Hierarchical Inference and Spoofing Alarm in HVDC Control Systems

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Electrical Engineering

in the

College of Graduate Studies

University of Idaho

by

John C. Bell

Major Professor: Dakota Roberson, Ph.D.

Committee Members: R. A. Borrelli, Ph.D.; Brian Johnson, Ph.D.

Department Administrator: Joe Law, Ph.D.

May 2020

Authorization to Submit Thesis

This thesis of John C. Bell, submitted for the degree of Master of Science with a Major in Electrical Engineering and titled "Hierarchical Inference and Spoofing Alarm in HVDC Control Systems," has been reviewed in final form. Permission, as indicated by the signatures and dates below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor:	Dakota Roberson, Ph.D.	Date
Committee Members:	R. A. Borrelli, Ph.D.	Date
	Brian Johnson, Ph.D.	Date
Department Administrator:	Joe Law, Ph.D.	Date

Abstract

The study of HVDC systems and cyber-attacks on their control systems can play an important role in the security and stability of large interconnected power systems. This work develops and analyzes a layer of security useful to detect and mitigate the negative impact of cyber-attacks directed towards high voltage direct current (HVDC) systems. It also identifies and categorizes potential attack types which may be harmful to power system operation if left unmitigated. Minimization of transients induced by remediation action are also addressed through the use of a classic control system technique: the bumpless transfer. Contained in this thesis is a summary of the testing performed on a HVDC cyber physical simulation environment, the performance of the security algorithms in terms of timing, detection rate, and relationship with false detection. Successful implementation of the approaches developed in this thesis can help allow the HVDC system to enhance resilience of the interconnected power system in the face of cyber-attacks.

Acknowledgements

I would like to thank my adviser, Dr. Roberson, for his continued commitment to his students, myself included. 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. Johnson for his help with my research, as well as the contributions to my thesis.

Finally, I would like to thank my wife, Cece, for her continued support and encouragement. I could not have done this without her.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

In 1954, a transmission line was needed to connect the island of Gotland and mainland Sweden. To meet the economic and technical challenges presented with this daunting task, the first successful installation of a high voltage direct current (HVDC) transmission line was introduced to the world [1]. Since then, more than 100 HVDC transmission lines have been installed around the world. While alternating current (AC) transmission lines make up the vast majority of lines operated worldwide, increasing advancements in power electronic technologies and digital controls have allowed direct current (DC) transmission lines to become more attractive than the conventional AC for certain transmission corridors which meet a specific set of criteria. These criteria include: long-distance bulk power delivery, asynchronous interconnections and long submarine cable crossings to name a few.

The last two decades have shown a renewed interest in HVDC technology, with the number of HVDC projects proposed or under construction steadily increasingly all across the globe. The decreasing cost and increasing capability of power electronic devices include advances in converter technology which has allowed for the increased possibility of a broader spectrum of applications [1] [2]. The broader spectrum for the new applications includes applications for underground, offshore wind generation, economic replacement of reliability-must-run generation, voltage stabilization and similar applications where AC options aren't as cost effective.

The added benefits of HVDC include supplying a commanded amount of power, quickly regulating that power (in comparison to AC voltage which depends upon the voltage magnitudes and phase angle differences between surrounding buses) and, as an approximate rule of thumb, proving more cost effective solutions for overhead transmission lengths longer than 500 km or for underground cables 50 km or longer. While the benefits of HVDC systems have increased, HVDC systems rely on measurements and communication within the converter station, between converter stations and the control center, to operate introducing surfaces that are vulnerable to cyber-attacks. The introduction of these new attack surfaces, therefore, will require engineers of the future to consider the possible vulnerabilities introduced, down to the control system level. This thesis will, therefore, discuss the design of HVDC control models to develop and test methods to detect cyber-attacks on HVDC transmission systems followed by proposing potential responses to these attacks [3].

1.1 Background Information

Popularity of AC transmission worldwide is due to the ease with which voltage levels can be changed. This is done with transformers which efficiently change the voltage and current levels by a certain amount,

dictated by the 'turns ratio'. The turns ratio has an inverse effect on the voltage and current levels. When the voltage is stepped up proportionally by the turns ratio, the current is stepped down. Transformers do experience power losses; they are, however, only a fraction of the losses that a power transmission line would lose if the voltage was not stepped up initially by the transformer. The power loss relationship can be seen in equation (1.1),

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

where P is power, I is current and R is equal to resistance. In order for a DC transmission line to be efficient, a transformer is used as the first step in the line. AC voltage is sent to a transformer to be stepped up and then that AC voltage is fed to a converter operating as a rectifier which changes the AC power into DC power. The newly converted DC power is then independent from the phase and frequency of the AC power supply. DC power is then transferred through a transmission line to an inverter that converts the power back to AC. The AC power at the receiving end is then ready to be injected into the network for utility use. In modern HVDC transmission systems there are two basic converter technologies. These converter technologies are known as line-commutated current source converters (LCC) and self-commutated voltage source converters (VSC). Figure 1.1 shows a HVDC converter station with a line-commutated current source converter and Figure 1.2 shows a HVDC converter station with a self-commutated voltage sourced converters [4].

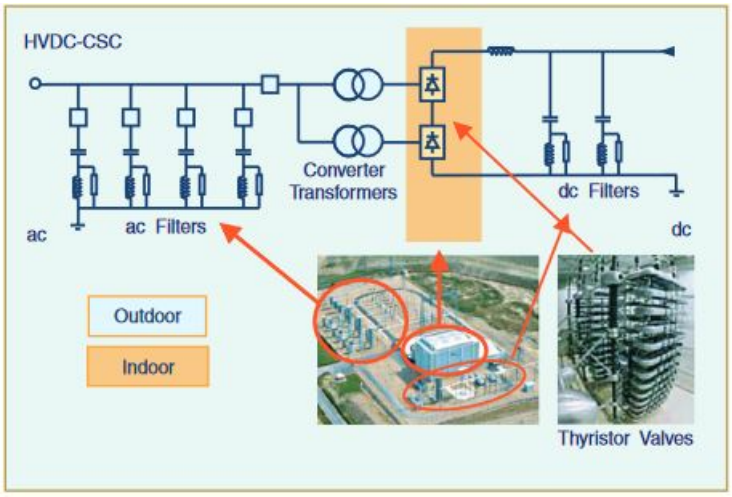

Figure 1.1: Conventional HVDC with current source converters [1].

LCC converters use thyristor-based converter technology and require a stiff AC voltage source in order to operate. The converter topology is based on the Graetz bridge. A Graetz bridge is a three-phase, full-

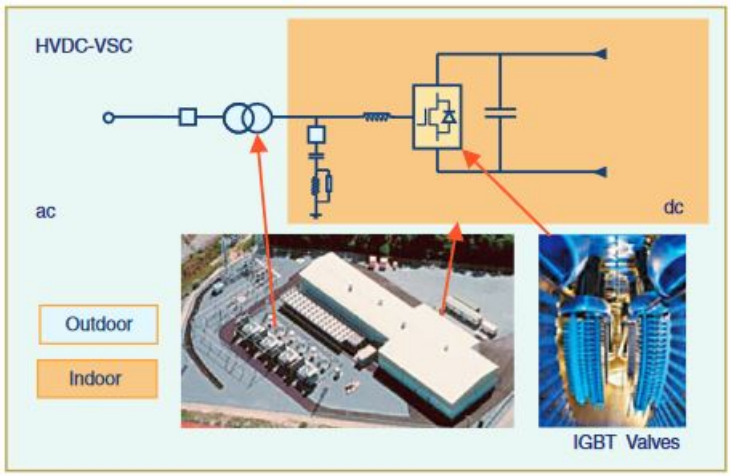

Figure 1.2: HVDC with voltage source converters [1].

wave bridge that includes six switching operations per period which results in a characteristic harmonic ripple of six times the fundamental frequency in the DC output voltage. There is one thyristor valve for each pulse in the Graetz bridge with six total with each valve having a select number of connected thyristors in series to achieve the necessary DC voltage. The thyristor in the line allows current to conduct until the current tries to reverse its direction at which point it will turn off and not allow any current to flow past that point. Thyristors require an AC voltage source to allow for them to act as an inverter which makes them perfect for AC voltage systems. LCC-HVDC systems are widely used in utility applications today, however they are limited for a number of reasons. The limitations are founded in the LCC technology which consumes reactive power, is sensitive to the strength of the AC system near the inverter, and produces low order AC and DC harmonics which require physically large AC and DC harmonic filters. The strength of the AC system is measured using the short circuit MVA of the connect AC system divided by the real power rating of the HVDC system. To overcome a number of these limitations, voltage sourced converter HVDC systems were developed in parallel by several manufacturers [1] [2] [5].

The first commercial application of VSC HVDC transmission went under the trade name HVDC Light [1]. The first project to utilize HVDC Light was the experimental Hellsjon project at ± 10 KV. The initial implementations for HVDC Light used two level voltage source converters with low frequency pulse-width modulation (PWM). VSC-HVDC systems were developed to overcome the limitations of LCC-HVDC systems for off-shore wind applications. The benefits of VSC-HVDC include improved voltage stability, more flexibility in location and rating for adding taps for new converter terminals, and power flow direction can be reversed by reversing direction of current flow instead of reversing voltage polarity. Newer

systems use self-commutated insulated gate bipolar transistor (IGBT) valves and require no reactive power compensation. If the DC line is connected in a symmetric monopole configuration the converter stations can use standard transformers and are more compact than the previously discussed LCC HVDC systems due to reduced filtering requirements. VSC HVDC systems that use bipole configurations or asymmetric monopoles require custom transformers similar to to LCC HVDC. With the many advantages of VSC HVDC, they are growing in popularity for the new wave of systems in remotely located wind and PV (photovoltaic) systems, and in tradition HVDC niches like underground and sea cable transmission, weak systems, and off-shore platforms [1].

While the usage of HVDC transmission systems have increased globally, modern high-speed digital electronics and sensory equipment have been developed simultaneously to fit the needs of these systems leading to increased flexibility in the performance of HVDC transmission systems. While some of the electronics have been developed simultaneously, much of the sensory and control infrastructure throughout the AC grid has not been updated as consistently as those of HVDC systems. In view of the fact that HVDC systems are embedded in AC power systems, they are vulnerable to cyber-attacks that penetrate the attack surface of the AC system. Attackers who successfully penetrate the defenses of the communication system for the AC grid can potentially penetrate the control and measurement system for a HVDC system. A number of additional changes in the power system industry have aided in creating a further complex dynamic to the sensory and situational awareness framework. Examples include wide area measurement systems (WAMS) and a growing mixture of governing bodies responsible for electricity generation and transmission. WAMS provide data sets useful for real-time monitoring and post-event analysis yet result in further hardware and networking protocols. The National Energy Policy Act (NEPA) of 1992 allowed for a mixture of individual transmission and generation owners, independent system operaters (ISOs), regional transmission operators (RTOs), and dozens of balancing authorities (BAs) to share in the generation and transmission of electricity resulting in a shared charge to secure all communication between each piece of equipment and each relevant party. As policies change and technology evolves, the need for additional research into every facet of cyber-security grows.

The number of possible threat vectors continues to rise as the evolution of technology in power grids increases resulting in a need for cyber-security research. Reference attacks (otherwise known as false data injection attacks) modify stored or transmitted data and can be directed against the SCADA remote terminal units (RTUs). The state estimation schemes commonly used in AC transmission control centers use static (also known as DC) approaches which are known to be susceptible to these types of attacks. Anomaly detection is a method for finding false data attacks in a system. This form of detection does not watch for the known intrusion signals rather it searches for abnormalities in the observed data

and triggers an alert when something outside the acceptable range is noticed. The acceptable range is set by identifying a normal deviation from the system's nominal behavior. This method is based in learning the usual behavior of the system over time [6].

The evolving infrastructure of the transmission and distribution system utilizing new technologies combined with the changing grid policies requires a new look at the operation of the power grid and redesign of the infrastructure. The authors of [7] discuss the limiting features for real-time stability control and the advances needed to make this feasible given the appropriate communication infrastructure. The limiting features presented include decentralized controls, and small signal instability.

The authors in [3] clarify that grid resiliency can be enhanced using the security of HVDC systems and discuss research that can improve the security of HVDC systems. High-level detection techniques are a necessity to ensure nominal operation of HVDC operation. The required detection needs to be independent of the AC system and associated devices to ensure that the hardware-level switching action is consistent with the action commanded by remote sensors and converter station communication equipment.

This thesis focuses on VSC HVDC technology and using anomaly detection to detect cyber-attacks impacting the converter control loops. It is proposed that when a detection occurs, the HVDC power-flow controller will be reconfigured to ensure lasting stability and safety while retaining the maximum amount of functionality allowing the HVDC converter to enhance resilience of the interconnected power system. The implementation of a bumpless transfer will be analyzed as a potential reaction to combat cyber-attacks, by taking sensors or the controller off line and replacing them if they are compromised.

1.2 Literature Review

The study of HVDC systems and cyber-attacks on their control systems is a relatively new area of study due to the fact that the realization that there are threats has developed recently. The following overview samples the broad categories of work which have been done to this end and the conclusions that have been drawn prior to this work. A MSEE thesis and a related paper titled "Potential Cyber-Attack Detection and Mitigation Techniques for Multi-terminal Direct Current (MTDC) VSC HVDC Systems" [8] concluded that with the advent of large VSC based MTDC transmission systems using measurements transmitted over internet protocol networks, the potential for a malicious hacker to attack these systems increases. The paper discussed a variety of attacks that used a combination of spoofed AC voltage, AC current, AC real power, DC power and DC voltage measurements. It was demonstrated in this paper that the potential cyber-attacks could be detected using the modulating and measurement signals or using calculations based on system measurements or signals. This paper discussed a potential reaction to detect cyber-attacks, by taking sensors or the controller off line and replacing them if they are compromised.

However, it was not discussed further and was stated that more research needed to be conducted in that area [4].

An IEEE publication titled "Improving Grid Resilience Using High-Voltage DC" found that recently developed HVDC technology could improve grid resilience as it is implemented into the power system. It was found that through efficient bulk power delivery and active power modulation, HVDC transmission allows an increase in stability and resilience of the modern power systems. However, it was noted that while adding resilience to the grid, HVDC simultaneously adds vulnerabilities in the form of cyber-security risks and failing to address the full extent of cyber-security concerns could lead to negatively impacting utility operations, cost by forced downtime and potential destabilizing of otherwise stable interconnections. An investment in smart controls in all aspects was the first suggest step in combating the arising issues [3].

The authors of "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy" explore the lack of cyber-security protocols in terms of supervisory control and data acquisition systems (SCADA) at the time the paper was written. Including information technology (IT) intrusion detection techniques to suit the needs of SCADA is a daunting task. Anomaly detection is introduced to fill the voids in SCADA systems. Anomaly detection does not watch for the known intrusion signals rather it searches for abnormalities in the observed data and sends an alert when something unusual is noticed. It is based in learning the usual behavior of the system over time. An acceptable range is set by identifying a normal deviation from the system's usual behavior. The difficult with this approach is developing a window that avoids false alarms while escaping false negatives [6].

The authors of "Designing the Next Generation of Real-Time Control, Communication and Computations for Large Power Systems" demonstrated the evolving infrastructure of the transmission and distribution systems utilizing new technologies that have been developed. The changing grid both in policy and technology required a new look at the operation of the power grid and redesign of the infrastructure. A system with flexibility and functionality was proposed showing promise, however the downfalls were inevitable. This system did not lend itself to analysis and performance. The ultimate goal for the real-time control, communication and computation scheme was to control the dynamics directly without having to set special protection parameters. This goal was unrealized due to a poor understanding of the complex math behind real-time control [7].

