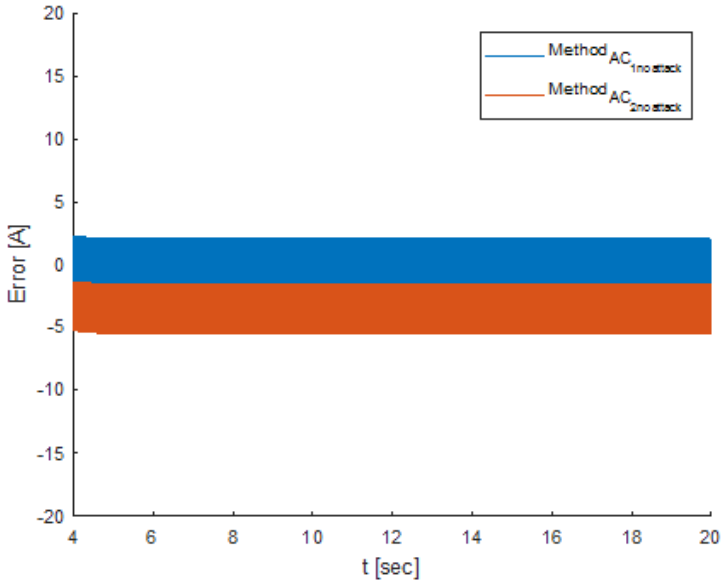

Figure 4.6: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $Method_{AC_1}$ and $Method_{AC_2}$ during normal operation

Figure 4.7 shows the second method works for detecting this type of double attack while $method_{AC_1}$ does not. These are the results that were expected since the AC current spoof was designed that way. The first method could still be used to detect

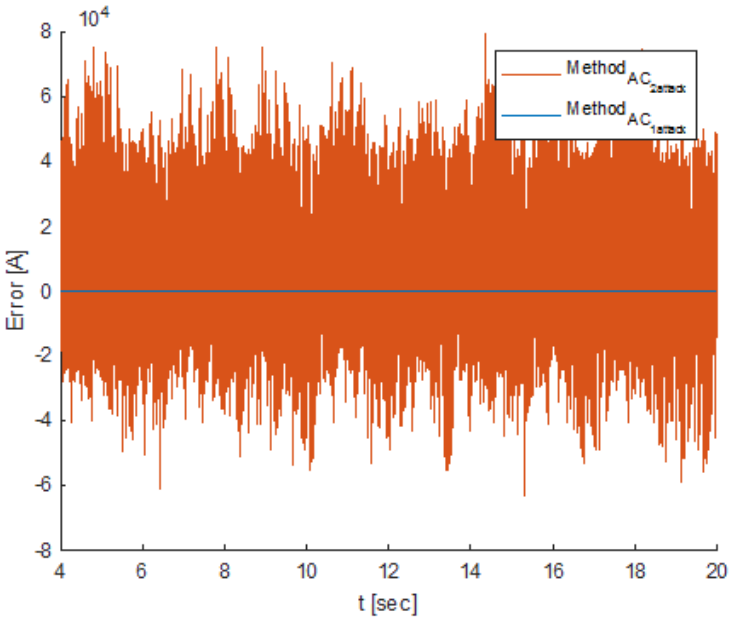

Figure 4.7: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $Method_{AC_1}$ and $Method_{AC_2}$ a double attack

double attacks if the current had been changed randomly without trying to maintain apparent power.

4.2.2 Combined Attack on AC Current and AC Real Power Measurements

For the double attack on the AC current and AC real power measurements, the spoofed AC current measurement was chosen to be 1500 A peak. The spoofed AC real power measurement is calculated to be the spoofed current in the synchronous dq frame multiplied by the correct components of the AC voltage measurement in the dq frame. This is equivalent to the equations used in the abc frame to calculate real power. This is done to try and fool the detectors into determining that these were realistic numbers. Equation (4.7) shows the calculation for the spoofed real power, where ϕ stands for power factor angle.

$$P_{3phase_{spoof}} = V_d I_{d_{spoof}} + V_q I_{q_{spoof}} + V_0 I_{0_{spoof}} = 3|V_{AC}||I_{AC}|cos(\phi) \tag{4.7}$$

To detect the simultaneous attacks on the AC current measurement and AC power measurement, two methods were employed. The first uses the AC power measurement, and the second uses two AC voltage measurements and the AC impedance. Since the AC power measurement is spoofed in this case, the first method is expected to fail.

$Method_{AC_1}$ starts by calculating the three phase apparent power magnitude from the spoofed AC real power and the AC reactive power measurement. Then an AC current magnitude is calculated by dividing the calculated AC apparent power by three times the AC line to ground voltage magnitude. This is shown in (4.8). This calculated AC current magnitude is compared to the measured AC current.

$$|I_{AC_{spoof}}| = \frac{|S_{3phase_{spoof}}|}{3|V_{AC}|} \tag{4.8}$$

$Method_{AC_2}$ calculates a current by calculating a voltage difference between two phasor voltages and the known impedance between them. This assumes both voltage measurements have a common time reference. This calculated AC current magnitude is compared to the measured AC current magnitude, with the outputs of the two detection schemes shown in (4.9).

$$|I_{AC_{expected}}| = \frac{|V_{AC_{terminals}} - V_{AC_{system}}|}{|Z_{AC}|} \tag{4.9}$$

Figure 4.8 shows the responses of $method_{AC_1}$ and $method_{AC_2}$ during normal operation with no attacks. Figure 4.9 shows the responses with a double attack on the AC current and AC real power measurements. Note that $method_{AC_1}$ does not detect this type of double attack. While $method_{AC_1}$ does not detect the attack, this plot shows that $method_{AC_2}$ produces a large enough error signal to be useful in detecting

