2018

Cyber attack-defense analysis for automatic generation control with renewable energy sources

Srikrishna Sarangan
Iowa State University

Recommended Citation

Sarangan, Srikrishna, "Cyber attack-defense analysis for automatic generation control with renewable energy sources" (2018). *Graduate Theses and Dissertations*. 16455.
https://lib.dr.iastate.edu/etd/16455

Cyber attack-defense analysis for automatic generation control with renewable energy sources

by

Srikrishna Sarangan

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Electrical Engineering

Program of Study Committee:
Manimaran Govindarasu, Major Professor
Venkataramana Ajjarapu
Zhaoyu Wang
Doug Jacobson

The student author and the program of study committee are solely responsible for the content of this thesis. The Graduate College will ensure this thesis is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2018

DEDICATION

Dedicated to my parents and my brother.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NOMENCLATURE

ACE	Area Control Error
AGC	Automatic Generation Control
BA	Balancing Authority Area
CPS	Cyber Physical System
DER	Distributed Energy Resources
DoS	Denial of Service
ICS	Industrial Control System
IT	Information Technology
MSSC	Most Severe Single Contingency
PID	Proportional Integral Derivative
PMU	Phasor Measurement Unit
RAS	Remedial Action Scheme
ROCOF	Rate of Change of Frequency
RTU	Remote Terminal Unit
SE	State Estimation
SPS	Special Protection Scheme
UFLS	Under Frequency Load Shedding
WAC	Wide Area Control
WAM	Wide Area Monitoring
WAMPAC	Wide Area Monitoring Protection and Control
WAN	Wide Area Network
WAP	Wide Area Protection

ACKNOWLEDGMENTS

I would like to express my biggest thanks to my advisor, Dr. Manimaran Govindarasu, for his continuous guidance and encouragement throughout the course of my research. I would like to thank my committee members, Dr. Venkataramana Ajjarapu, Dr. Zhaoyu Wang, and Dr. Doug Jacobson, for consenting to be a part of Program of Study committee and supporting me throughout the course of this research. I thank my colleagues and fellow graduate students Aditya Ashok, Pengyuan Wang, Vivek Kumar Singh, Subramanian Arunachalam, Jacob Drahos, Jacob Ulrich, Haythem Ebrahem and Steven Perez who were willing to assist and help me out.

In addition, I would also like to thank my friends, the department faculty and staff for making my time at Iowa State University a wonderful experience. Without them, this thesis would not have been possible.

ABSTRACT

The advancements in the power grid due to integration of new technology arises concerns regarding its reliability in terms of performance and security. On one hand, the gradual shift towards renewable energy sources leads to rise in uncertainty in terms of control and demand satisfaction. On the other hand, the integration of communication devices in order to make the grid smart increases its vulnerability to malicious activity. Automatic Generation Control (AGC), which is needed to maintain the system frequency and inter-area exchange, has an important priority in both the concerns. With rising shares of renewables and retiring of fossil-fuel based generation, a grid almost entirely served by renewables is a highly possible scenario. In such cases, the impact of an attack on the grid is likely to be influenced by the effect of renewables. Although previous research conducted crucial studies of malicious cyber events on the power grid, analysis in the presence of renewables is still at a nascent stage. As a contribution, this thesis presents an attack-defense analysis on the AGC operation of the power grid under varying conditions of renewables. It has two main contributions – determination of the influence of renewables during an attack and development of an effective algorithm for defense.

First, this thesis discusses a cyber-attack on the AGC algorithm with various levels of renewable penetration, to analyze the effect of an attack with renewables. The results confirm that the impact of a cyber-attack will be increasingly aggravated by displacement of conventional generation with renewables. Then an algorithm for AGC using a PID based approach aimed at reducing the impact is proposed. From the experiments, the proposed algorithm is shown to reduce the impact of the attack. Secondly, an algorithm for attack mitigation is designed and its performance is analyzed for both the AGC algorithms. The various factors tested are its effectiveness in reducing the impact on the system, and its adverse effects on AGC operation during normal conditions and contingency response. The results show that the algorithm could mitigate the attack without having a negative impact on normal AGC operation. The contingency response analysis shows that during events resulting in a significant change in generation-load balance, the response could be adversely affected by the mitigation. The experiments were conducted using the Power Cyber CPS security testbed at Iowa State University.