The authors of "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks" established that the evolution of smart power grids led to an increase in the cyber-part of electric power systems which in turn leads to an escalation in the number of possible threat vectors for false data attacks. AC systems have been an area of study in vulnerability assessment for quite some

time [9].

The authors of "Data Integrity Attacks and Their Impacts on SCADA Control System" demonstrated data integrity attacks that are accomplished through manipulating sensor or control signals and are an area of growing concern for SCADA networks. Data integrity attacks not within an acceptable range don't pose as great a threat as an attack within an acceptable range that could be missed by an operator. More importantly, such attacks can be designed to defeat the bad data detectors used with state estimation software [10].

The authors of "Variable Loop Gain Using Excessive Regeneration Detection for a Delayed Wide-Area Control System" discussed how Wide-Area Damping Controllers (WADCs) are required for stabilization of large interconnected grids with separate generating and load centers. Any time delay in WADCs is of concern to the stability and performance of the system engaging the WADC. High traffic, cyber-attacks, and GPS spoofing are all forms in which the network can be congested and a time delay created. To combat such time delays, an excessive regeneration detector (ERD) methodology was presented to provide stability due to any delays in the WADC systems [11].

The authors of "Almost Output Regulation Bumpless Transfer Control for Switched Linear Systems" discussed the problem of almost output regulation bumpless transfer control for switched linear systems. A switched system is a hybrid system expressed by a family of subsystems and a rule, which is usually named as a switching law determining the active time and order of the subsystems. Unsuitable switching designs may bring undesirable transient behaviors, which are named as bumps. The bumps are introduced to the system by the discontinuities of the control input of a switched at the switching instants. These bumps cause trouble to the system including damage of the equipment, degradation of performance, and even instability of switched systems. Bumpless transfers suppress those transient behaviors caused by the switching [12]. The authors of "An Improved Anti-windup Bumpless Transfer Structures Design for Controllers Switching" discussed a new kind of control structure proposed for switching different controllers smoothly in a unified framework. It was demonstrated that the H_2/H_∞ performance, pole constraint, and passivity of the closed loop systems can be preserved through controller switching [13].

Demonstrated throughout this section is that the study of HVDC systems and cyber-attacks on their control systems is a relatively new area of study due to the fact that the advances in this field have been developed recently and the HVDC scheme inherits the cyber-security vulnerabilities of the AC systems that they are connected to. Some work has been done in developing a potential cyber-attack detection technique for HVDC systems. Potential cyber-attacks were able to be detected by using modulating and measurement signals using calculations based on system measurements. Further research is needed to create a detection scheme combining criteria for thresholds and number of samples exceeding the

threshold to confirm an attack. Testing detection methods in real time while an attack takes place to confirm the efficiency of the system and trying to build in a control response when a detection takes place.

1.3 HVDC Technology Applications

As stated previously, the characteristics of HVDC technology make it especially sought after in certain transmission applications. The most well known application is for long-distance transmission; however, HVDC transmission is useful when considering bulk-power delivery, asynchronous interconnections and long underground or submarine cable crossings. The rationale for choosing HVDC transmission is many times economic, but there are instances when there are other reasons for selection.

Dynamic reactive compensation can become costly and because of them DC lines have historically been assumed to become more cost effective after about 600-800km [4]. As stated in [2], HVDC may be the only feasible way to interconnect two asynchronous networks, or to reduce fault currents, utilize long cable circuits, bypass network congestion, share utility rights-of-way without degradation of reliability and mitigate environmental concerns. In all of these applications, HVDC complements the AC transmission system.

HVDC transmission systems are able to transmit more power (than AC systems) over long distances due to the electric and magnetic fields of the lines. AC lines require charging twice every cycle while DC lines need to only be charged once. The charging current for these lines increases as the length of the line increases. The charging current continues to increase which leads to a need for reactive compensation in order to increase the amount of power that can be transferred. Under DC operation, capacitance behaves as an open circuit in steady-state allowing the DC line to operate in steady-state without a charging current once it has been already charged to the operational level. This process allows for the DC line to transmit current up to the thermal rating of the line without being hampered by the charging current.

HVDC transmission systems provide a controllability and asynchronous nature that provides a number of advantages for applications. Interconnections can be made between asynchronous networks allowing for a buffer between the two systems in some cases using back-to-back converters with no transmission line. The asynchronous link acts as an effective firewall against propagation of cascading outages from one network to the next [2]. Electric grids which are AC transmission constrained for various geopolitical and economic reasons may also utilize HVDC-enabled wide-area damping control systems to help retain stability in the presence of lightly-damped oscillatory dynamics [14].

Chapter 2: Cyber-Attack Methods on Power Systems

2.1 Methods

Threat of cyber-attacks worldwide has dramatically increased simultaneously with the increase in the cyber-enabled portions of electric power systems. The electric utility industry is undergoing a significant transition to digital hardware and microcontroller-based applications. The increased possibility of cyber-attacks has created a field of research related to the preparation and mitigation of such threats. This research into cyber-attacks warrants focus on two main types of attacks: reference attacks and initialization attacks.

Reference attacks are, in simple terms, an attack that occurs when stored or transmitted data is *modified* during an ongoing cyber-attack. Control system inputs or 'reference' values can be changed arbitrarily, or measurements spoofed. Reference values of concern in this thesis include, but are not limited to: AC system voltage, AC current, AC real power and DC voltage. There is an ever-increasing number of possible threat vectors for reference attacks.

The second type of attack which is of great concern are known as initialization attacks. These attacks change the *basic configuration* of the hardware or the controller inside the power system under attack. Due to the complexity of the controllers and hardware, these attacks can be more destructive than the previously mentioned reference attacks. Both categories of cyber-attacks must to be addressed, however, and potential solutions put forth to prevent large-scale power system failure.

2.2 SCADA Attacks and Vulnerabilities

Supervisory control and data acquisition (SCADA) and associated networks are typically the conduit through which the collected data flows while regularly informing the HVDC system on operating conditions and changes on the connected AC system. SCADA systems are connected through the internet and therefore now face the threat of cyber-attacks [3]. Conventional information technology intrusion detection techniques cannot be used to detect attacks on SCADA due to the original designs and consequent lack of cyber security [6]. (Some SCADA specific systems have been developed in the ten years since [6] was written.)

Due to the communication between SCADA and HVDC systems and the large number of potential threat vectors to SCADA systems, HVDC systems have consequently become vulnerable. HVDC

converter stations that use IEC 61850 sampled values to connect sensors to the converter controls are vulnerable if attackers penetrate the station's cyber perimeter. SCADA systems and sample-value based converter station systems are vulnerable to both reference and initialization attacks due to the SCADA network traffic being unauthenticated as a result of constraints on computation and communication [3] [6].

One of greatest threats to a large scale power system stability can come from a successful attack on an operational WADC. The bandwidth of a functioning WADC lies in the range of frequencies from $\omega_b \in [1.0, 4.0]$ Hz and the controller is expected to have a normally large power flow modulation within that frequency range. The normally large power flow modulation creates devastating issues when trying to detect attacks. This report does not dive into the WADC systems but it can be noted that the simplistic detection methods currently in use would not be able to detect destabilizing power flows of potentially devastating amplitude and therefore, the system response itself must be investigated for trends toward instability to halt destabilizing actuation [11].

Chapter 3: Control System Architecture

3.1 Control System Configuration

VSC HVDC transmission uses a technology able to control both the active and reactive power to the AC system independently of each other. The reactive power is controlled at each terminal independent of the DC transmission voltage level and power transfer level allowing flexibility to place converters anywhere in the AC network. The converters themselves have no reactive power demand and use that flexibility to regulate the AC system voltage like a generator. VSC HVDC has the ability to operate in all four quadrants on the AC side due to the ability the converters have in controlling the phase angle and magnitude of the fundamental component of the converter voltage. The first VSCs used in HVDC applications were two-level or three-level and used pulse width modulation (PWM) techniques with low switching frequencies at about 1 kHz limited by the available power electronic devices. Pulse width modulation has various techniques but, in the case used in this work, it compares a high-frequency periodic triangular waveform and the carrier signal against a modulating signal. The intersections between the carrier and the modulating signal will determine the switching instants of two input signals [5] [15] [16].

The two-level VSCs are built using three single phase half bridges connected to a common DC line. Each phase leg includes an upper and a lower switch cell, which are fully controllable, unidirectional switches. Both the upper and lower switches have an anti-parallel connection with a diode. This configuration allows for a reverse-conducting switch. As VSC technology continued to improve, different configurations began to emerge.

The most recent VSC schemes use modular multilevel converter (MCC) configurations. MCC technology connect hundreds of standardized modules in series. This configuration has lower losses, modularity, scalability and lower harmonic content in the output AC voltage when compared to the previous two-level converters. In addition to the advantages discussed above, VSC HVDC schemes have the ability to work with weak AC systems, can't experience commutation failures as happens with LCC within the converter, and can more easily be configured and controlled as multiterminal of direct current systems.

Multiterminal HVDC (MTDC) systems have become a growing force in the academic research community because systems with more than three terminals can be controlled without total dependence on communication between each terminal. Communication would still be used to enhance performance. More importantly, VSC technology allows each converter to be reverse direction of power flow without manual switching of the network. This technology has made it possible for widespread multiterminal

systems to become a reality in the coming decade. The concepts for control schemes presented in the literature for MTDC has changed over the past thirty years, and there has been two main appraoches presented. One approach uses a master controller to determine power setpoints for each converter and set appropriate DC voltage setpoints to support that power flow. The control of reactive power was placed within the control system of each terminal [16].

The master controller based schemes are highly dependent on communication links. The second approach for MTDC systems came most recently and uses a coordinated control concept based on voltage droop developed for industrial DC systems in middle of the last century. The DC voltage control is generally assigned to one particular terminal while each of the remaining terminals controls its own power flow. This type of system utilizes a voltage droop control to account for the changes in DC voltage caused by changing power flow. Such schemes still have a master controller to improve performance but are able to operate with temporary communication loss. MTDC systems can potentially reduce costs, allow for the input and output power to be controlled flexibly for an increase in total power transportation capacity and facilitate the gradual expansion of distributed networks with the addition of additional converter terminals over time [15].

The basic controller system architecture used in this thesis is in Figure 3.1. The HVDC power error command signal $e[n]$ is usually presented in the literature as regulated using a proportional-integral type controller [5]. This compensated actuation command signal controls the power electronic equipment ultimately responsible for HVDC line flow. If compromised, the control system in this detection and remediation framework switches to an air-gapped 'Standby' unit using the proceeding 'Detector' methodology while informing the operator and any other supervisory control systems that a cyber-attack or other operational issue is underway. The air-gapped 'Standby' unit is disconnected from the network to ensure that measurements or commands from the compromised network are not able to penetrate the 'Standby' unit.

3.2 Detection

Anomaly detection can readily detect some forms of cyber-attacks. Attacks which result in obvious outlier actuator command signals or exaggerated actuator saturation when compared to nominal operating conditions are those most easily detected [8]. To ensure that cyber-attacks of all types can be discovered, filtered energy detection is also applied along with observable saturation and outlier detection. Cyber-security intrusion is also indicated by increases in aggregate energy at particular frequencies. Detection methods are developed to ensure secure operation of the MTDC converters in these situations. However, as discussed in previous sections, some attacks can come in more subtle forms. Systems

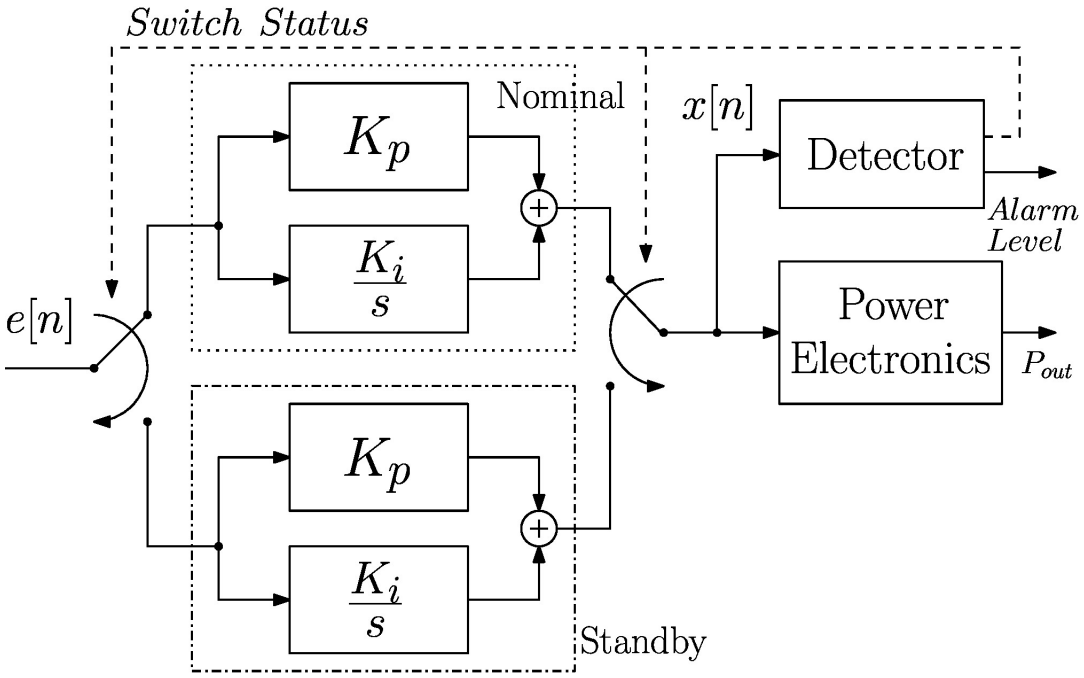

Figure 3.1: Basic controller architecture, including both nominal and standby controllers.

equipped with WADC are susceptible to even the most subtle of attacks and can result in system-wide failures. The control system and air-gapped detection mechanism replaces the compromised equipment for a controller on an isolated network to avoid catastrophic misoperation of sensitive HVDC equipment [14].

Due to the flexibility of the energy detector, very few assumptions are necessary for adequate probability of detection which ensures that the detector is capable of perceiving both obvious and not obvious attacks, regardless of the origin. The algorithm developed here is described first with the underlying theory used to detect operational change (as a function of cyber-security intrusion or equipment malfunction), emphasizing the variables with the highest sensitivity and importance in the detection scheme. Layering the basic detection scheme while varying detection window length, threshold, and alarm type provides a tiered response which keeps operational functionality at the design's forefront. Basic concepts for understanding detection thresholds for a fixed probability of false alarm (P_{fa}) is presented for a simple case, but can be expanded in future work.

The Neyman-Pearson test suitable for the detection of a broadband spectral energy change assumes the model

$$\begin{aligned} H_0 &: x[n] = w[n], \\ H_1 &: x[n] = s[n] + w[n], \qquad n = 0, 1, ..., (N-1), \end{aligned} \tag{3.1}$$

where H_0 is the *null* hypothesis, H_1 the *alternative* hypothesis, $w[n]$ zero-mean Gaussian noise with covariance matrix C_X, and N the record length of the data. Thus, the presence of (or lack thereof) $s[n]$ is the condition to be detected. Shorthand notation for the N-point data set of observed data is to let $\boldsymbol{x} = \{x[0], x[1], \ldots, x[N-1]\}$, where $\boldsymbol{x}$ is a vector of length N. To claim null hypothesis acceptance or rejection, a function referred to as the *test statistic* $T(\boldsymbol{x}) = T(x[0], x[1], \ldots, x[N-1])$ maps the observed data set and compares it to threshold γ. For conditions where $T(\boldsymbol{x})$ exceeds the threshold, the null is rejected, i.e. the alternative is accepted. Conversely, when the threshold exceeds the test statistic with the addition of s[n], the null is accepted.