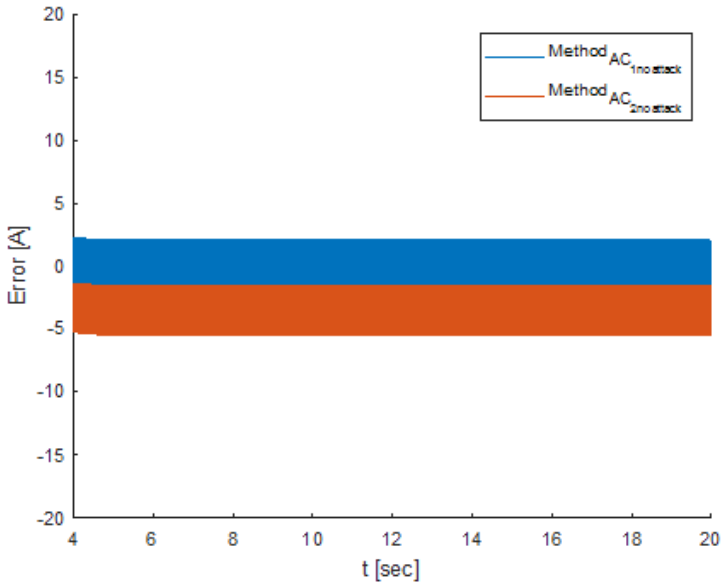

Figure 4.8: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $Method_{AC_1}$ and $Method_{AC_2}$ during normal operation

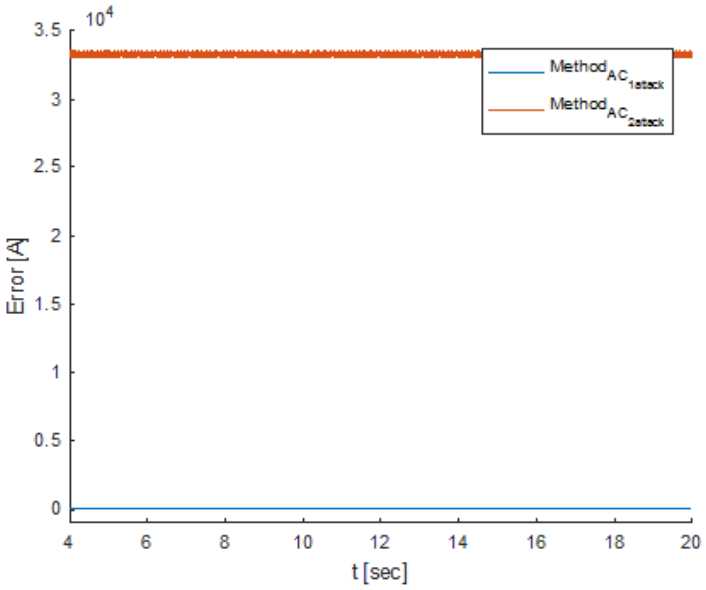

Figure 4.9: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $Method_{AC_1}$ and $Method_{AC_2}$ during a double attack

the attack because this signal is far above zero. However, the first method would be useful in detecting attacks if the AC real power measurement had been crafted differently.

4.2.3 Combined Attack on DC Voltage and DC Power Measurements

For the simultaneous attacks on the DC voltage and DC power measurements, the spoofed DC voltage was chosen to be 420 kV because it was within the normal range for the DC voltage, which is between 405 and 495 kV. The spoofed value is also far enough below the nominal 450 kV to keep this converter in inverter mode as was original setting in the simulation. The spoofed DC power measurement was chosen to try and prevent the attack from being detected. The calculation for the spoofed power is shown in (4.10).

$$P_{DC_{spoof}} = V_{DC_{spoof}} I_{DC} \tag{4.10}$$

Two methods are used to try to detect the attack on the measured DC voltage and the attack the DC power measurement. If the DC power measurement had not been spoofed to match the DC current, the first method would have been able to detect the attack. $Method_{VDC_1}$ calculates the expected DC voltage based off of the DC current and DC power. This expected voltage is then compared to the measured V_{DC}, as shown in (4.4). This error between the measured signal and the calculated signal and should remain at or close to zero for no attack.

The second method uses the each of the converter's measured DC voltages to calculate the expected DC line currents. The measured line currents on each DC line leaving the converter are used to calculate the expected total DC current for each converter. The current for the line connecting converters one and two is calculated using (4.11) and a similar approach would be used for each line current. This method depends on maintaining secure communication between terminals. Equation (4.11) uses the pole-to-pole voltages, so the voltage difference is divided by the total resistance of the positive and negative poles (2^*R_{12}). Equation (4.13) is used to com-

pute the total DC current leaving converter one. A similar equation can be used for each converter. Figure 4.10 shows a diagram of the DC system with a symmetrical monopole configuration. This calculated value is then compared to the measured DC current and the error of those two signals and should remain at zero under normal operating conditions with no attack.