The thesis further briefly discusses the prospective research considering various developments in the power grid, renewables and attack vectors.

CHAPTER 1 **INTRODUCTION**

The smart grid consisting of complex power network and more complex communication network faces increasing challenges in reliability, security and stability with its growth. As the shift to sustainable energy sources is on the rise, the reliability of stable power delivery becomes more fragile [8]. The need for superior control methods in order to counter the effects of uncertainty and instability introduced by the renewable sources is evident. An even greater problem is the growing threat of malicious activity in cyber-space. With the push towards making the grid smarter, critical industrial control systems (ICS) such as the power grid have become as vulnerable to cyber threats, as their counterparts in information technology such as banking, share markets, service sectors, etc. This is further undermined by the retention of legacy equipment in order to optimize costs and complexity faced during the transformation. With increasing interdependence between the physical and cyber networks [32], the impact of any attack can be astronomical. The December 2015 attack on the Ukrainian power grid which affected thousands is one of the most sophisticated attack on the power grid [34]. The ability of the attackers in performing long-term reconnaissance operations to learn about the system and a highly synchronized attack, served as an eye opener and as quoted, “a wakeup call” in coming to terms with the fact that these events are far from being merely an unpleasant hypothesis.

SCADA Overview

The smart grid is one of the largest and most complex systems made, that spreads over large geographical areas and comprising of the traditional physical system to provide the basic functionality, and the cyber network for support in control and management. Figure 1.1 shows the layout of the smart grid. The physical layer consists of the power system which includes the generation, transmission, distribution systems, and equipment for measurement, protection, etc. The communication layer includes the control center and substation Remote Terminal Units (RTU), devices such as phasor measurement units (PMU) which are directly connected to the communication layer, smart meters, etc.