A *hypothesis test*, as described in the previous paragraph poses the null hypothesis is either accepted or rejected based on a test statistic that is developed and compared to a threshold value. When the null is rejected, it is because the test statistic was greater than the threshold (and vice versa). This particular test asks the questions:

- How is a meaningful test statistic developed?
- How is the threshold calculated?
- What impact does the threshold have on the detectors performance?

Considering the system, a natural test statistic was defined as "the amount of energy" in a signal compared to the "expected amount of energy". For this model, it was reasonable to assume that the signal will be Gaussian distributed noise with a variance θ_s^2, without loss of generality, and the noise term w[n] is assumed Gaussian, as well, but with variance θ^2. The two signals are statistically independent.

The "energy detector", as described by Kay [17], is indicated here and implemented using the test statistic $T(x)$. The test statistic is derived using the ratio of log-likelihoods under the null and alternative hypothesis.

$$T(\boldsymbol{x}) = \sum_{n=0}^{N-1} x^2[n] > \gamma \tag{3.2}$$

Test statistic $T(\boldsymbol{x})$ is the scaled sample variance of the data set $\boldsymbol{x}$. A comparison of the scaled sample variance of the signal to a threshold, γ, is therefore the hypothesis test. Threshold γ is chosen based on a chosen P_{fa}. The test statistic assesses the energy of the signal. When an attack or malfunction is present, s[n] is detected as 'present' and the energy of the observed signal should be approximately equal to the sum of the two variances $\theta_s^2 + \theta^2$. If the signal s[n] is not present, then the energy of the observed signal should be approximately equal to just θ^2. To produce the most accurate detector it is necessary to pick a threshold that lies between the two true values. Choosing a threshold arbitrarily gives

the probability of false alarms. A carefully-chosen threshold is helpful in illustrating the probability of the detector incorrectly identifying an exogenous signal (i.e. 'False Alarm') while giving insight to the inherent trade-off between false alarms, misses, and true detection.

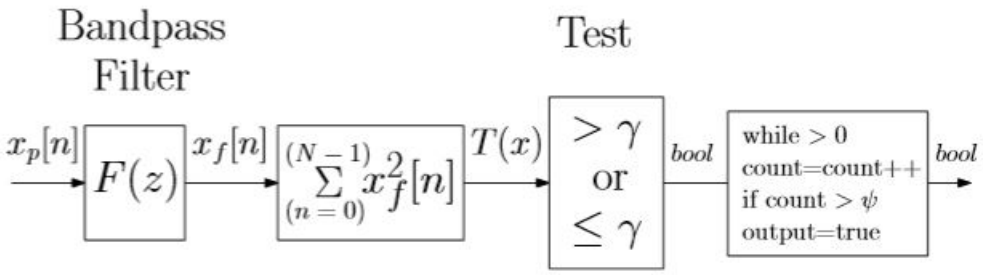

Figure 3.2: Block diagram of test statistic generation logic.

Prefiltering signal x_p with filter $F(z)$ changes the spectral content of the signal under test, x_f, and builds in flexibility in order to 'search' specific frequency bands for content, as in Figure 3.2. Other (nonlinear) operations can be employed as post-processing measures to reduce false alarms (trading off time-to-detect), and form the basis for a layered response.

3.3 Layered Response

When exploring detection methods for a system that faces a malicious cyber-attack it is important to up front understand the operational characteristics of the system so that the detection method might resolve the attack in the most effective way possible with the least damage to the system. In the following, a detection sequence for cyber-attacks is explored, ensuring that those pieces maintain a hierarchical configuration to ensure prioritization of operational considerations.

Overburdening real-time operations with unnecessary false alarms while ensuring no threats are left undetected is the top of the hierarchical configuration. To ensure that the highest goal of the hierarchical configuration is fulfilled, a three-stage detection and remediation design is employed. The fastest, most responsive stage is used to minimize the time-to-detection and begin an 'inquiry', while incurring more false alarms by inferring an aggregate increase in energy in an identified frequency range to indicate malfunction or cyber-security intrusion.

System operators and their respective responses to a cyber-attack detection demonstrates the trade-off between a high and low threshold. High thresholds have the possibility of missing a malicious cyber-attack, while low thresholds can create an overburdening of false alarms for the system operator. If a system operator has a drastic response to any detection alarm that requires time or money spent, a low threshold

that has the possibility of triggering many false alarms would not provide a worthwhile detection system.

To combat this problem, the following layered detection and response is proposed. An alarm is provided only if the detection algorithm is sufficiently confident in the presence of a noteworthy abnormality within the system's operations. This proposal requires hours of research and testing to find the most confident threshold that sounds the alarm when needed yet strays from an overbearing number of false alarms. However, once the threshold is chosen, it provides a rapid and (potentially) automatic response to the threat while minimizing redundant data provided to an operator already inundated with data.

Due to the variance of the moving average energy estimate, i.e. variance of the variance estimate, is inversely proportional to data set length N, a longer data window has a smoothing effect on this estimate. While smoothing provides a more accurate measure of variance, detection is delayed in time as N increases. Therefore, the design of the 'Detector' block in Figure 3.1 considers data set length timescales on three orders-of-magnitude: hundreds of milliseconds, seconds, and tens-of-seconds. These time constants are used to separate actions to be taken in the event of a cyber-attack:

1. Alarm,
2. Inform,
3. Switch.

Subscripts in Figure 3.3 correspond to the above three actions. The multi-stage inference method utilizes three parallel detection branches of varying window length and a comparative analysis between the different results recorded by the three separate branches to determine the appropriate "alertness level". Escalation which reconfigures the controller switch status only occurs upon consensus of all three detector stages.

The basic form of the detector described is instantiated three separate times in layers L_s, L_i, and L_a shown in Figure 3.3, varying the length of the sampled data N and threshold γ to achieve the detection goals necessary to inform the alertness level. By using a short data set $\boldsymbol{x}$, i.e., window length, in the "Alarm" stage rapid detection is possible. Upon detection, however, the operator is not yet to be informed; instead, a longer variance window in the "Inform" stage is analyzed for similar information, filling a longer variance window to determine if the event detected by the shorter window has inferred a legitimate event or simply a false alarm. The "Inform" stage is the first layer that performs an action to alert the operator of an attack. This poses the question of "Why have the first 'alarm' stage if it doesn't serve a purpose in alerting the operator of the attack?" The alarm level is used primarily for recording and logging data for offline and post-attack analysis. The analysis of the data recorded by the alarm level

can demonstrate the quick detection of the detector and provide patterns and data that prove crucial in adjusting thresholds or the length of the sampled data windows for continued optimization of the energy detector. The second and third stage data is all logged for offline analysis. Consistent with the trade-off previously noted, detection is delayed proportional to relative window length but resulting in a more trustworthy result than with the shorter window length.

The operator, in this case, may be informed on the possibility of an attack that is underway, in addition to other supervisory equipment which may be initialized and put on standby. In the case of a WADC-equipped HVDC system, this output may be used to inform a gain reduction algorithm, as in [11], to ensure overall system stability is not compromised.

Modifying the "switch status" output requires additional validation that an attack is indeed underway, as this will trigger significant post-event analysis and investigation into the event. Thus, a third and final stage with a correspondingly longer window is used to validate or reject the previous detectors' inferences. Only when the individual stages are in agreement is the change-out of controllers, referenced in Section 3.5, allowed to take place.

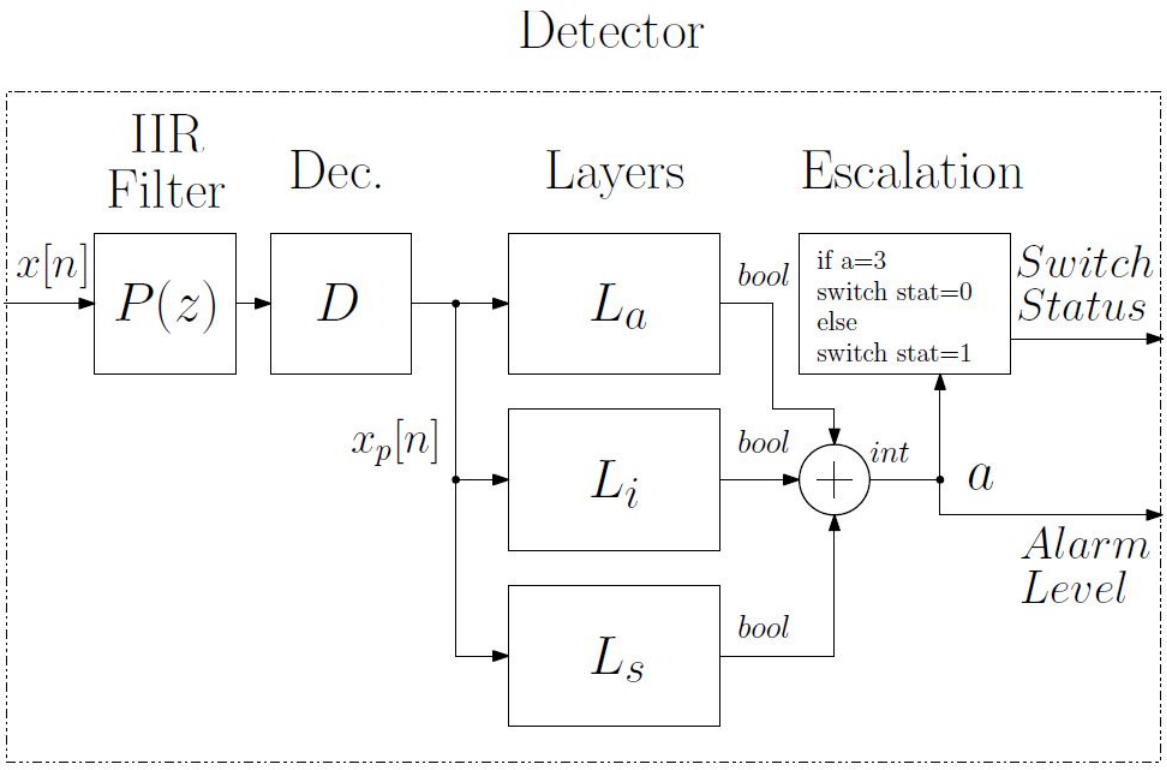

Figure 3.3: Internal block diagram of "Detector" sub-block of Fig. 3.1.

For online fine tuning of the algorithm, only aggregated single-point detections accrued over a pre-

determined amount of time are passed through to the alarm/inform/switch logic output. Logic circuits initiate a counter once timer threshold ψ is exceeded, counting additional detections until the requisite number is achieved. Otherwise, the logic resets the detection counter and the previous detections are considered anomalous. This has the added benefit of allowing a minor threshold reduction without notably increasing P_{fa}, quickening detection slightly.

3.4 Threshold Calculations

A basic discussion of the underlying statistics show how in-the-field tuning parameters' performance impact performance and helps choose a threshold given a P_{fa} chosen *a priori*. It's also useful for analyzing iterative design parameters used in detection. If the detector behaves outside of regular operation, sensitivities uncovered here lend insight into the parameters which may be the cause. Calculating the threshold requires an understanding of the test statistic, where the distributions of $T(\boldsymbol{x})$ under each hypothesis are determined analytically.

As described in Section 3.2, traditional energy detection assumes a white Gaussian noise (WGN) random process signal model with variance σ_s^2, where noise $w[n]$ is also a WGN random process with variance σ^2, statistically independent of $s[n]$. Distributions of the test statistic under each hypothesis are derived in full in [17] and are contained in Eq. (3.3)

$$\begin{aligned} \frac{T(\boldsymbol{x})}{\sigma^2+\sigma_s^2} &\sim \chi_N^2, \quad \text{under } H_1 \\ \frac{T(\boldsymbol{x})}{\sigma^2} &\sim \chi_N^2, \quad \text{under } H_0, \end{aligned} \tag{3.3}$$

where $\sim$ reads 'is distributed as' and χ_N^2 is the central Chi-squared distribution with N degrees of freedom. From these distributions, γ is calculated using the classical statistical $\mathcal{Q}$ function, where $\mathcal{Q}_K(\gamma) = \int_\gamma^\infty f_K(k)dk$, where $f_K(k)$ is the PDF of the random variable (RV) K. Identifying an acceptable probability of false alarm P_{fa} *a priori* facilitates the calculation of threshold γ using the relationship

$$\begin{aligned} P_{fa} &= pr\left\{T(\boldsymbol{x}) > \gamma; H_0\right\} \\ &= \mathcal{Q}_{\chi_N^2}\left(\frac{\gamma}{\sigma}\right) \end{aligned} \tag{3.4}$$

where $\mathcal{Q}_{\chi_N^2}\left(\frac{\gamma}{\sigma}\right)$. indicates the integral from γ/σ to infinity of the PDF of the N-degree of freedom Chi-squared distribution, for instance. Detection performance, characterized by the probability of detection P_D, is determined as

$$P_D = pr\{T(x) > \gamma; H_1\} \tag{3.5}$$

This standard approach is applied more generally, using the PDF of $T(\boldsymbol{x})$ and the $\mathcal{Q}$ function used to determine P_{fa}; coloration of the noise through filters $P(z)$ and $F(z)$ violate the assumptions of the basic energy detector, however, requiring a modification to this result for accuracy.

Figure 3.4 demonstrates the detection probabilities for input signal to noise ratio. These performance curves are developed based on a preselected false alarm probability P_{f_a} which can be see in Figure 3.4. The graph shows that when demanding a low rate of false alarms, the detector picks up very low amplitude signals poorly.

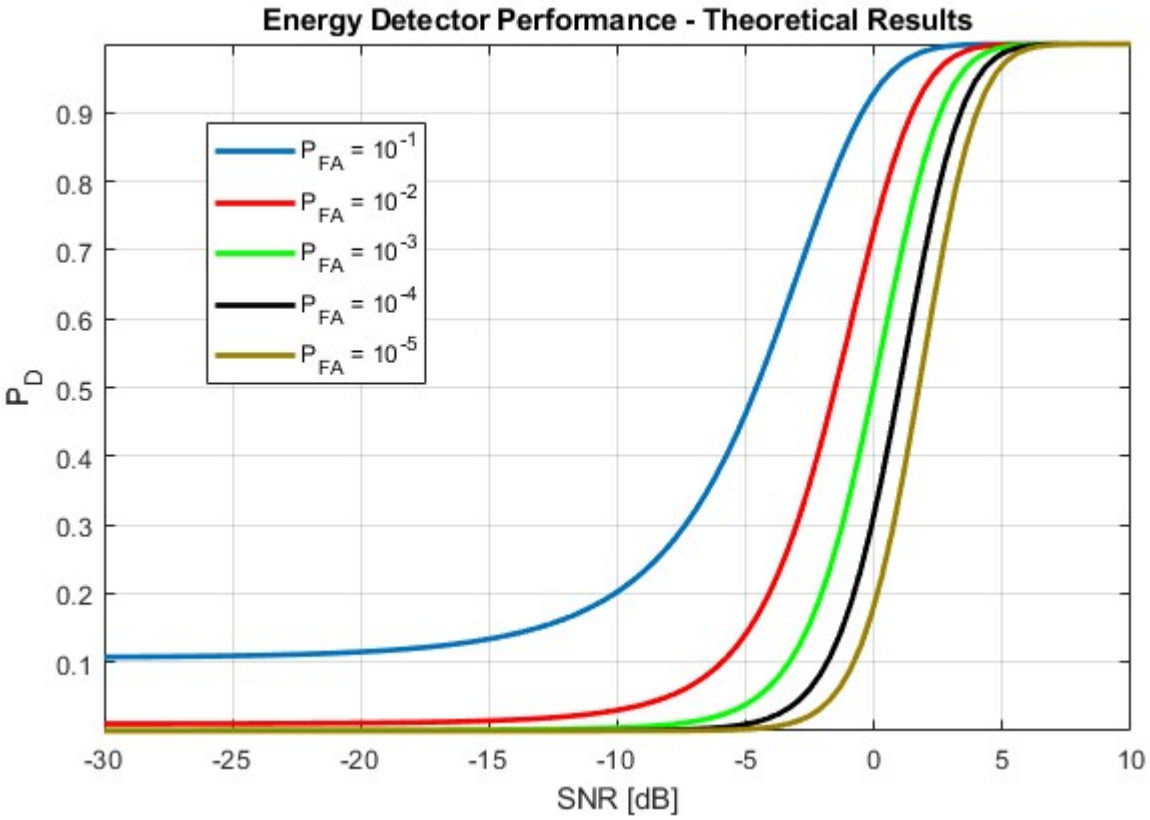

Figure 3.4: Detection probabilities for input signal to noise ratio (dB).