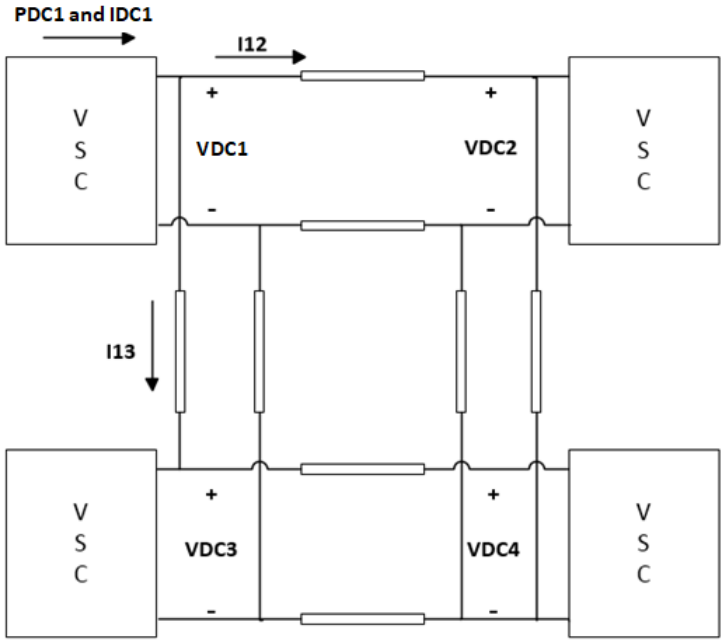

Figure 4.10: DC System Grid to Identify Spoofed Signals

$$I_{DC_{12}} = \frac{V_{DC1} - V_{DC2}}{2R_{12}} \tag{4.11}$$

$$I_{DC_{conv1}} = I_{DC_{12}} + I_{DC_{13}} + ... + I_{DC_{1N}} \tag{4.12}$$

As stated previously, the output signals from both methods should be at zero for normal operation, as shown in Figure 4.11. When $method_{VDC_1}$ is zero, the voltage resulting from DC power measurement, divided by the DC current measurement is equal to the measured voltage. When $method_{VDC_2}$ is zero, the measured DC current for converter one is the same as the calculated currents using the voltages of each

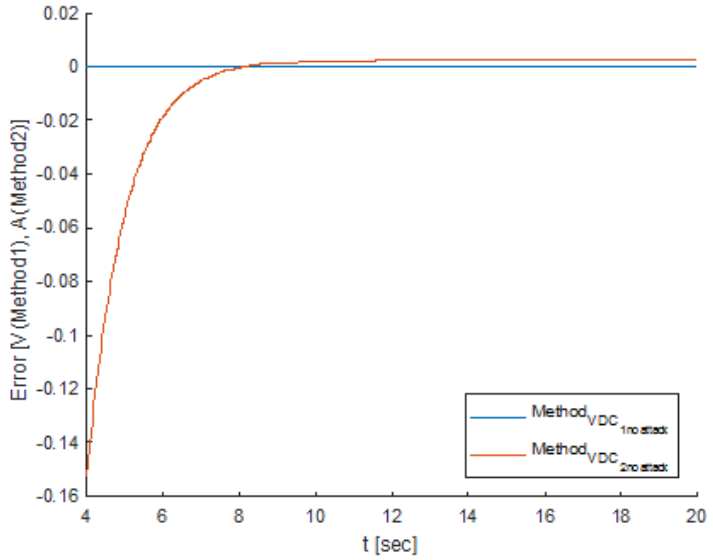

Figure 4.11: Error results during normal operation from $Method_{VDC_1}$, which calculates V_{DC} from P_{DC} and I_{DC}, and $Method_{VDC_2}$, which calculates I_{DC} from the system's DC voltages and resistances

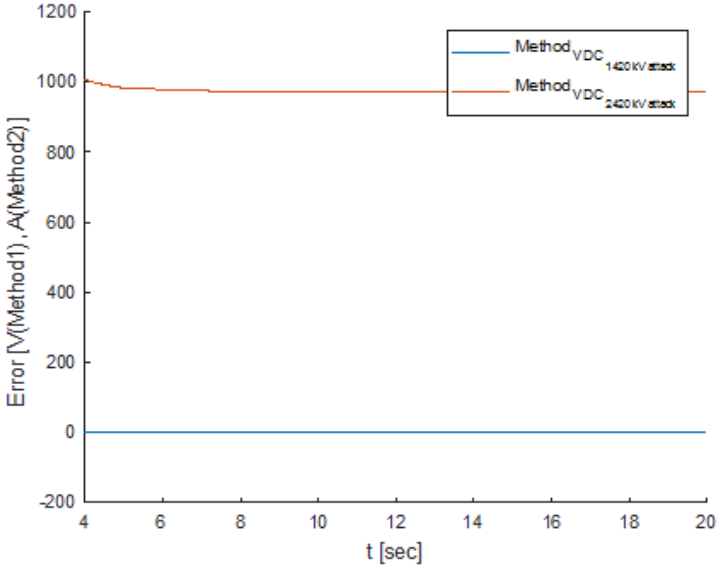

Figure 4.12: Error results from $Method_{VDC_1}$ which calculates V_{DC} from P_{DC} and I_{DC}, and $Method_{VDC_2}$, which calculates I_{DC} from the system's DC voltages and resistances, during a DC voltage and DC power measurement double attack with the DC voltage spoofed to 420 kV

converter and each line's resistance. $Method_{VDC_2}$ detects the specific double attack, while $method_{VDC_1}$ was unable to do so due to the way P_{DC} is spoofed.

The double attack described above would have limited impact on the system operation since the DC voltage did not change significantly, and the converter operating mode did not change. The change in P_{DC} would have some impact. If the DC voltage had been spoofed to a value outside of the range where the converter controls maintain constant power it would have a larger impact on operation. Figure 4.13 shows the outputs from the same detectors when the DC voltage is spoofed to 496 kV. It can be seen from the figure that the output signal for $method_{VDC_2}$ is oscillating far above and below zero, indicating that an attack is detected.