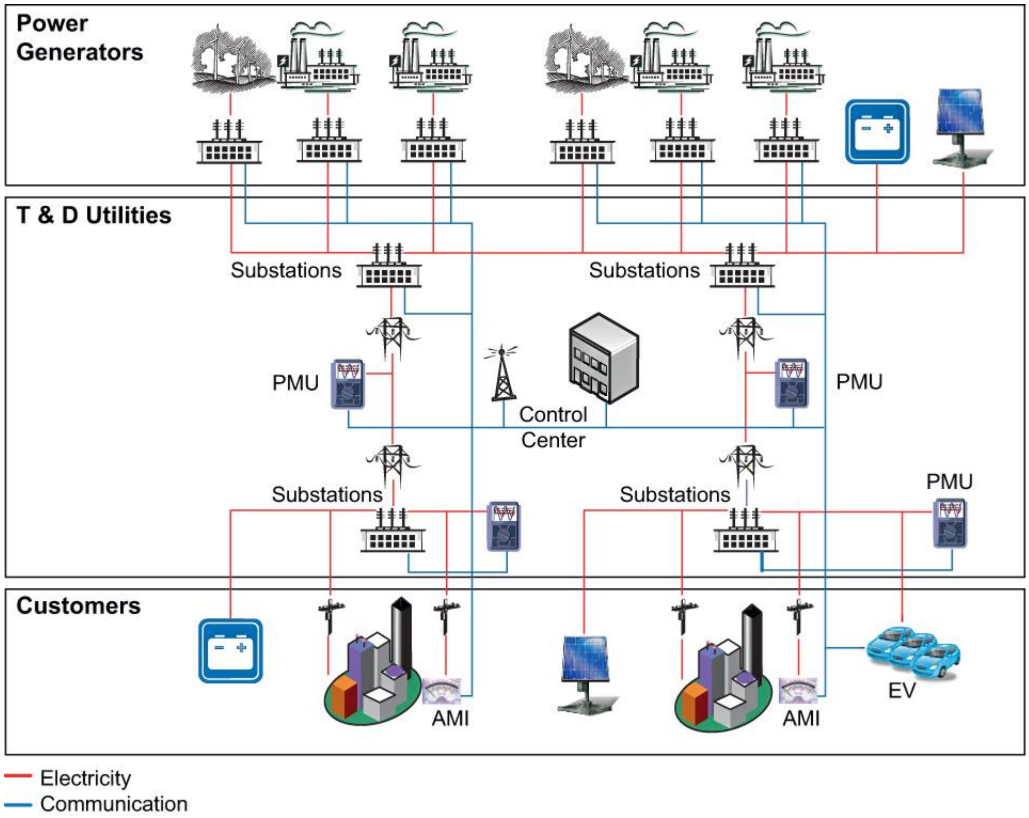

Figure 1.1 Smart grid layout

Wide Area Monitoring, Protection and Control (WAMPAC) operations, viz., State Estimation (SE), Remedial Action Scheme (RAS) and Automatic Generation Control (AGC) are the most crucial tasks that help in maintaining stability, adequacy and security [30].

Wide Area Monitoring (WAM) is performed by SE and is used to obtain values of the critical system parameters or states used to analyze system stability. Wide Area Protection (WAP) is used to help restore the system stability during any abnormal events such as faults, overloads, etc. One of the methods is Special Protection Scheme (SPS) or RAS which detects unhealthy system conditions and performs the necessary action to prevent the situation from aggravating. Wide Area Control (WAC) is accomplished using Automatic Generation Control (AGC) that helps maintain the system frequency, load balance and inter-area exchange using control loops.

The signals necessary for these operations are transmitted through the cloud and are thus vulnerable to malicious activity that can adversely affect the grid. The following sections describe the current scenario and briefly depict the previous work that has been done in the respective areas.

Cyber Security of Smart Grids

Although the WAMPAC applications operate with the objective of maintaining the power grid stability, they are traditionally unequipped to deal with cyber threats. With increasing devices connected to the cyber layer and complexity of system operations, the risk posed by cyber-attacks has reached alarming levels. The retention of legacy equipment while conversion to smart system poses a serious threat. Power grids were previously connected using traditional communication devices. While conversion to smart systems, these devices are directly connected to the internet without sufficient secure equipment, so as to avoid costs and inconvenience. This leaves the smart grid with a lot of vulnerabilities to cyber-attacks. The lack of compatibility of traditional IT security measures to address the security needs of Industrial Control Systems (ICS) is also an issue.

There is a growing spike in attacks in cyberspace over the past years. Malware based attacks, like Stuxnet that corrupted the ICS of nuclear fuel enrichment equipment, are being widely used repeatedly in several applications. The attacks on the Ukrainian power grid in 2015 and 2016 were the first major attacks on a power grid and affected more than 200,000 customers. Hence, research in this area to identify potential attacks and development of effective security measures is of crucial importance.

There has been extensive research in analyzing attacks and impacts on WAMPAC operations. Aditya et.al. present an implementation of a successful data integrity attack on AGC operation on the Power-cyber testbed at Iowa State University [9]. Siddharth et.al. provide a descriptive analysis for various attacks on AGC operation, and also provide an effective mitigation algorithm employing a model based anomaly detection that uses real time load forecast [10]. Siddharth et.al in [11] describes attack models for integrity and DoS attacks, and develops templates for attack on AGC. Aditya et.al. in [12] present an attack defense analysis by conducting stealthy attacks on AGC and a mitigation using model based anomaly detection techniques. In [13], Aditya et.al discuss about attack resilient architecture for WAMPAC by developing a detailed framework that addresses the entire security cycle of risk assessment, attack prevention, detection, mitigation and resilience. They also provide a defense-in-depth architecture that elaborates security at both infrastructure and application layers, and discuss various issues faced in implementing security measures. Tan et.al. in [14] discuss an optimal approach towards developing an attack vector on AGC by analyzing the impacts on the system due to several attacks based on captured sensor measurements and system data. Siddharth in [31] presents an in-depth study on risk modeling and analysis for coordinated attacks, and provide an online mitigation strategy using heuristics based contingency analysis and attack resilient control using real time load forecasts. In [33] Vivek et.al. discuss an approach to stealthy cyber-attacks on RAS operation of a power grid using a coordinated attack involving malware based system corruption and modification of signals, considering multiple values of the attack parameter.