It should be noted that these calculations are for a set of specific conditions where the signal is distributed WGN in the ambient condition which may or may not be the case for this application. These conditions represent a "best case scenario" for the application. To obtain a more accurate threshold for scenarios other than "best case", a relaxation may be applied to the assumption. Obtaining a more

accurate threshold will consequently lead to a more accurate P_fa.

The Lindeberg-Feller Central Limit Theorem (LFCLT) provides a more computationally efficient and accurate solution while simultaneously allowing for a more general covariance structure between samples, thus reflecting a more accurate in-the-field condition for the HVDC control system signal. The LFCLT provides

$$\frac{1}{s_n}\sum_{n=0}^{N-1}(x[n]-Ex[n]) \rightarrow N(0,1) \tag{3.6}$$

where $N(0,1)$ is the standard normal (Gaussian) distribution, s_n is the sample standard deviation, and $E\{.\}$ is the expected value operator. This approximation provides several advantages with only minor drawbacks. The advantages include: it becomes easier to calculate, more intuitive and simpler overall. The drawbacks are that it is inaccurate for small N numbers and incorrect false alarm rates will be experienced. Although advantages are attained using this method, more analysis is required to justify this approach to make certain that the limitation on the size of N does not prove to be unacceptable.

While it is the case that the true distribution function will be asymmetric with positive skewness, the approximation is symmetric with zero skewness - the approximation will therefore tend to *under-approximate* the true distribution for small record lengths and/or low P_{fa}, suggesting that a more conservative threshold γ is calculated in practice. A record length N should be chosen as $N > 30$, as the general rule of thumb, for sufficient application of the approximation [18].

This approximation and its accuracy is found in much statistics literature [18] and is sufficiently out of scope to be omitted, with a note on record length. For acceptable accuracy, the record length is quite dependent on underlying signal spectral properties. 'Rules of thumb' hold that the standard CLT, under assumed independent, identically distributed distributions, begins to kick in around $N > 40$. The LFCLT assumes, however, that the distributions are not identically distributed; therefore, the record length needs to be longer before normality becomes an acceptable approximation. If the spectral density is quite flat, values are very close to one another and the Lindeberg-Feller CLT is *essentially the same* as the standard CLT. The approximation therefore holds for $N \approx 40$ and larger. However, if the spectrum is modal and varying, N should be larger.

The effect of the approximation's accuracy on performance is seen in Figure 3.5. If a threshold is calculated assuming normality and a small P_{fa}, the integrated area under the CLT curve is smaller than that of the true PDF. Thus, the true P_{fa} is slightly less than that originally specified, implying that the detector will perform marginally worse. Of course, as $N \rightarrow \infty$, the difference between this and true PDF vanishes, as does the difference in performance. For this application specifically, this is not an issue - it

is simply an observation for those who would use smaller windows for similar applications. N is at least $10\times$ greater than the minimum required for acceptable accuracy.

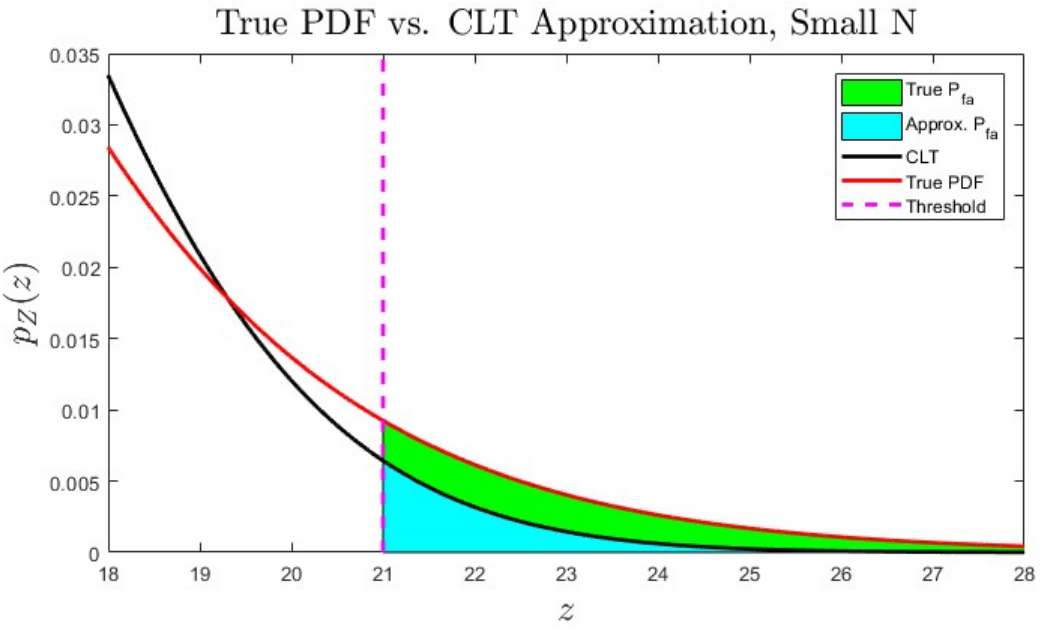

Figure 3.5: CLT Approximation for a fixed, small N.

Values for P_{fa} range widely from 10^{-2} to 10^{-7} and depends on which error of the two (i.e. false alarm or missed detection) a user is more willing to accept, from a performance perspective. That is, if the application requires the user to very rarely miss detecting an oscillation, then the operator must be willing to accept a higher rate of false alarms. However, if the application requires very few false alarms but is willing to accept worse performance and an increase in missed detections, then P_{fa} can be chosen to be very small. It is not possible to minimize both errors simultaneously.

Once P_{fa} is chosen, the threshold is easily calculated. The signal's spectral values $\phi_x(\omega)$, which define the signal's underlying statistical qualities [17], must be calculated (or estimated with a very high degree of confidence) using a spectrogram, periodogram, or other spectral technique and applying it to equation (3.6) with

$$s_n = \left(\sum_{n=0}^{N-1} \phi_x^2(\omega_n) \right)^{\frac{1}{2}}, \tag{3.7}$$

and

$$E[X_n] = \phi_x(\omega_n), \tag{3.8}$$

the threshold is readily calculated.

Thus, the threshold is given in equation (3.9),

$$\gamma'' = \left(\sum_{n=0}^{N-1} \phi_x^2(\omega_n) \right)^{\frac{1}{2}} \mathcal{Q}^{-1}\big(P_{fa}\big) + \sum_{n=0}^{N-1} \phi_x(\omega_n) \tag{3.9}$$

where $\mathcal{Q}^{-1}(*)$ is the inverse $\mathcal{Q}$ function of the standardized normal distribution.

3.5 Bumpless Transfer

In utility applications, it is common to implement a 'bumpless transfer' to ensure the controller transitions from manual to automatic mode without disruption in the process. For the common use of bumpless transfers, when a system switches from manual to automatic it is necessary that there isn't a sudden transient (or bump) in the system controller. The bumps are created by the difference in the setpoint and the process variable, commonly the 'error'.

While in manual mode the controller, if not informed otherwise, will continue to try and drive the process variable toward the setpoint. The controller at this point is no longer in control of the device and if switched back to automatic, the build up of the controller trying to adjust the process variable will unload and create a major disturbance all at once when the system is put back into automatic mode. If there is a large spike in the system it can trigger alarms, or error codes which can cause problems and if there was a large enough value between the setpoint and the process variable that can cause major disruption in the system in the next cycle.

The classic bumpless transfer is useful in a HVDC control system equipped with the previous detection and mitigation system so that a backup controller, compensator, or sensor can be switched out in place of the normal operating equipment under conditions of attack without inducing large transients. If the normal operating controller is under attack, a secondary controller could be used to replace the operating controller and regain control of the system before the cyber-attack spreads. The secondary controller could include all of the same signals of the normal operating controller while maintaining its cyber-secure system. The switching out of the controller would create a disturbance in the system that a bumpless transfer could help in avoiding.

3.5 Implementation of Bumpless Transfer into HVDC Control System

In [4], a MTDC system was developed in an electromagnetic transients program known as ATP. The system was developed using control schemes from [5] and [19]. The MTDC system in this work connects four VSCs by HVDC transmission lines while each VSC is connected to an isolated AC grid [4]. Figure 3.6 shows the control center portion of the system model where a secondary controller is modeled.

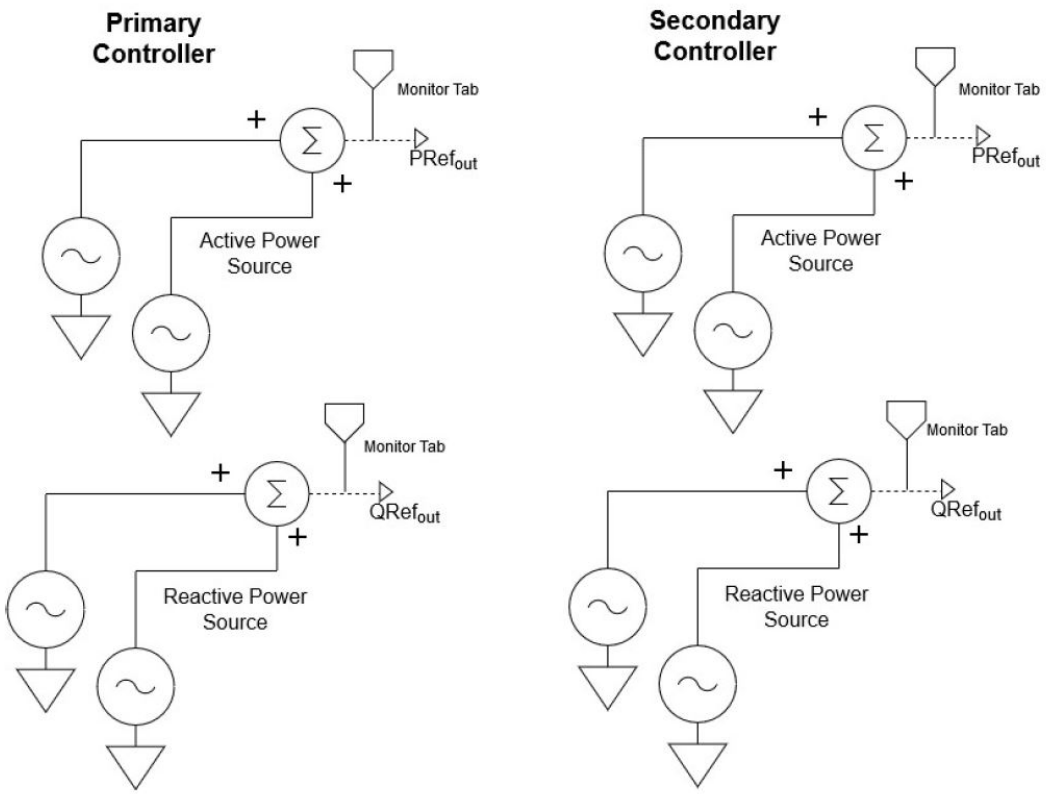

Figure 3.6: This figure shows a modeled control center for the system model developed in ATP and highlights the primary and secondary controllers.

The secondary controller included all of the same components of the normal operating controller but the references are changed for both reactive and active power. The reference voltage is not changed. Switches are implemented before the voltage droop control that take the primary controllers active power reference and switch it out with the secondary controllers. A similar set of switches is used in the closed loop modulating functions portion of the system model to change the reactive power reference. Both switches are set to switch at ten seconds after the system started up, allowing time for the system to stabilize.

The absence of any form of bumpless transfer illustrates that both the reactive and active power outputs experience a large 'bump' at the ten second mark just as the primary controller is switched out for the secondary controller. Figures 3.8 and 3.9 demonstrate the bump for both outputs. Several methods are considered for smoothing the transition bump - the most promising is a control logic that is designed to track the reactive and active power inputs. The logic includes taking the reference input and running it through a gain twice, once to get a minimum and once for the maximum. The gains which are set at 1.1 and 0.9 for the maximum and minimum respectively are chosen to allow room for some form

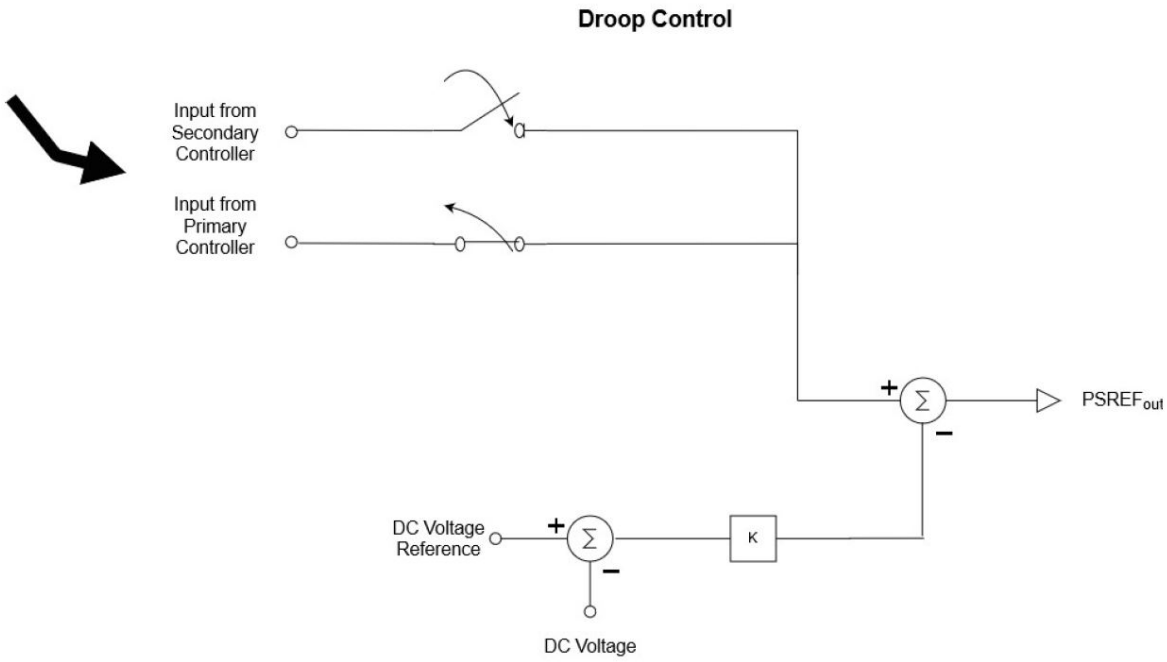

Figure 3.7: This figure demonstrates the voltage droop control of the system model and uses the arrow to point to the two different controller inputs that are switched at ten seconds.

of noise but not allowing a sufficiently large enough signal to drastically perturb the system. When the input is either below the minimum or above the maximum, the logic takes a different course of action by notifying the controller to make a smooth transition to the new input without any large disturbances. A similar approach was used with mode switching in LCC converter controls for switching from current regulation to voltage regulation, or constant firing angle, etc. The logic for the reactive and active powers can be seen in Figure 3.10 and Figure 3.11.