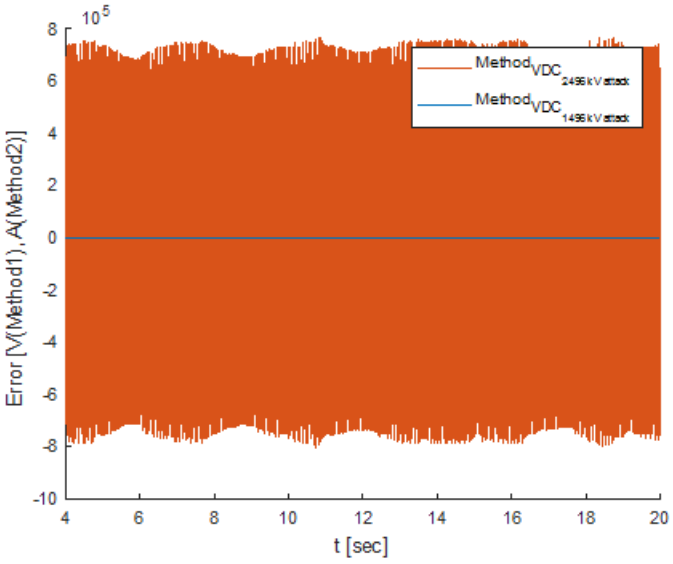

Figure 4.13: Error results from $Method_{VDC_1}$ which calculates V_{DC} from P_{DC} and I_{DC}, and $Method_{VDC_2}$, which calculates I_{DC} from the system's DC voltages and resistances, during a DC voltage and DC power measurement double attack with the DC voltage spoofed to 496 kV

If the DC voltage is spoofed to be 404 kV, which is outside the DC voltage range for the converter operating as an inverter, the result of the detectors are shown in Figure 4.14. Figures 4.13 and 4.14 both show that $method_{VDC_1}$ does not detect the attack but $method_{VDC_2}$ detects the double attacks.

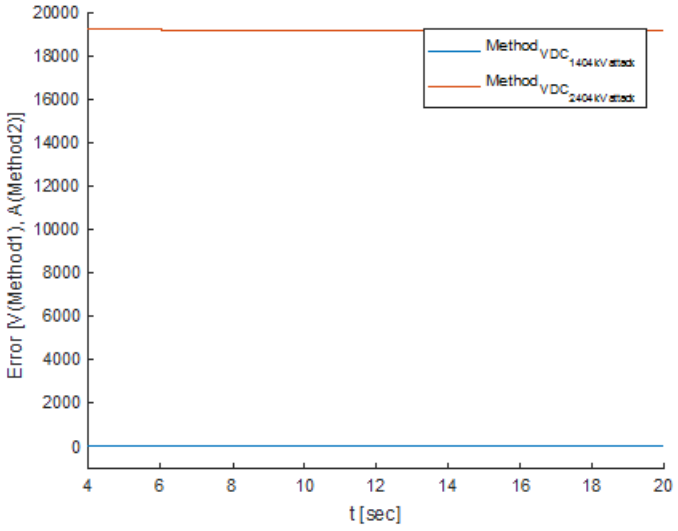

Figure 4.14: Error results from $Method_{VDC_1}$ which calculates V_{DC} from P_{DC} and I_{DC}, and $Method_{VDC_2}$, which calculates I_{DC} from the system's DC voltages and resistances, during a DC voltage and DC power measurement double attack with the DC voltage spoofed to 404 kV

4.2.4 Combined Attack on AC Real Power and AC Voltage Measurements

To implement the AC real power and AC voltage measurement double attack, the spoofed AC real power measurement was chosen to be 500 MW where the power rating of the converter is 900 MW. The actual power setting before the droop control is 544.43 MW, but with droop control the power set point is about 262 MW. The AC voltage measurement was chosen to be the spoofed AC real power measurement divided by three times the magnitude of the AC current times the power factor of converter one to attempt to make detecting the attack more difficult. This is shown in (4.13) where ϕ stands for power factor angle. The location of the spoofed AC voltage can be seen in Figure 4.1.

$$V_{AC_{spoof}} = \frac{P_{3phase_{spoof}}}{3|I_{AC}|cos(\phi)} \tag{4.13}$$

Two methods were tested to try to detect this attack. The first method uses a three phase apparent power magnitude and the measured AC voltage magnitude to calculate the expected current magnitude, as shown in (4.14). The three phase apparent power magnitude is calculated from the measured real and reactive power. In this case, the real power is spoofed. The calculated current magnitude is then compared to the measured current magnitude, with the difference used as the output for this $method_{AC_1}$. This method is the same method that was used in 4.2.1 and 4.2.2.

$$|I_{AC_{expected}}| = \frac{|S_{3phase}|}{3|V_{AC}|} \tag{4.14}$$

The second method uses the AC voltage phasors at the terminals of the converter, the AC voltage phasors at the point of interconnect, which is the spoofed AC voltage, and the line impedance to calculate a current magnitude. This is the same method that is used in 4.2.1 and 4.2.2 and is shown in (4.6). This magnitude is then compared to the measured current magnitude, and the difference is the output for plotting and could be an input to detection logic.

Figure 4.15 shows that when there is no attack on the system the detectors output near zero, indicating they do not detect an attack. Figure 4.16 shows that the second method detected the attack, note that the vertical scale is 10 orders of magnitude higher than in Figure 4.15. While $method_{AC_1}$ did not detect the attack since the AC voltage measurement was designed to match the spoofed AC power and the measured current. If the AC voltage had not been spoofed consistently with the AC current, the first method would have detected the attack.

This chapter has demonstrated single and double attacks on measurements used as inputs for control loops can be detected on an MTDC VSC HVDC transmission system. While these methods seem promising, more research is needed in this area to determine thresholds of the detectors to minimize false positives.

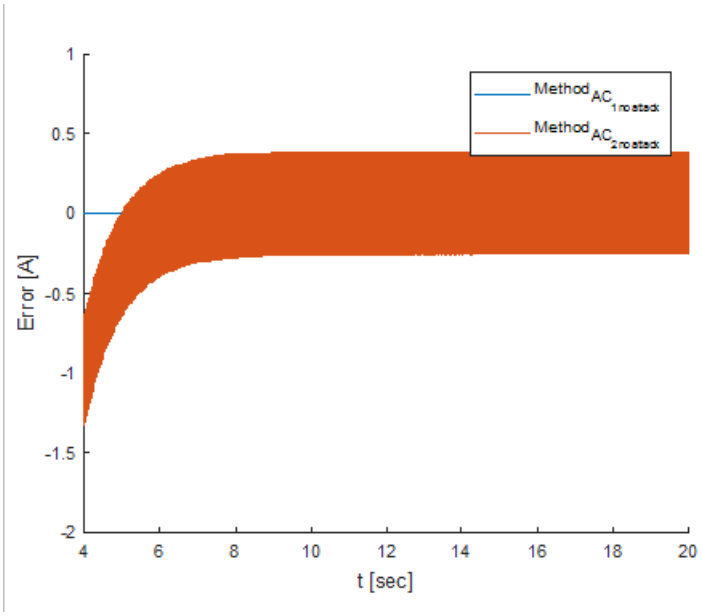

Figure 4.15: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $method_{AC_1}$ and $method_{AC_2}$ during normal operation