Integration of Renewable Energy Sources

One of the biggest revolutions in the power grid is the shift towards renewable energy sources, wind and solar being the major share. There is a global trend towards conversion to cleaner and sustainable energy sources. Most nations have renewables up to at least 10% of their total capacity. Some of the driving factors for this shift include [36]:

1. Environmental impact of fossil fuel based generation.
2. Depleting fossil fuel reserves.
3. Low operational costs.
4. Growing energy demand.
5. Ability to electrify remote locations without dependence on the transmission network.

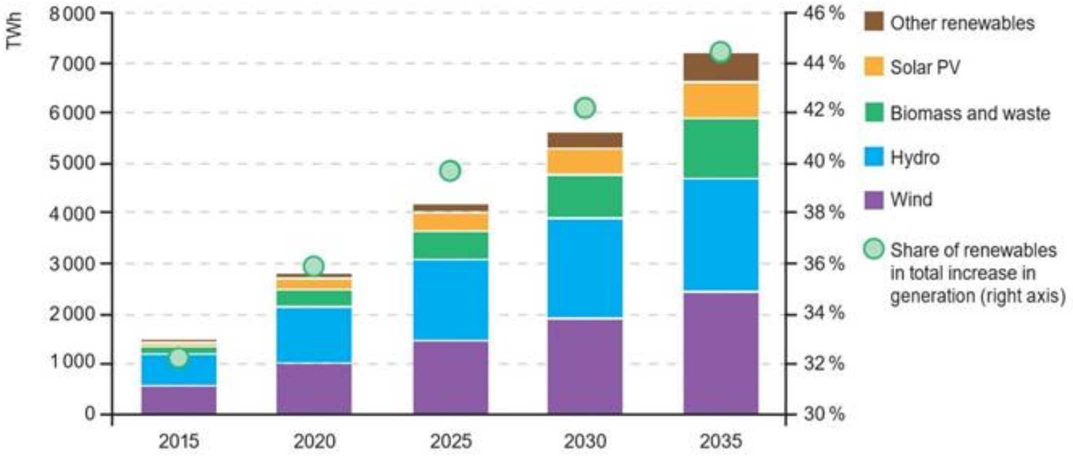

Figure 1.2 Incremental global renewables-based electricity generation relative to 2009 by technology (Figure from [36])

The graph in Figure 1.2 shows the expected increase in generation capacity for each technology over the next two decades. It is evident that in the future nearly half of the added capacity will be renewable based generation. Also, considering that many nations are planning to retire fossil fuel based power plants, a power grid that is served almost entirely by renewable generation is not an unexpected scenario.

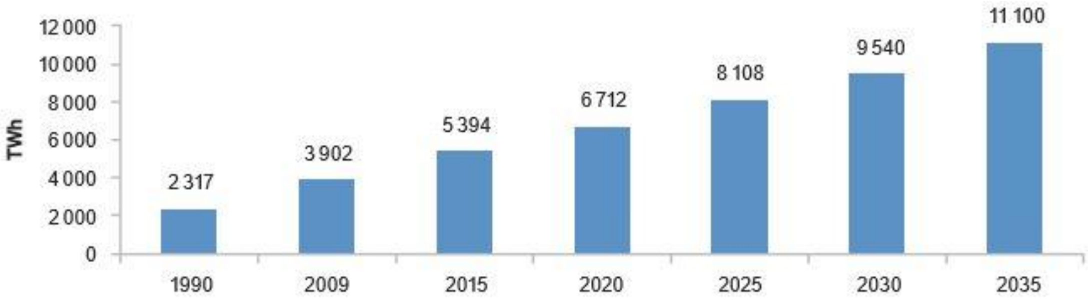

Figure 1.3 Expected global renewable generation (Figure from [36])