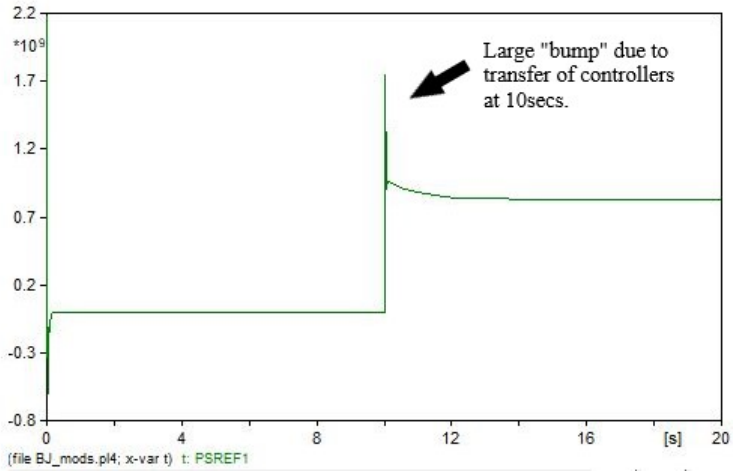

Figure 3.8: This figure shows the active power output after being adjusted by the voltage droop control and uses an arrow to demonstrate the "bump" in the system.

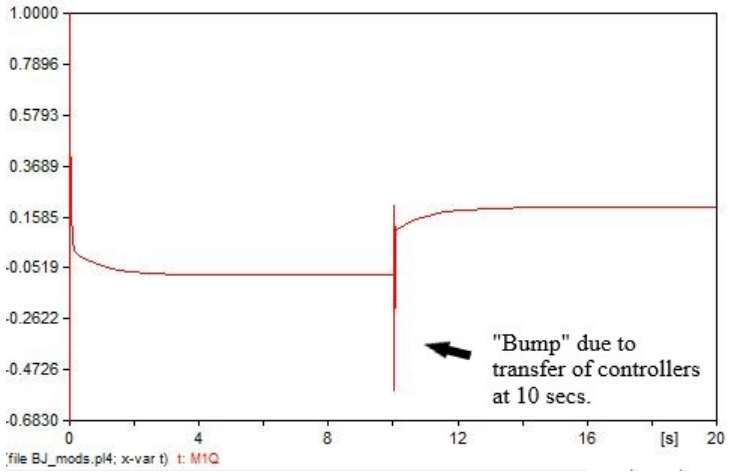

Figure 3.9: This figure shows the reactive power output of the closed loop modulating function and uses an arrow to demonstrate the "bump" in the system.

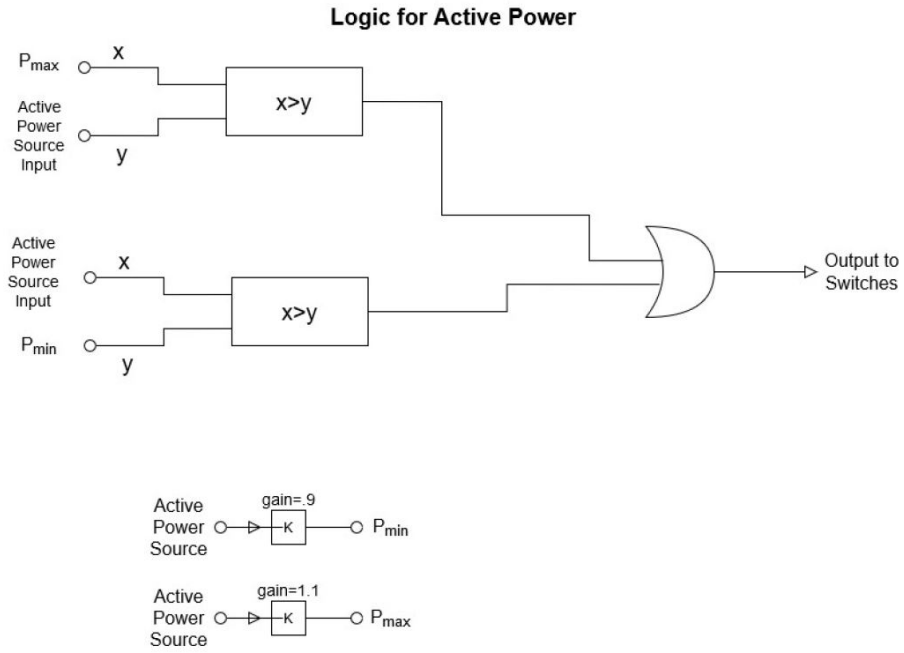

Figure 3.10: This figure shows the logic behind the active power including solving for a minimum and maximum based on the set point and monitoring the input for any significant changes.

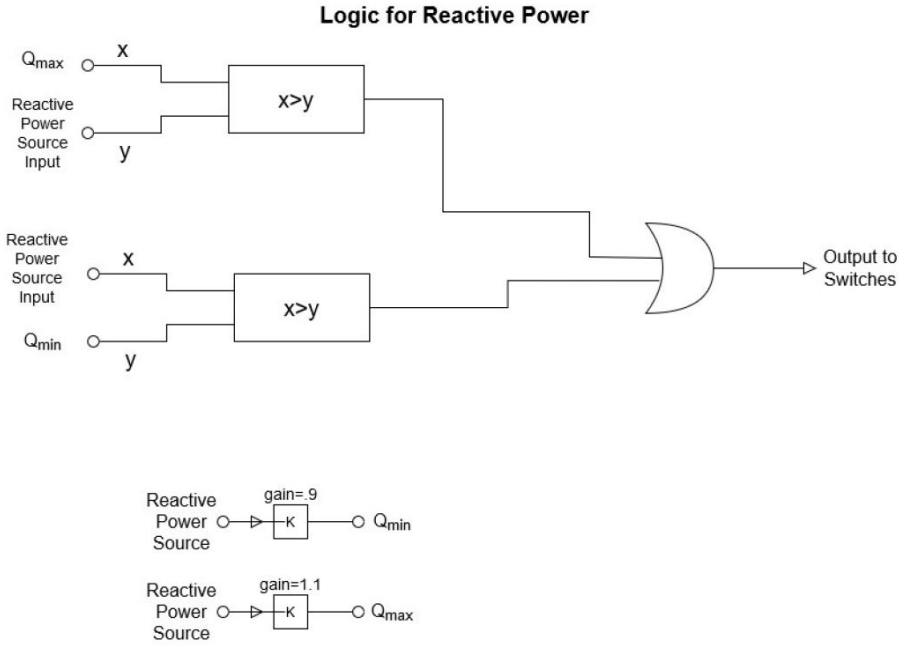

Figure 3.11: This figure shows the logic behind the reactive power including solving for a minimum and maximum based on the set point and monitoring the input for any significant changes.

Chapter 4: Results

After incorporating a detection algorithm, threshold calculation, and a layered response to the energy detector, a number of tests are performed to see how each case impacts the system. The energy detector is designed to mitigate the amount of potential false alarms while providing true detection for cyber-attacks. The results from twenty-two test cases provide an insight into the performance of the energy detector. Table 4.1 shows the attack scenarios for each of the twenty-two test cases performed and includes a description of each attack scenario.

The attack scenarios range from single attacks to combined double attacks and included various ranges of thresholds. Table 4.2 is a more detailed record of each individual test case. Along with the test case number, a variety of information and observations are included. The table includes the time it takes during each case to alarm, inform and switch. Also included is the probability of detection and the probability of false alarms. The final two columns in Table 4.2 include the signal-to-noise (SNR) ratio and a column for notes that highlight the important details from each test case.

Table 4.1: Test cases used to describe performance of detection algorithm under various plausible operating conditions and attacks.

Test Case	Attack Scenario	Description
1-4	Single Attacks, Measurements	These test cases simulate attacks on AC Voltage/Current/Power and DC Voltage/Power measurements and is used to characterize the effect on modulation signals, used in detection methodology development.
5-8	Double Attacks, Measurements	These test cases simulate simultaneous attacks on AC Voltage/Current/Power and DC Voltage/Power measurements and is used to characterize the effect on modulation signals, used in detection methodology development.

Table 4.1: Test cases used to describe performance of detection algorithm under various plausible operating conditions and attacks.

Test Case	Attack Scenario	Description
9-12	Combined Attacks on Monitoring Signals	These test cases simulate simultaneous attacks on AC Voltage/Current/Power and DC Voltage/Power measurements and is used to characterize the effect on modulation signals, used in detection methodology development.
13-15	Range of thresholds for several initial conditions (measurement noise floor, varying window lengths, etc.)	This test case is used to determine the sensitivity of detection rate and probability of false alarm to the threshold calculation.
16-22	Varying SNR of signal introduced by cyberattack	This test case is used to determine the sensitivity of the detector to low-amplitude disturbances.

Table 4.2: A number of test cases are summarized in the proceeding table. The salient results from these tests are summarized in the section to follow. Columns representing time to alarm, inform, and switch are in the unit of seconds. The columns representing the probability of detection and false alarms are in decimal percentage units. The SNR column is in dB.

Test Case	Time to Alarm	Time to Inform	Time to Switch	Prob. of Detection	Prob. of False Alarm	SNR	Notes:
1	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (negative), saturation
2	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: High amplitude oscillation
3	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (positive), saturation
4	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (positive), saturation
5	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: DC Bias
6	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: DC Bias

Table 4.2: A number of test cases are summarized in the proceeding table. The salient results from these tests are summarized in the section to follow. Columns representing time to alarm, inform, and switch are in the unit of seconds. The columns representing the probability of detection and false alarms are in decimal percentage units. The SNR column is in dB.

Test Case	Time to Alarm	Time to Inform	Time to Switch	Prob. of Detection	Prob. of False Alarm	SNR	Notes:
7	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (positive), saturation
8	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (positive), saturation
9	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Large DC Bias (positive), saturation
10	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: High amplitude, high frequency oscillation
11	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Oscillation
12	N/A	N/A	N/A	N/A	N/A	N/A	For characterization: Oscillation
13	0.8	2.25	6.38	0.998	0.026245	-10dB	Thresholds set: conservatively high, nominal window lengths, no “Inform” or “Switch” false alarms
14	0.43	1.44	4.56	0.999	0.092897	-10dB	Thresholds set: moderate, nominal window lengths, no “Inform” or “Switch” false alarms
15	0.42	1.34	3.90	0.999	0.014539	-10dB	Thresholds set: aggressively low, nominal window lengths, several “Inform” false alarms, negligible “Switch” false alarms
16	0.48	1.48	4.95	0.999	0.016663	-10dB	Thresholds set: moderate, short window lengths, no “Inform” or “Switch” false alarms

Table 4.2: A number of test cases are summarized in the proceeding table. The salient results from these tests are summarized in the section to follow. Columns representing time to alarm, inform, and switch are in the unit of seconds. The columns representing the probability of detection and false alarms are in decimal percentage units. The SNR column is in dB.

Test Case	Time to Alarm	Time to Inform	Time to Switch	Prob. of Detection	Prob. of False Alarm	SNR	Notes:
17	0.64	2.14	5.91	0.997	0.0033326	-10dB	Thresholds set: moderate, intermediate window lengths
18	0.71	3.01	8.48	.999	0.0022912	-10dB	Thresholds set: moderate, long window lengths, no "Inform" or "Switch" false alarms
19	0.73	1.61	5.21	0.979	0.020621	-13dB	Thresholds set: moderate, intermediate window lengths, no "Inform" or "Switch" false alarms
20	1.31	3.90	12.96	0.787	0.024162	-19dB	Thresholds set: moderate, intermediate window lengths, no "Inform" or "Switch" false alarms
21	0.56	1.35	4.40	0.999	0.016871	-7dB	Thresholds set: moderate, intermediate window lengths, no "Inform" or "Switch" false alarms
22	0.51	1.21	4.08	0.99	0.010414	-1dB	Thresholds set: moderate, intermediate window lengths, no "Inform" or "Switch" false alarms

From both Tables 4.1 and 4.2 it can be determined that the detection algorithm is flexible, easily tuned, and difficult to fool. Depending upon the operator's level of comfort with the automatic detection, it may be adjusted to detect quickly but less accurately, as opposed to the standard configuration which values accuracy and the minimization of false alarms. With the understanding of how each of these tuning parameters impacts detection speed and accuracy, the engineer is able to tune the detector for various different conditions, depending on provided requirements.

Figures 4.1 - 4.4 show the detailed results of a "standard" testing scenario with the SNR at $\approx$ -7dB.

The total simulation length is 60 seconds. The attack appears at time t=10 seconds, and is removed at time t = 45 seconds.

Figure 4.1 shows the results of the simulation being ran with a nominal configuration with a short window length for the alarm portion of the layered response. It can be seen that at 10 seconds the attack is initiated and the system responds well. The time to detection is less than one second. It should also be noted that several single-point false alarms (points in which the test statistic rose above the threshold but only momentarily for a single point and not continuously) are present in the short window variance estimate but no false alarms were triggered because there were insufficient consecutive numbers to trigger an alarm.

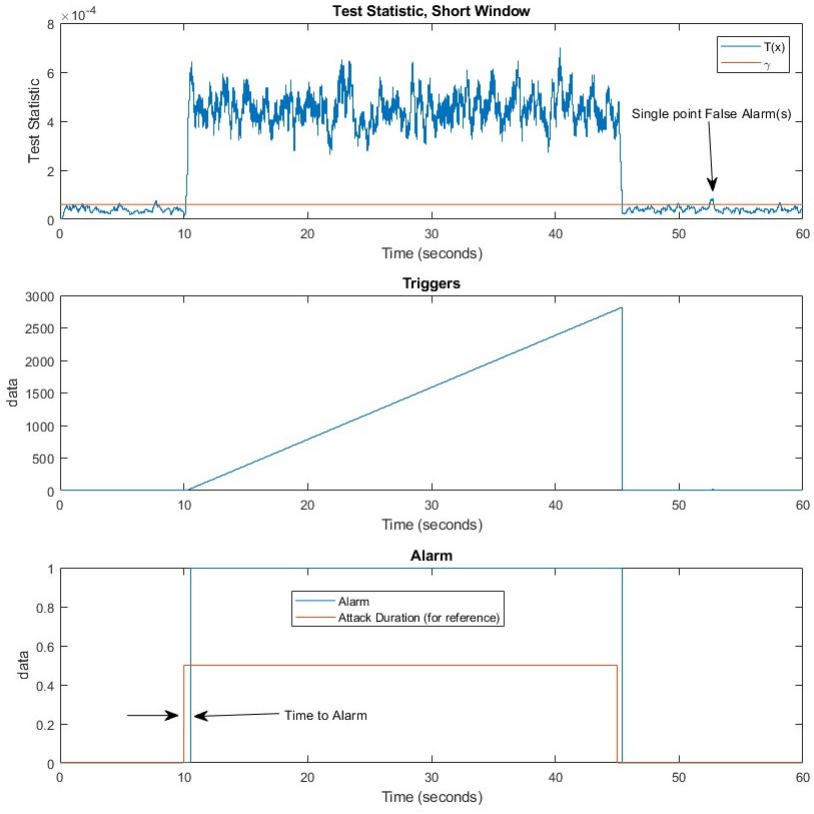

Figure 4.1: "Alarm" layer of the detector shown operating for a "standard" testing scenario with the SNR at ≈ -7dB.

Figure 4.2 demonstrates the inform stage of the standard testing scenario. The inform stage uses the intermediate length window and the time to the alarm is at approximately two seconds. It is important to note that Figure 4.2 does not demonstrate any single-point false alarms.