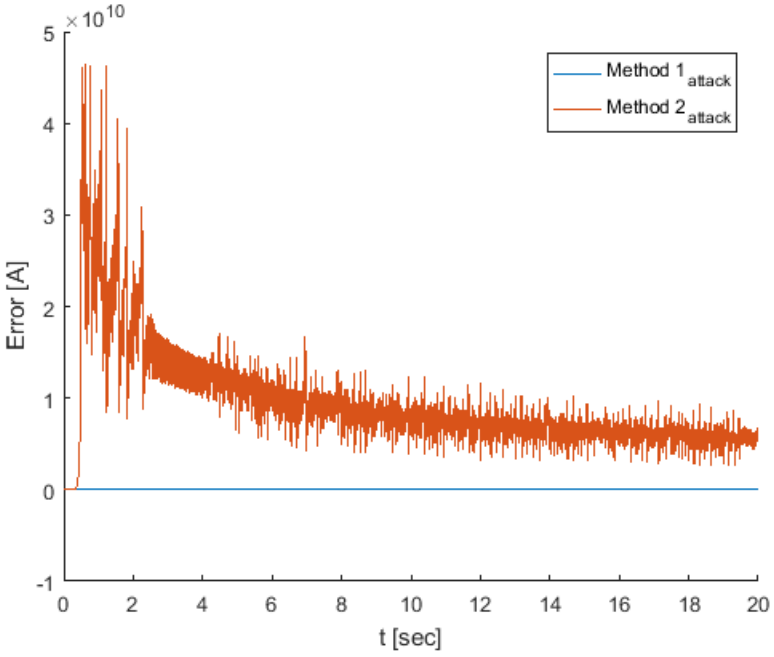

Figure 4.16: Error between $|I_{AC_{expected}}|$ and $|I_{AC_{meas}}|$ for $method_{AC_1}$ and $method_{AC_2}$ during a double AC real power and AC voltage attack

CHAPTER 5

Application to CIGRE HVDC Benchmark Model

To demonstrate that these techniques can be applied to a general MTDC VSC HVDC system, the basic concepts were applied to the DCS1 20140630 model from the CIGRE B456 DC set of test systems [12]. This model has four isolated AC grids with four voltage source converters. The DC grid is designed such that there is one DC line to connect the two pairs of converters. The basic configuration of the system is shown in Figure 5.1.

Figure 5.1: Basic diagram of the DCS1 Released 20140630 model of the CIGRE B456 DC test systems

One single spoof attack was performed on the system and the detection methods developed in Chapter 4 were used. The attack performed on the system was spoofing the AC real power measurement on a single converter. The spoofed power was set to 0.5 pu, where the S_{bases} for this system is 200 MVA. The power was calculated using AC voltage and AC current measurements. This calculated value was then compared

to the measured AC power, which in this case was the spoofed AC power. If the error is at or close to zero, this would mean that the calculated and measured signals match, and the detector output suggests that there is no attack. The error signal is shown in Figure 5.1. This error reaches a peak of approximately 0.5 pu, which would be about 100 MW.

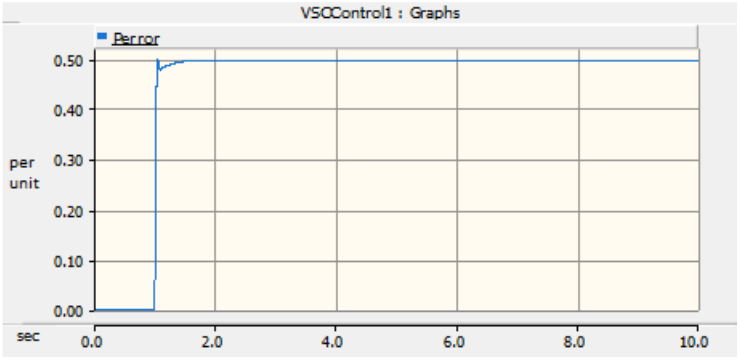

Figure 5.2: The error between the calculated real power and the measured spoofed AC real power signal for an AC real power spoof on the DCS1 20140630 model in the CIGRE B456 DC benchmark test systems

This model was chosen because it is a MTDC VSC HVDC transmission system in the CIGRE B456 DC test systems. This model also closely resembles the simulation model used for Chapters 3 and 4, but has a control system design that varies from the model used in Chapters 3 and 4.

CHAPTER 6

Detection Methods Based on Monitoring Signals

The methods developed in Chapter 4 are able to detect many cyber-attacks on measurements used by the control loop, but it is possible to craft attacks to fool these methods. This chapter presents some general purpose methods to detect attacks that are potentially harder to fool. One of the methods works best if the detection scheme has access to the M_d and M_q synchronous reference frame modulating variables from the current regulators.

6.1 Combined Attack on AC Voltage and AC Current Measurements

Figure 6.2 shows M_d and M_q at converter one during the simultaneous AC voltage and AC current spoof attack described in Section 4.2.1. It can be seen from the figure that M_d and M_q are oscillating between the saturation limits of 1 and -1. While saturation should be a clear indicator that the system is not operating as intended, an energy detector can be implemented to differentiate between an attack and an abnormal operating condition due to an AC or DC disturbance.