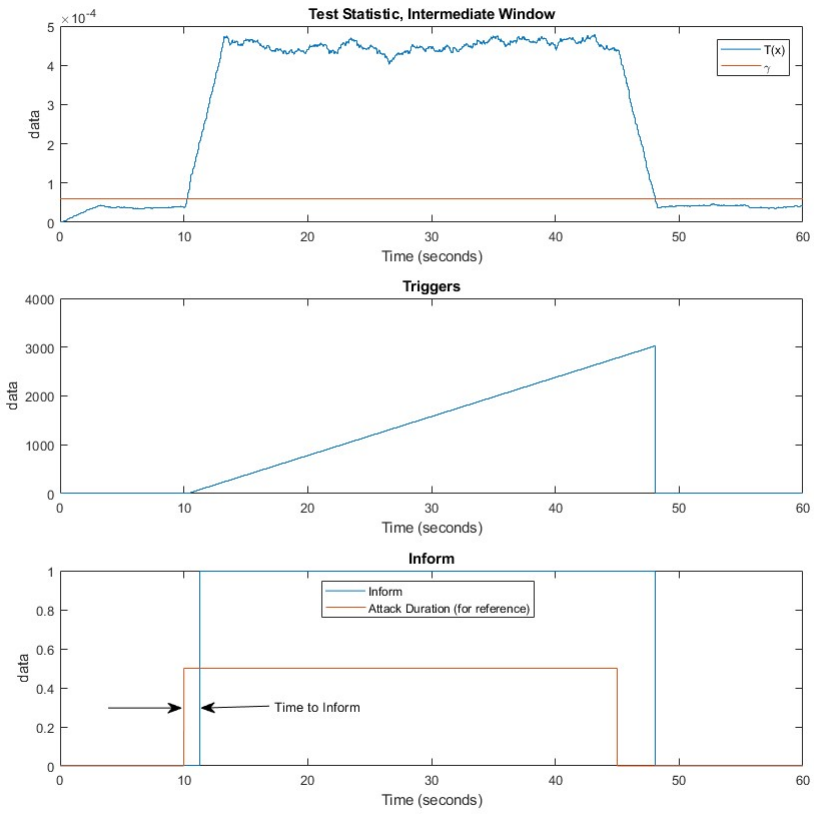

Figure 4.2: "Inform" layer of the detector shown operating for a "standard" testing scenario with the SNR at ≈ -7dB.

Figure 4.3 shows the switching portion and third layer of the layered response described earlier. The switching layer uses the longest window of the three layers and takes the must wait for the first two stages to be cleared before initializing. It can be seen on the bottom graph that it takes about five seconds for the controller to be switched out due to the attack. Having the system react in less than five seconds is faster than most operators would be able to respond to any system disturbances. This quick response is important because the faster the response, the more likely that the system can prevent any catastrophic or cascading failures. As for human responses, the operator has other priorities that come before making meaningful distinctions before things go haywire which makes early detection even more important. It also demonstrates why this detector is automated. The automation takes the decision out of the operator's hands who generally speaking do not have an in depth understanding and knowledge of the system and the necessary actions/responses to cyber-attacks.

As with 4.2, Figure 4.3 shows no single-point false alarms. The final figure pertaining to this first

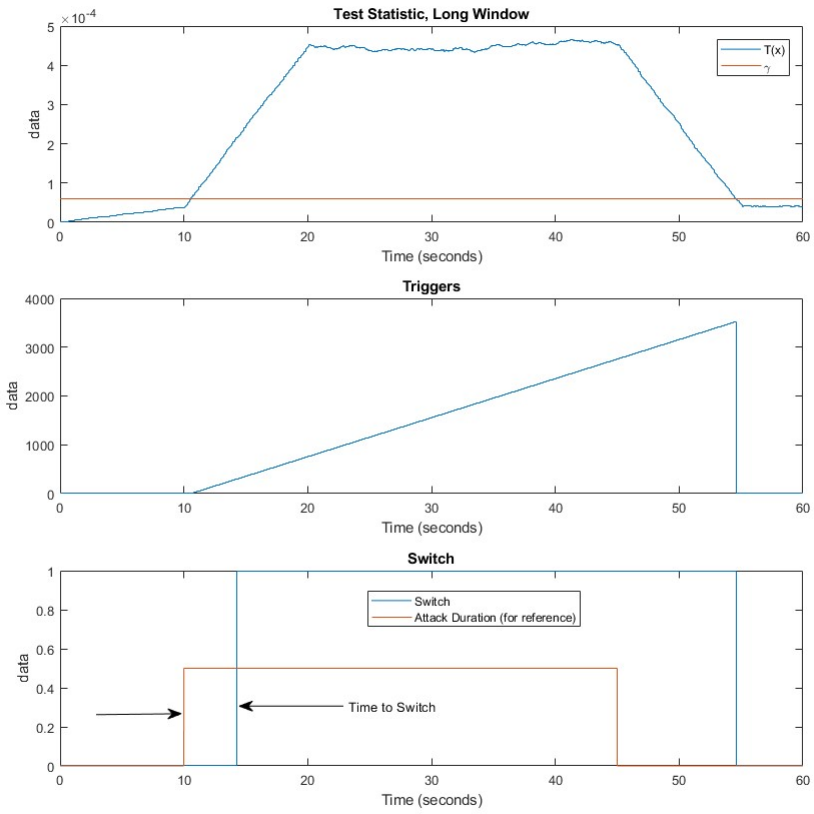

Figure 4.3: "Switch" layer of the detector shown operating for a "standard" testing scenario with the SNR at ≈ -7dB.

simulation model is Figure 4.4. Figure 4.4 shows the three layers of the layered response transcribed onto a single figure. Looking at the "Level of Alertness" graph it demonstrates the three layers and their response times. The attack initiates at ten seconds, one second later the first alarm sounds, another second after that the operator is informed and finally five seconds after the attack begins, the controller is switched off to standby mode. This assures that the detector is working properly and that the layered response is allowing for a confidence in an attack before taking steps that could potentially derail the system.

A condition in which the controller works insufficiently is where the SNR is insufficient for detection. Figures 4.5-4.8 demonstrate the situation. There are no negative impacts to the controller due to the low amplitude nature of the attack which makes this situation not quite as troubling as others, it must be noted that the detector is unable to consistently detect the attack. The attack for this situation again starts at 10 seconds and ends at 45 seconds. When the SNR is insufficiently low for consistent detection,

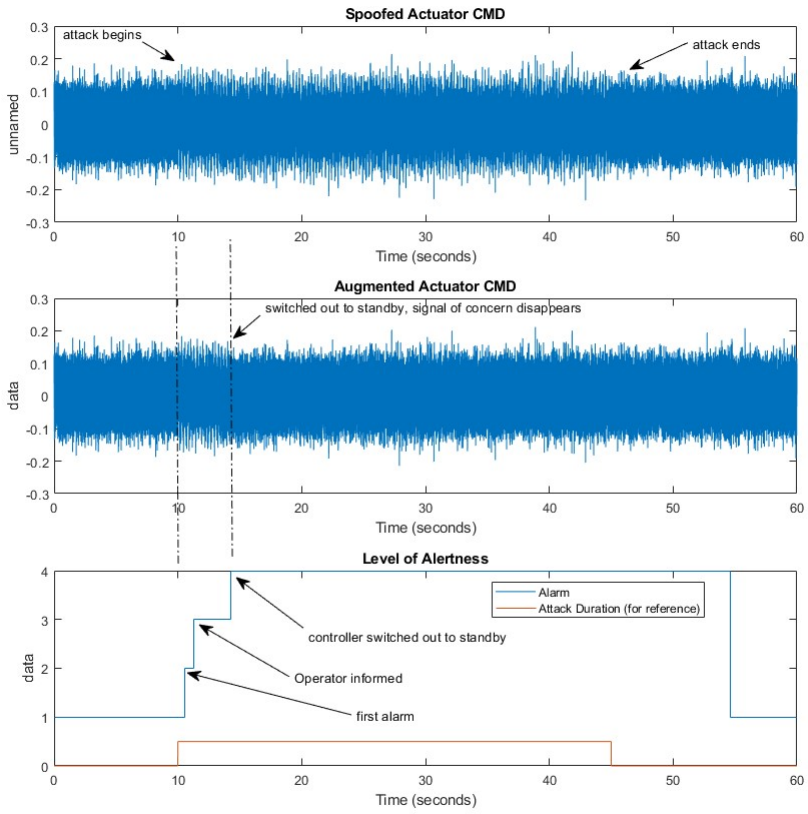

Figure 4.4: Combined layers of the detector shown operating for a "standard" testing scenario with the SNR at ≈ -7dB.

it should be noted that this is a good example of a case where later analyzing logs from the three layers of detection could provide insight to the system. It is possible that with a low SNR, there is the potential of someone probing the system while preparing for a larger attack later and offline analysis could provide an insight into preparing for that larger attack to come.

Figure 4.5 demonstrates the first layer of the detector with the short window. As can be seen in the first graph of the figure, the attack is almost unnoticeable amongst the white noise leading to an excessive amount of triggers and alarms (shown in the second and third graphs). Due to the low amplitude nature of the attack the detector is reading a large amount of single-point attacks. This is a result of the attack only being able to cross over the threshold for single points and not multiple in a row which is required for the each layer of detection to confirm the attack. Overall, the short window provides sporadic detection throughout the attack. The singular upside to the short window simulation is that detection is still possible within the first second after the attack initializes.

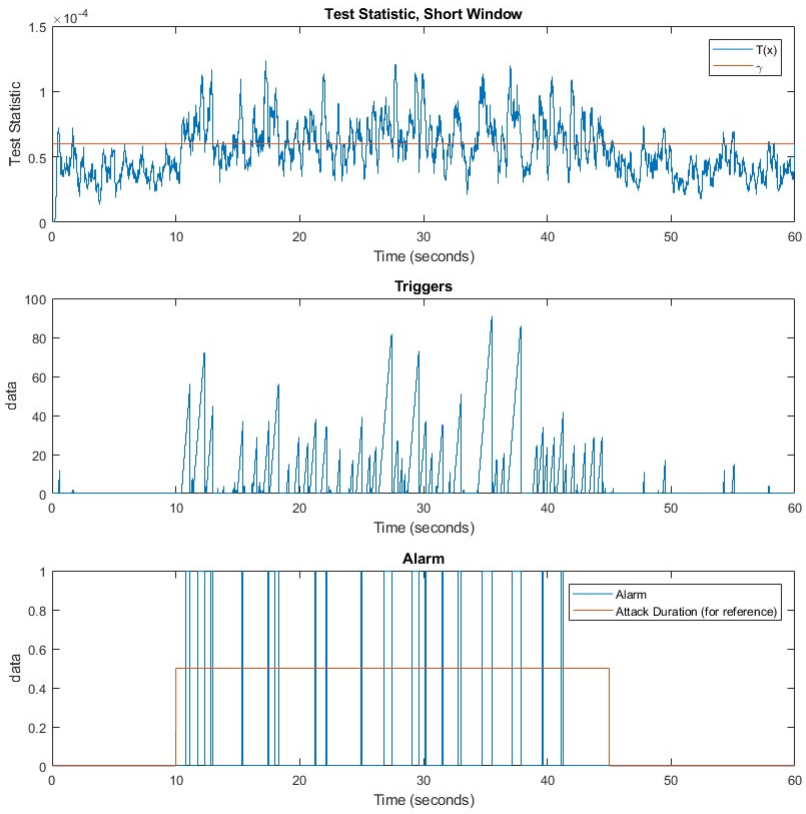

Figure 4.5: "Alarm" layer of the detector shown operating for a testing scenario in which the SNR is insufficient for recognition.

Figure 4.6 shows similar patterns to that of Figure 4.5. Detection is sporadic due to the almost unnoticeable attack amongst the white noise. It is important to note that as a result of a medium length window, there are fewer triggers and fewer alarms than from the short window, however it is not a consistent detection for the length of the attack. Being that this is the second layer of the layered response, it is the layer in which the operator is informed of the attack. In this case, the operator is not informed for roughly three and a half seconds after the attack begins. Due to the multiple triggers and alarms, it is concluded that the detection is sporadic and the detector inconsistent.

Figure 4.7 is the third and only layer of the simulation that provides just one trigger and one alarm. However, due to the long window nature of the window and the low SNR, it takes approximately eleven seconds to switch the controller.

The final figure pertaining to this first simulation model is Figure 4.8. Figure 4.8 shows the three layers of the layered response transcribed onto a single figure. In the "Level of Alertness" graph it is

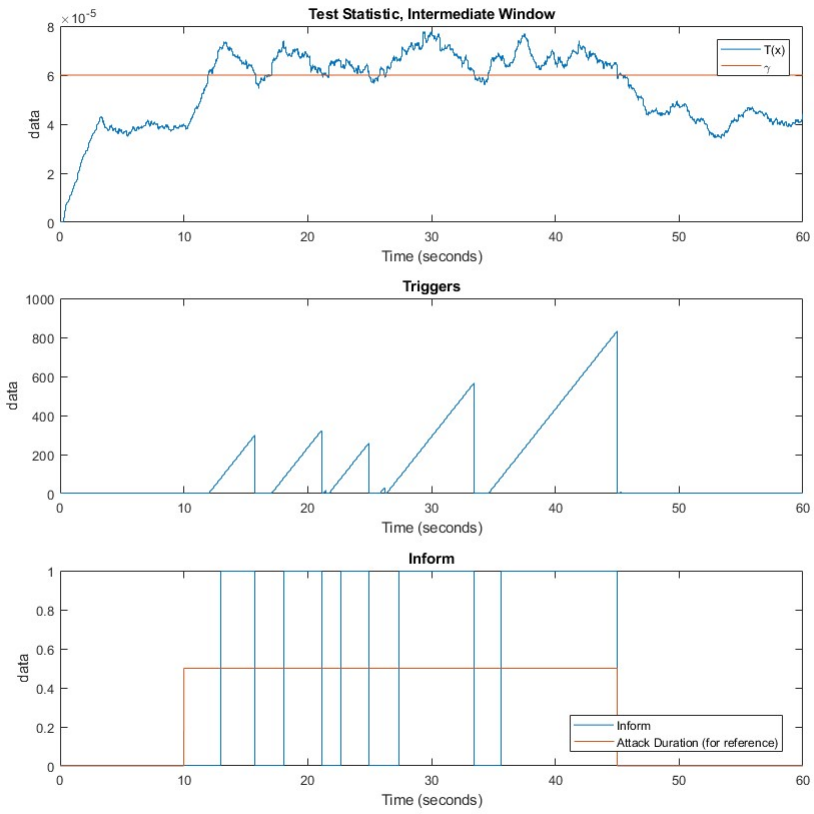

Figure 4.6: "Inform" layer of the detector shown operating for a testing scenario in which the SNR is insufficient for recognition.. Detection is sporadic

found that the detector struggles to identify the attack. Alarms begin to sound within one second of the initial attack but it is not one continuous alarm throughout the course of the attack. There are six alarms triggered throughout the attack but it takes roughly eleven seconds after the initial attack for the detection to be certain and remain on alarm throughout the remainder of the attack. Due to the above ten second delay in confirming the presence of an attack, it is deemed that the detection is late and the controller insufficient for detection.

A final simulation is run where the threshold is set aggressively low. The low threshold results in a great deal of false alarms but improves the overall detection *time* of the attack. Figures 4.9-4.12 demonstrate this simulation.