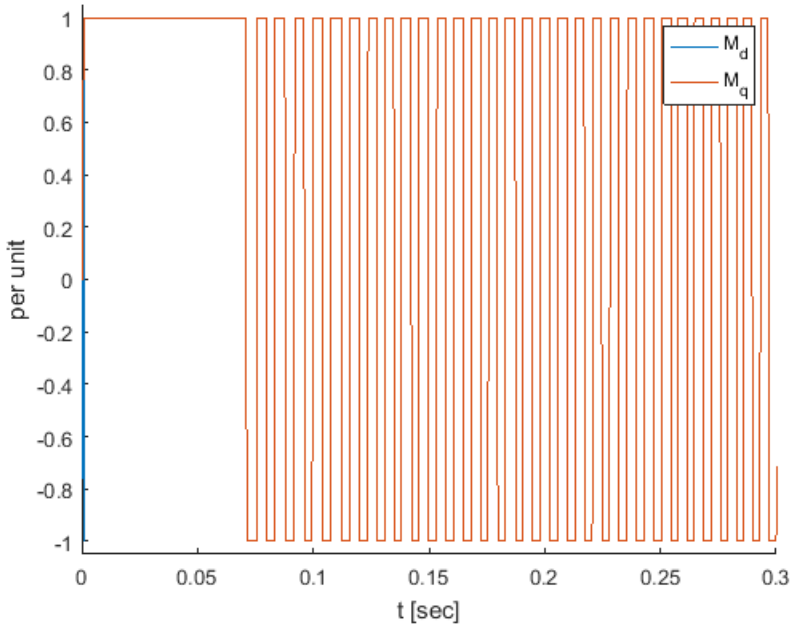

Figure 6.1: M_d and M_q during a simulation AC voltage and AC current measurement cyber-attack and converter one

6.2 Combined Attack on AC Current and AC Real Power Measurements

Revisiting the AC current and AC real power measurement spoof attack from Section 4.2.2, Figure 6.2 shows M_d and M_q at converter one during the attack. The figure shows that M_d is saturating. This is a clear indicator that the system is not operating as expected, as the system is designed such M_d and M_q should never saturate under normal operating conditions. Since abnormal conditions can cause similar behavior this does not give a clear idea of where the system is being attacked, but it does give a clear signal to the operator that the system is not under normal conditions.

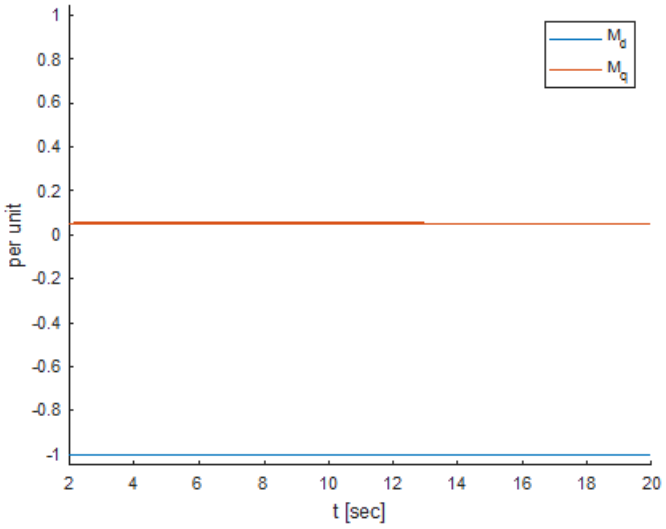

Figure 6.2: M_d and M_q during an AC current and AC real power measurement cyber-attack and converter one

6.3 Combined Attack on DC Voltage and DC Power Measurements

In one of the DC voltage and DC power measurement spoof attacks from Section 4.2.3, the DC voltage was set to 496 kV and the DC power measurement followed (4.10). Figure 6.3 shows M_d and M_q at converter one during that attack. It can be seen from the figure that M_d and M_q are oscillating back and forth between the saturation limits of 1 and -1. As stated earlier, while saturation should be a clear indicator that the system is not operating as intended, similar to the spoof attack on the AC voltage and AC current measurements, an energy detector could be implemented in this case to identify that the system is under attack or not operating as intended.

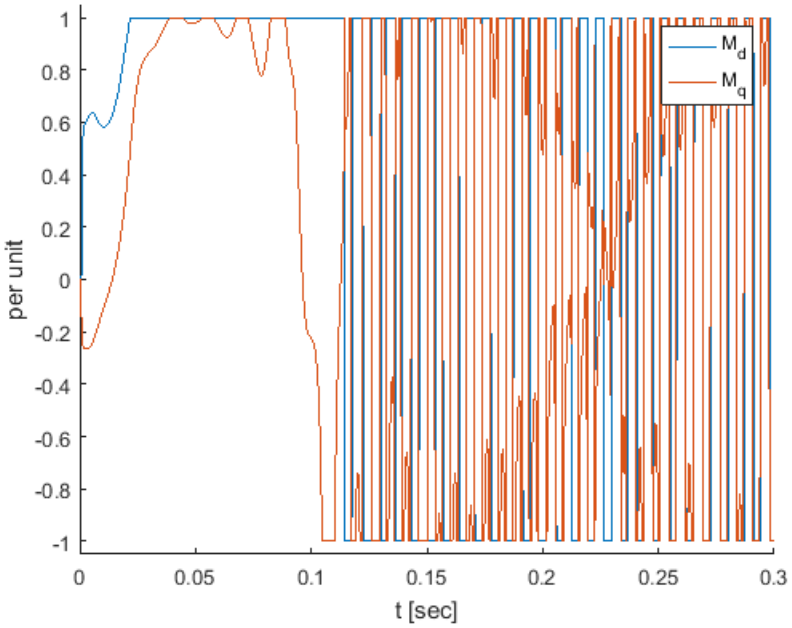

Figure 6.3: M_d and M_q during simultaneous DC voltage and DC power measurement cyber-attack and converter one

6.4 Combined Attack on AC Real Power and AC Voltage Measurements

For the AC real power and AC voltage double attack from Section 4.2.4, the modulating functions did not saturate, however the V_d signal that was spoofed to match the AC power and the AC current, was far above normal levels. Figure 6.4 shows V_d at converter one during the attack, note the vertical axis has is order of 10^{11}. It can be seen from the figure that V_d is far above the normal 147 kV. If the signals were monitored to check that they are within an expected range, the operator would be able to see that they system is not operating normally. The represents and addition measure that could be used for detecting attacks.

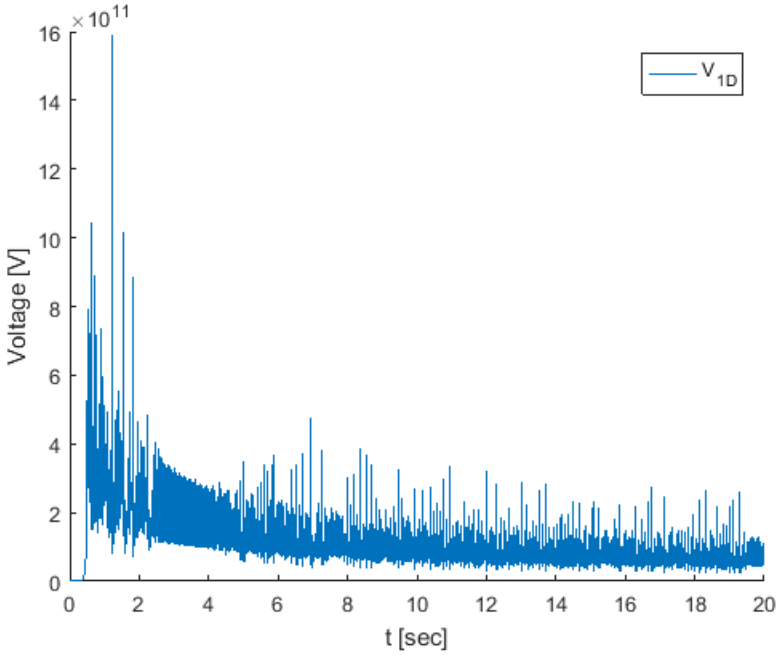

Figure 6.4: V_d for converter one during simultaneous AC real power and AC voltage measurement cyber-attack and converter one

CHAPTER 7

Control Response To Secure System Operation When an Attack is Detected

Detecting the attack is only the first step. An equally important step is the response to the detection. After a cyber-attack is detected the device(s) that are being tampered with should be taken off line and replaced. This is done by either switching out the controller or the measurement devices with secured back-up devices that would be on site and that use independent communication networks, as shown in Figure 7.1.

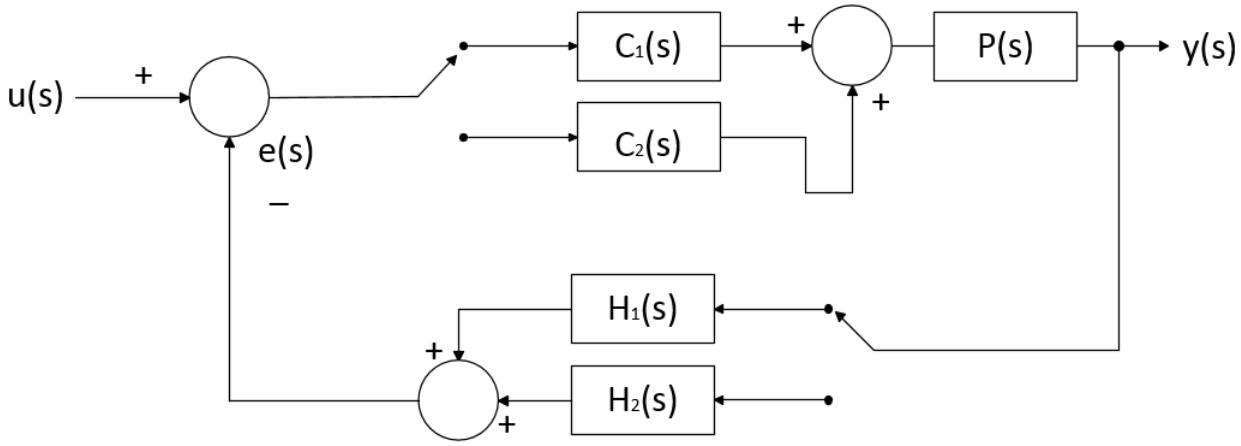

Figure 7.1: Response to Cyber-Attacks

In Figure 7.1, u(s) is the reference, C(s) is the controller, P(s) is the plant or in this case the HVDC system, y(s) is the output signal, H(s) is the sensor, and e(s) is the error between the reference and the measured output. This figure shows two switches. One is at the input to the controllers and the other is at the input to the sensors. These switches are there to represent that the sensors or controller may need to be taken off line and replaced if they are outputting incorrect values. The controller, $C_2(s)$, that replaces the original controller, $C_1(s)$, may have a slower response time as the system is operated more conservatively while being evaluated to determine

whether or not an actual attack is taking place and the extent of the attack. More research is needed in this area to determine when to respond to an attack and how effective this response is.

CHAPTER 8

Summary, Conclusion, and Future Work

8.1 Summary

MTDC VSC HVDC technology has advanced to allow several initial MTDC transmission grids to be built. HVDC systems allow for a more direct control of power flow and a longer transmission distance for underground cables when compared to AC systems. However, due to the technology involved with these systems, the potential for a malicious hacker to attack the system increases.