Figure 4.9 shows the first layer of the detection process. It can be seen in the first graph that the threshold is dropped to $.4 * 10^{-4}$ (the other simulations had a threshold of $.6 * 10^{-4}$) which allows for a lot of single-point attacks throughout the entire sixty second simulation. There are multiple triggers

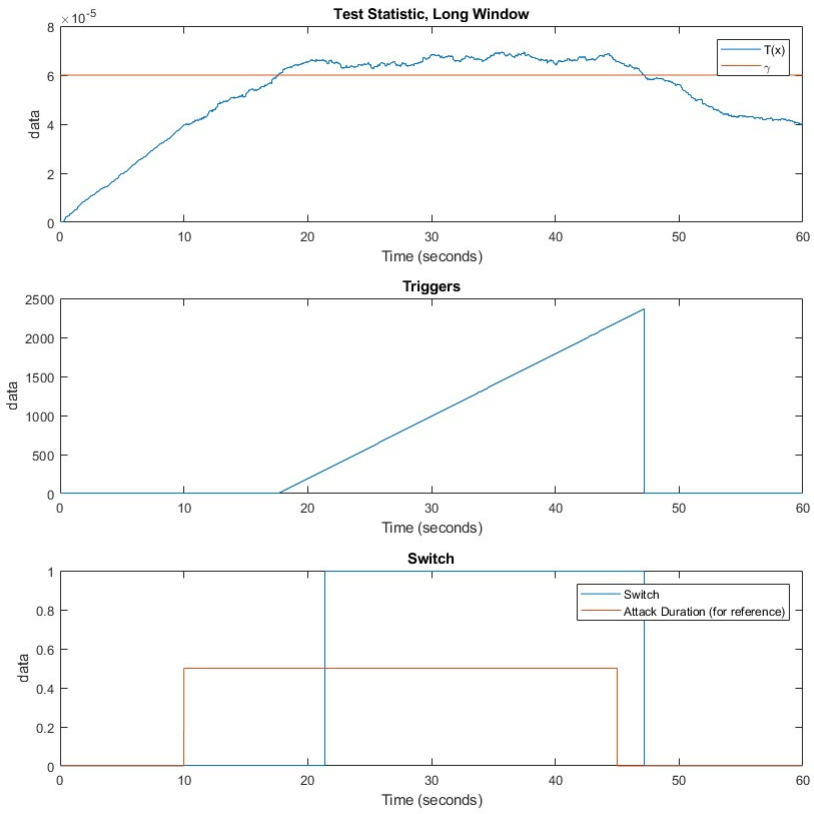

Figure 4.7: "Switch" layer of the detector shown operating for a testing scenario in which the SNR is insufficient for recognition.

both before and after the attack as demonstrated in the second graph, and to go along with those triggers there are a number of false alarms in the third graph. Prior to the attack, there are four false alarms but the positive result of the low threshold is yielded in the time it takes for the detector to detect the attack. Less than half a second is all that it takes for the alarm to sound and to stay on for the duration of the attack. It is important to note that there a number of false alarms after the attack as well.

Figure 4.10 demonstrates the second layer of the detection process. Utilizing an intermediate window, the number of false triggers and alarms decreases while still being notable. Before the actual attack there is only one false alarm compared to the previous four false alarms at the first layer of the detection process, and the operator is able to be informed of the attack within one second.

The third and final layer of the detection process is demonstrated in Figure 4.11 which utilizes a long window length to minimize potential false triggers. Based on the second and third graph, there were no false triggers or false attempts at switching the controller. With the application of the low threshold,

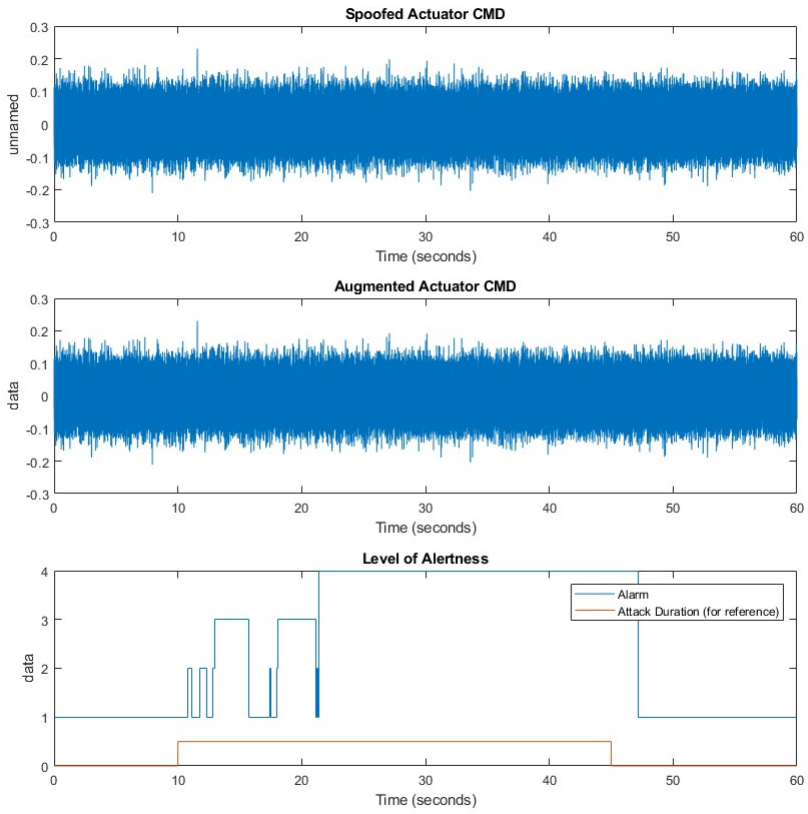

Figure 4.8: Combined layers of the detector shown operating for a testing scenario in which the SNR is insufficient for recognition.

the controller was switched out at approximately three and a half seconds which bested the standard simulation by almost two full seconds.

Figure 4.12 shows the three layers of the layered response transcribed onto a single figure. In the "Level of Alertness" graph it is found that the detector is able to sound the alarm, inform the operator and switch the controller faster than the standard simulation limiting the total detection and layered response to roughly three and a half seconds. This quick detection is due to the lowered threshold and does not come without it's trade-offs. Taking note of the "Level of Alertness" graph, it can be seen that two false alarms sounded at the "alarm level" and one false alarm sounded at the "inform" level. Again this demonstrates the always present trade-off between the accurate detection and false alarms.

The detector delivers in its ability to accurately and quickly detect cyber-attacks of various types. The detector shows promise in its capabilities to deliver to the system's individual needs. Tuning the algorithm to the ambient conditions of the system is key to ensuring optimal detection capabilities,

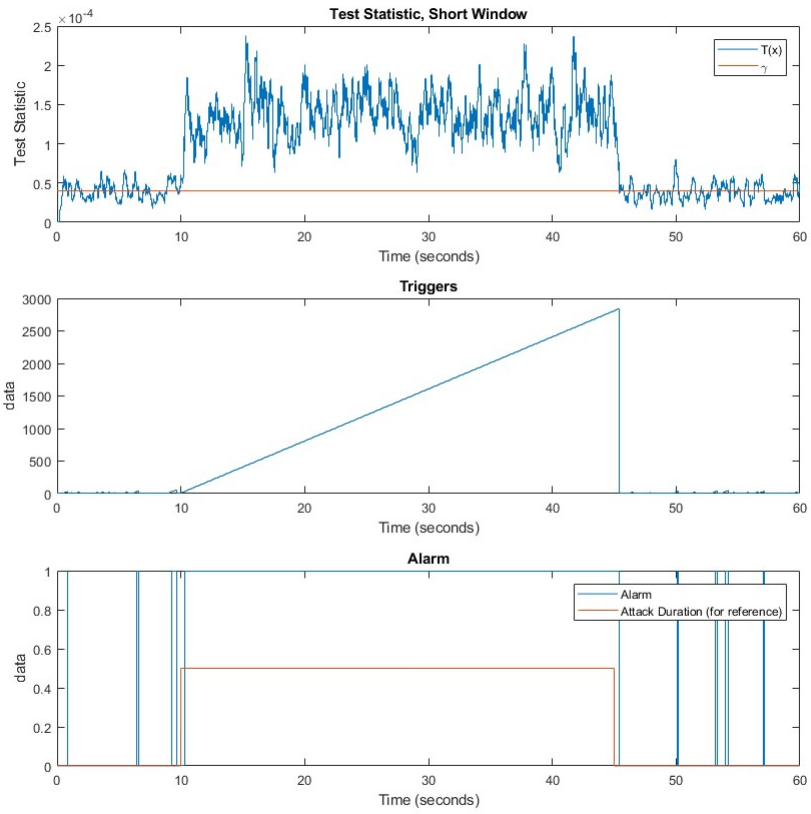

Figure 4.9: "Alarm" layer of the detector shown operating for a testing scenario in which the threshold is set aggressively low.

especially for a predetermined probability of false alarms. To meet a system's needs, the following steps can be followed to ensure accurate and quick detection,

- Gather historical data of record length to produce a very large N,
- Alter the window lengths if additional degree(s) of freedom are needed to tune the controller to the system's needs.
- Determine an acceptable rate of false alarms (P_{fa})
- Calculate the threshold in respect to the acceptable rate of false alarms.

  Using LFCLT, a standard Gaussian distribution probability table can be used for the integration.

  A threshold needs to be determined for each of the parallel detectors.

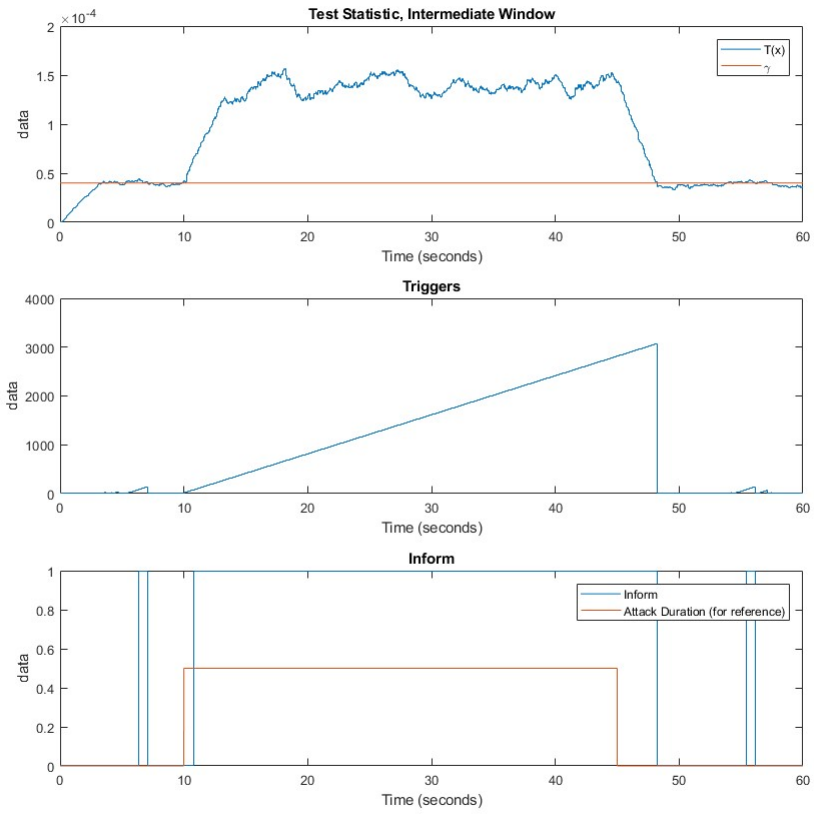

Figure 4.10: "Switch" layer of the detector shown operating for a testing scenario in which the threshold is set aggressively low.

The ever present trade-offs between quick detection and false alarms, and optimal detection while minimizing the impact on operations while not under attack must be kept in mind to carefully determine the correct variables in setting up a successful detector.

It was mentioned previously that the action of the switching layer of the detector in which a controller and/or sensor are switched to standby position depending on the type and severity of detected attack. As discussed, care must be taken in making that switch to avoid large transients that have been introduced into the command signal. Figure 4.13 demonstrates a scenario in which a switch between two identical signals is necessary at 150 seconds. If an attack takes place and a signal has been compromised, the system is reconfigured for a different controller with an identical reference controller. The "memory" of the previous controller remains and the system must take this in to account in order to avoid a substantial bump as seen in Figure 4.14. When this process is done correctly, a smooth, seamless transition can be seen as in Figure 4.15.

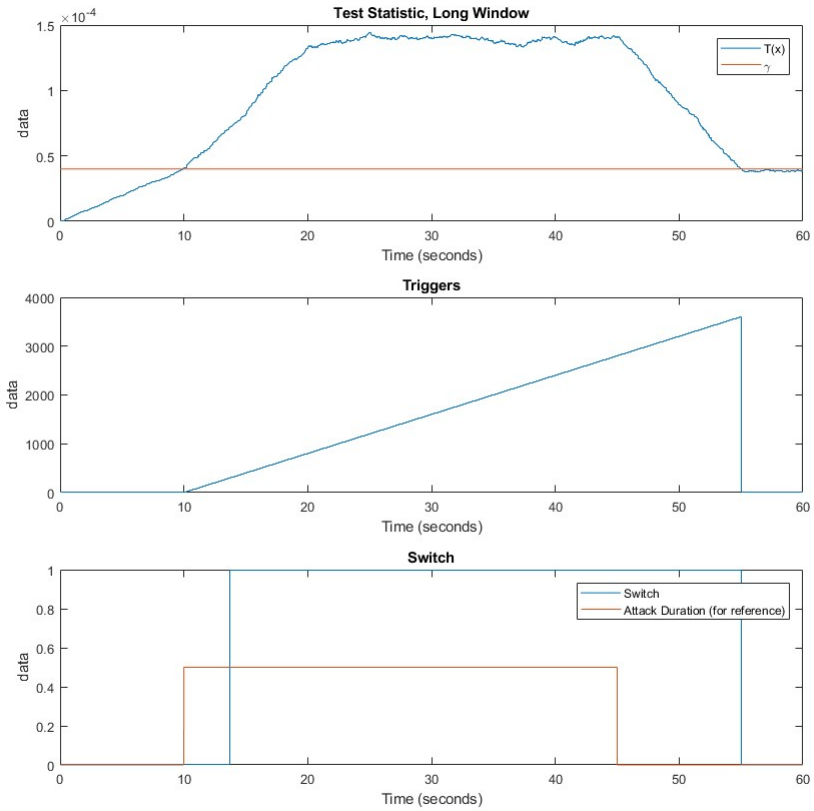

Figure 4.11: "Inform" layer of the detector shown operating for a testing scenario in which the threshold is set aggressively low.

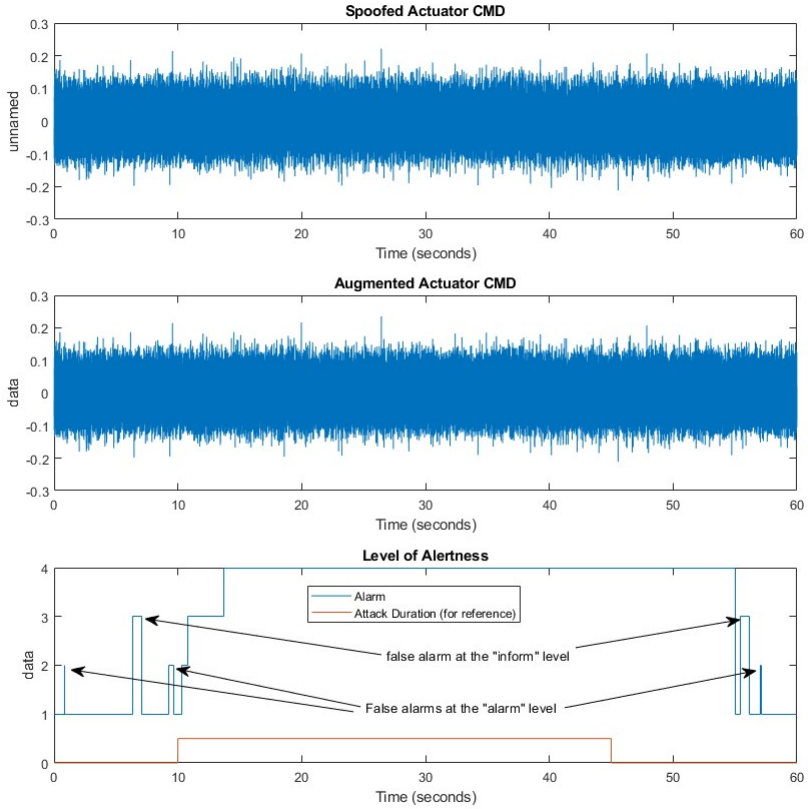

Figure 4.12: Combined layers of the detector shown operating for a testing scenario in which the threshold is set aggressively low.

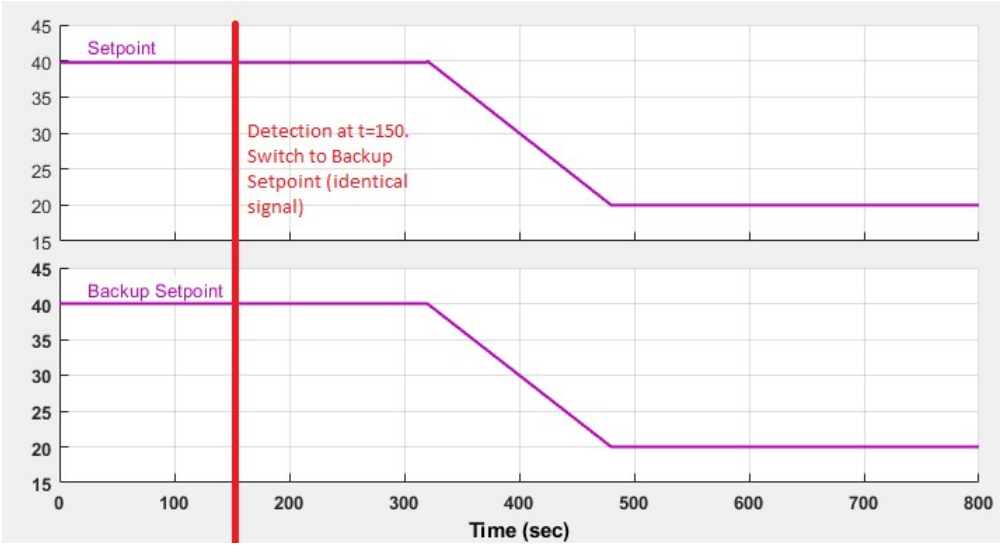

Figure 4.13: References for controller using a bumpless transfer.

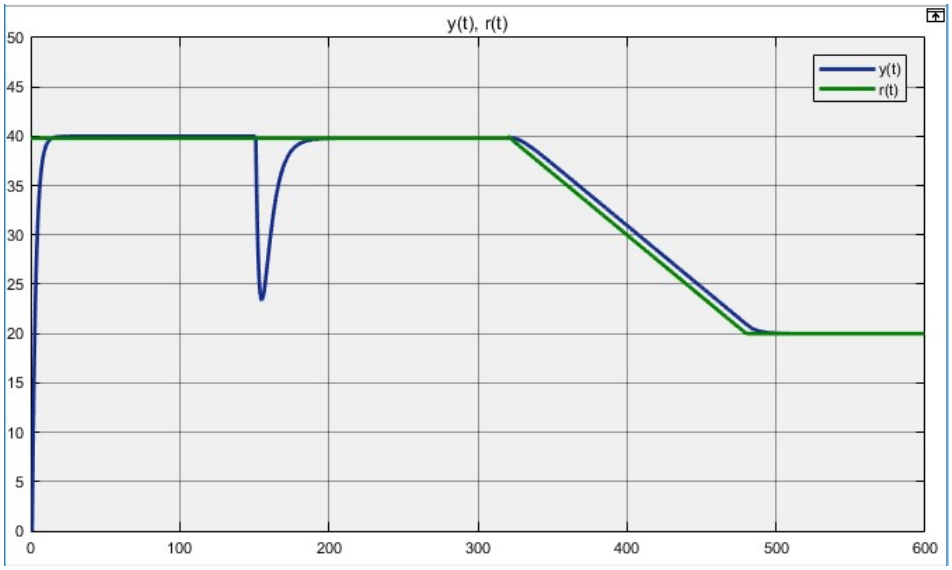

Figure 4.14: Bumpless transfer not in service, creating a large transient.

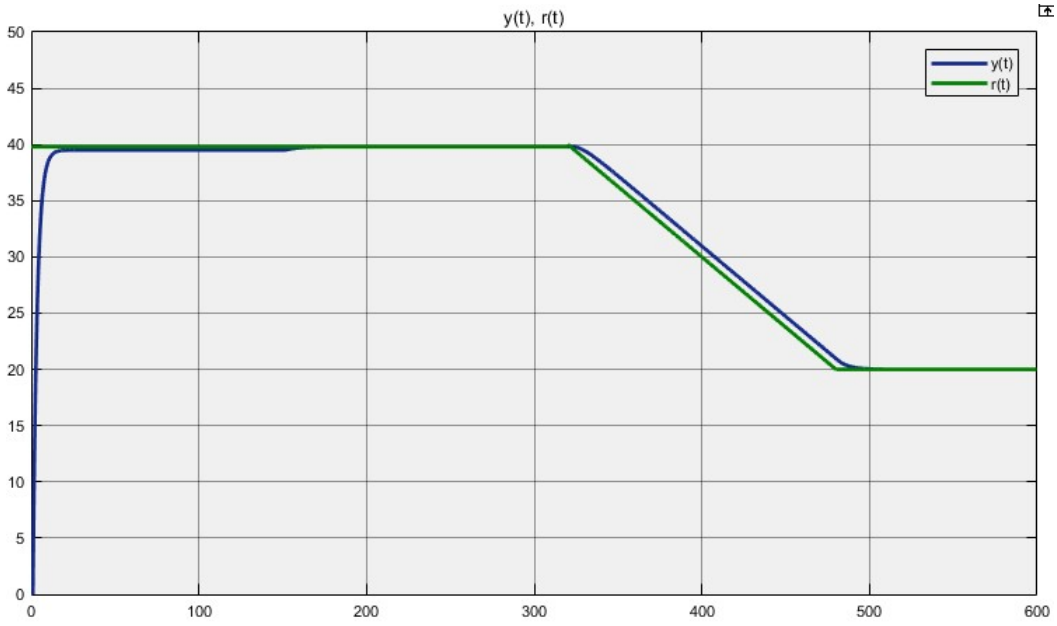

Figure 4.15: Bumpless transfer in service, smoothing out the transient.

Chapter 5: Conclusions and Future Work

AC transmission lines, while more frequently used throughout the world in all power systems, are not ideal for long distribution or connecting asynchronous systems. With recent advancements in power electronics, DC transmission has become more attractive than conventional AC for some applications in many developed and developing countries. HVDC systems were previously restricted to power transmission between two points; with the newest technological advances available at a lower price point, a broader range of HVDC systems allow for new applications previously overlooked, especially with the growing popularity of renewable energy sources. Benefits of HVDC systems include reducing costs for some bulk power transfer cases and allowing for the input and output power to be controlled flexibly for an increase in total power transportation capacity.

In modern HVDC systems there are two basic converter technologies, one of which utilizes a thrysitor based line-commutated converter technology (LCC) and the other utilizing voltage source converters (VSC). The newer of the two technologies, the voltage source converter technology, is more compact and requires only standard transformers when the symmetric monopole topology is applied while providing additional benefits such as improved support for AC voltage stability, less limitations adding taps for additional converter terminals, and power flow direction can be reversed by reversing current polarity. However, despite the advantages, the advances in modern high-speed digital electronics and sensory equipment for HVDC systems has created a list of potential threat vectors for cyber-attacks. This is due to the fact that these systems are increasingly reliant upon sensory infrastructure for measurements in regards to control action.

As stated, HVDC systems are reliant upon sensory infrastructure for measurement in regards to control actions with digital measurements communicated using internet protocols replacing hardwired analog measurements. This leaves HVDC systems potentially vulnerable to cyber-attacks. Two main types of attacks are of greatest concern in this thesis. First, reference attacks which modify stored or transmitted data and second, initialization attacks which change the basic configuration of the hardware or the controller inside the attacked power system. SCADA systems are typically the conduit through which the collected data flows while regularly informing the HVDC system on AC system operating conditions and changes. This means that SCADA systems now face the threat of cyber-attacks. New methods of detection for SCADA systems must be developed because conventional information technology intrusion detection techniques do not catch all possible types of intrusions.

The basic system architecture applied in this thesis uses a proportional-integral type controller to regulate the HVDC power error command signal $e[n]$. The regulated error command signal is responsible for controlling the power electronic equipment responsible for the HVDC line flow. When compromised the control system in the detection and remediation framework switches to use a detector methodology. To ensure that detection meets the needs to respond to multiple types of attacks, filtered energy detection is applied along with observable saturation and outlier detection. Limited assumptions, due to the flexibility of the energy detector, were made to ensure that the detector is capable of perceiving both obvious and not obvious attacks. The detection algorithm was layered with basic underlying theory used to detect operational change with varying detection window length, thresholds, and alarm types to provide a tiered response keeping operational functionality at the design's forefront. Bearing in mind the operational characteristics of the system, a layered three-stage detection was utilized to resolve attacks in the most effective way possible with the least damage to the system performance. It was important not to overburden real-time operations with unnecessary false alarms while ensuring no threats were left undetected. The three-stage detection process includes the following layers:

- Alarm,
- Inform,
- Switch.

The three-stage detection method utilizes three parallel detection branches of varying window length and a comparative analysis between the three different results to determine an "Alertness Level." The alarm stage ensures that detection is as quickly as possible utilizing the shortest window length and provides data for offline analysis. The medium window length for the inform stage ensures that the operator is informed of the attack as soon as it is determined to be a legitimate threat. The final stage, switch, ensures with the use of a long window length that the system is compromised and the need for a controller switch is necessary. All three stages must be in agreement for the change-out of controllers to occur. The threshold at which the detector monitors for possible cyber-attacks needs to be calculated with respect to the acceptable rate of false alarms.

A bumpless transfer would be the solution to avoid any aggressive disturbances in outputs while allowing a backup controller to be switched with the normal operating controller at any time. The logic and secondary controllers were developed according to the MTDC model discussed in [4].

The detector framework developed shows significant promise in its ability to quickly and accurately detect cyber-attacks of various types. The generality of the detector allows it to be used to detect other forms of attacks, pushing past the two focused on (reference and initialzation attacks) in this work. It is stressed that tuning the algorithm to the ambient conditions of the system is key to ensuring optimal detection capabilities, especially for a predetermined probability of false alarm. By first determining an acceptable rate of false alarm, then calculating the threshold, the detector is easily tuned to the system's needs. Window lengths may be varied, providing one or more additional degrees of freedom with respect to tuning the rate of detection. Care must be taken to titrate the tradeoffs for optimal detection while minimizing the impact on operations while not under attack.

5.0 Future Work

As the progression in these fields continue it is necessary for the research to continue simultaneously to update all pieces of the grid together. As stated previously, the energy detector is able to detect a variety of different types of attacks due to the generality of the detector. However, this thesis focused on specific types of attacks to show how the detector would function against them. This leaves research to be done in studying a wider range of attacks and if any types of attacks are not consistently detected with this particular energy detector then a new method of detection can be explored. As well, tests can be ran to determine how the detector and corresponding systems would react to a hardware failure in the control system. Combining this detector technology with other detectors could be a possible solution to creating an optimized detector for all forms of cyber-attacks.

Continued progress in the area of bumpless transfer technology can include connecting the logic for the bumpless transfer to separate proportional integral derivative (PID) controllers that could then link back into the system. The logic will recognize when the controller is being switched and with that knowledge it could alert a PID controller which would temporarily take over the input for reactive and active power. The PID controller could use a feedback loop to smooth out the transition if the inputs on the secondary controller are different. If the secondary controller has the same inputs it will also work. Once the new input has been reached inside the PID loop then it would pass control back over to the secondary control. This would allow the system to be prepared for a sudden change of inputs or for the same inputs. It would be the final step in completing the bumpless transfer. The large bumps that were seen in Figures 3.8 and 3.9 would be left as smooth transitions. There are other options that could also be pursued in finishing the bumpless transfer and all possibilities should be explored to find the best and most efficient solution.

References

[1] M. P. Bahrman and B. K. Johnson, "The ABCs of HVDC Transmission Technologies: An Overview of High Voltage Direct Current Systems and Applications," *IEEE Power & Energy Magazine*, pp. 32–44, 2007.

[2] M. P. Bahrman, "Overview of HVDC Transmission," *IEEE Power Systems Conference and Exposition*, 2006.

[3] D. Roberson, H. C. Kim, B. Chen, C. Page, R. Nuqui, A. Valdes, R. Macwan, and B. K. Johnson, "Improving Grid Resilience Using High-Voltage dc: Strengthening the Security of Power System Stability," *IEEE Power Energy Magazine*, pp. 38–â47, Apr 2019.

[4] J. Hatton, "*Potential Cyber-Attack Detection and Mitigation Techniques for MTDC VSC*," Master's thesis, University of Idaho, August 2018.

[5] A. Yazdani and R. Iravani, *Voltage-Sourced Converters in Power Systems*. Wiley, 1 ed., 2010.

[6] B. Zhu and S. Sastry, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy," *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, vol. 11, 2010.

[7] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the Next Generation of Real-Time Control, Communication, and Computations for Large Power Systems," *Proceedings of the IEEE*, vol. 93, pp. 965–979, May 2005.

[8] J. Hatton, B. K. Johnson, D. Roberson, and R. Nuqui, "Increased Grid Resilience Via Cyber-Secure VSC Multiterminal HVDC Systems," in *2019 IEEE Power Energy Society General Meeting (PESGM)*, pp. 1–5, 2019.

[9] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks," *IEEE Transactions on Smart Grid*, vol. 3, pp. 1362–1370, Sep. 2012.

[10] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *IEEE PES General Meeting*, pp. 1–6, 2010.

[11] D. Roberson and J. F. O'Brien, "Variable Loop Gain Using Excessive Regeneration Detection for a Delayed Wide-Area Control System," *IEEE Transactions on Smart Grid*, vol. 9, pp. 6623–6632, November 2018.

[12] Y. Zhao, D. Ma, and J. Zhao, "Almost output regulation bumpless transfer control for switched linear systems," *IET Control Theory Applications*, vol. 12, no. 14, pp. 1932–1940, 2018.

[13] G. Qin, Z. Duan, G. Wen, Y. Yan, and Z. Jiang, "An Improved Anti-Windup Bumpless Transfer Structures Design for Controllers Switching," *Asian Journal of Control*, vol. 16, 07 2014.

[14] D. Roberson and J. F. O'Brien, "Loop shaping of a wide-area damping controller using HVDC," *IEEE Transactions on Power Systems*, vol. 32, pp. 2354–2361, May 2017.

[15] N. M. Kangwa, C. Venugopal, and I. E. Davidson, "A review of the performance of VSC-HVDC and MTDC systems," in *2017 IEEE PES PowerAfrica*, pp. 267–273, 2017.

[16] Jiebei Zhu and C. Booth, "Future multi-terminal HVDC transmission systems using Voltage source converters," in *45th International Universities Power Engineering Conference UPEC2010*, pp. 1–6, 2010.

[17] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory.* Prentice Hall, 2 ed., 1998.

[18] A. DasGupta, *Asymptotic theory of statistics and probability.* Springer, 2008.

[19] D. Jovcic and A. Khaled, *High-voltage direct-current transmission: converters, systems and DC grids.* John Wiley & Sons Ltd., 2015.