This thesis developed a simulation model of a point-to-point VSC HVDC transmission system and then built upon it to build a multiterminal VSC HVDC transmission system. Each system was demonstrated under normal operating conditions. Then several potential cyber-attacks on measured signals transmitted to the controller via a communication network were performed on the multiterminal VSC HVDC transmission system. Several types of attacks were performed which were chosen because of their potential impact on the system based on how it was controlled.

Methods to detect single or double cyber-attack on the system were developed and tested. These methods were also applied to the DCS1 Released 20140630 model from the set of CIGRE B456 DC test systems. It was shown that the principles of detection could be applied to different systems.

Alternatively, it was shown that the cyber-attacks could be detected using the modulating signals and the measured signals.

Once an attack was detected, the sensor and/or the controller should be switched out with a functional device to return the system to normal operation. Some basic concepts for this approach were presented.

8.2 Conclusion

Overall, this thesis demonstrated that cyber-attacks can be detected using calculations based on system measurements or signals. For the cyber-attacks that were performed on this system, all were able to be detected using at least one method discussed. This was done with several combinations of measurements, some utilizing basic circuit theory, and another using the modulation function outputs from the controller. These methods were shown to be able to apply to other MTDC VSC HVDC transmission systems using the DCS1 Released 20140630 model from the set of CIGRE B456 DC test systems. More research would need to be conducted in this area to apply the ideas explored in this thesis onto other MTDC VSC HVDC transmission systems.

This thesis also established a potential reaction to detected cyber-attacks. This response is to take sensors or the controller off line and replace them if they are compromised. More research is needed to determine criteria to switch controllers or measurement sources to reduce the impact of false positives.

8.3 Future Work

This thesis introduced methods to identify a set of single and double cyber-attacks along with a possible response to an attack detection that can be applied to multi-terminal VSC HVDC transmission systems. More research needs to be conducted to build upon these approaches. Future work that could be done includes:

1. Simulating and analyzing a more comprehensive set of cyber-threats. While different cyber-attacks were created, they do not cover much of the set of cyber-attacks that could happen. The type of attacks that cause the most impact to the system could differ based upon the system design and control.

2. Create a general purpose detection scheme combining the methods developed in Chapter 4 running in parallel. Develop criteria for setting thresholds to declare an attack is taking place and determine criteria for the number of samples exceeding the detection threshold in order to declare an attack.

3. Evaluate response of detection methods with measurement noise and present and evaluate the response during changes in system loading and in response to AC and DC transients and disturbances.

4. Test detection methods and response in real time. The cyber attacks and the detection used were performed at the same time with the same person acting as attacker and defender. Once the criteria for a threshold to declare an attack has been set, the system response should be tested in real time with the cyber-attack and detection roles played by different users.

5. Testing the methods for detecting cyber-attacks on a hardware implementation of the control system in a hardware-in-the-loop simulation environment. The cyber-attacks in this thesis were performed on a simulation of a system.

6. Build on detection methods introduced in Chapter 6. The expansion could include criteria for the decision to declare a cyber-attack is occurring versus a routine power system disturbance. This work could also detail how reaction time to the energy detector outputs would impact false detection frequency. The trade-offs between the impact of a failure to detect an attack and a false positive should also be studied.

7. Expand on the control response discussed in Chapter 7. Further testing of the effectiveness of this response is needed. Further research should also be put into when to switch out controller and the sensors. Possible considerations could be the length of the time window necessary to positively identify the attack,

the impact of false positives on system operation, and methods to insure the replacement controller and measurements are not compromised.

References

[1] G. Moore, *The Last Days of Night*. 1 ed., Random House, 2016.

[2] D. Jovcic, and K. Ahmed, *High Voltage Direct Current Transmission: Converters, System, and DC Grids*, Hoboken, NJ: John Wiley & Sons, pp.xi-11, 2015.

[3] H.A. Wheeler, (1942). 'Formulas for the Skin Effect'. *Proceedings of the IRE*. 30. 412 - 424. 10.1109/JRPROC.1942.232015.

[4] A. Yazdani, and R. Iravani, *Voltage-Sourced Converter in Power Systems: Modeling, Control, and Applications*, Hoboken, NJ: John Wiley & Sons, pp.4-53, 2010.

[5] A. Yazdani, and R. Iravani, *Voltage-Sourced Converter in Power Systems: Modeling, Control, and Applications*, Hoboken, NJ: John Wiley & Sons, pp.100-130, 2010.

[6] G. Hug, and J.A. Giampapa, (2012). "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, Vol. 3, No. 3, pp. 1362-1370. 2012

[7] S. Sridhar, and G. Manimaran, (2010, July). "Data integrity attacks and their impacts on SCADA control system." *Power and Energy Society General Meeting.* July 2010 IEEE pp. 1-6.

[8] Zhu, Bonnie, and Shankar Sastry. "SCADA-specific intrusion detection/prevention systems: a survey and taxonomy." Proceedings of the 1st Workshop on Secure Control Systems (SCS). Vol. 11. 2010.

[9] A. Yazdani, and R. Iravani, *Voltage-Sourced Converter in Power Systems: Modeling, Control, and Applications*, Hoboken, NJ: John Wiley & Sons, pp.334-384, 2010.

[10] A. Yazdani, and R. Iravani, *Voltage-Sourced Converter in Power Systems: Modeling, Control, and Applications*, Hoboken, NJ: John Wiley & Sons, pp.145-222, 2010.

[11] D. Jovcic, and K. Ahmed, *High Voltage Direct Current Transmission: Converters, System, and DC Grids*, Hoboken, NJ: John Wiley & Sons, pp.324-338, 2015.

[12] *CIGRE B4-57 working group developed models, PSCAD, https://hvdc.ca/knowledge-base/read,article/57/cigre-b4-57-working-group-developed-models/v:. Accessed 22 April 2018.*

[13] D. Jovcic, and K. Ahmed, *High Voltage Direct Current Transmission: Converters, System, and DC Grids*, Hoboken, NJ: John Wiley & Sons, pp.307-315, 2015.