From the graph in Figure 1.3, that shows the expected growth in energy generation by renewables, it can be inferred that net generation by renewables is predicted to double within the next two decades. However, these changes arise serious concerns about reliability. The unpredictable nature of renewable sources is a major contributor to the instability in the power grid. With its rapid influx, there is a crucial need for efficient load frequency control. Although the impact of renewables on the power grid has not been completely assessed, studies have generated numerous important findings as given below:

1. Partial unpredictability or uncertainty due to limitations in forecast.
2. Fluctuating output power or variability due to varying wind and solar input, leading to frequency fluctuations.
3. The above property has led to decline in control performance metrics such as CPS1.
4. Reduction in system inertia causing faster frequency response and increased Rate of Change of Frequency (ROCOF).

A detailed description of the factors to be considered while integrating significant content of renewables is provide in [4]. This thesis considers two of the factor discussed in [4] - inertia and regulation.

There has been significant research in the direction of reliability and real-time markets in the presence of renewables. There is widespread study in this area with debates on various techniques. Multiple methods have been suggested as alternatives to the conventional AGC with or without considering renewables. Arman et.al in [15] present a hierarchical control architecture that includes market mechanisms, economic dispatch and frequency regulation for a system with uncertain load and generation. Zhang et.al propose a consensus based controller approach to AGC using distributed load side frequency regulators with the impact of renewables on the system frequency [16]. Keyhani et.al. developed an alternative to expensive spinning reserves used for integration with renewable sources using a three-step method involving addressing load fluctuations, calculating accurate set points for generators, and fast cyber communication for monitoring and control [17]. In [18] Gauthier et.al. discuss a dynamic frequency control system for isolated grids using fast acting energy storage units to provide inertial response and improve transient performance. Moslehi et.al in [21] describes the existing scenario for smart grids elaborating on the challenges faced in reliability and security due to trend towards renewables, while weighing on the need for protective measures and analyzing their technical feasibilities.

Another grave concern is the effect of the presence of renewable in the event of a cyber-attack. This is an area that has seen very useful, although limited exploration. In [19] Ayar et.al propose a nonlinear distributed controller that improves transient stability margins of synchronous generators by means of distributed storage systems, that helps during disturbances caused due to cyber-attacks, while also considering resilience to time delays that are introduced during communication. Giovanna et.al. conducts a cyber risk assessment study and suitable mitigation by means of security measures, on the voltage regulation of medium voltage equipment that connect Distributed Energy Resources (DER) to the rest of the grid, in [22]. Moness et.al presents an overview of Internet of Energy (IoE) and next generation Wind Energy Control Systems (WECS) while considering the challenges of integration and concerns about cyber security in [27].

Table 1.1 SCADA advancements in the power grid

Publication title	**Topic addressed**		
	Cyber security	**WAMPAC application**	**Renewable integration**
Experimental evaluation of cyber-attacks on automatic generation control using a cps security testbed.	✓	✓	✗
Model-based attack detection and mitigation for automatic generation control.	✓	✓	✗
Data Integrity Attacks and their Impacts on SCADA Control System.	✓	✓	✗
Testbed-based performance evaluation of Attack Resilient Control for AGC.	✓	✓	✗
Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid.	✓	✓	✗
Optimal False Data Injection Attack against Automatic Generation Control in Power Grids.	✓	✓	✗
A Hierarchical Transactive Control Architecture for Renewables Integration in Smart Grids: Analytical Modeling and Stability.	✗	✓	✓
Distributed Load-Side Frequency Regulation for Power System.	✗	✓	✓
A New Automatic Generation Control with Heterogeneous Assets for Integration of Renewables.	✗	✓	✓
Dynamic Frequency Control Support by Energy Storage to Reduce the Impact of Wind and Solar Generation on Isolated Power Systems Inertia.	✗	✓	✓
A Distributed Control Approach for Enhancing Smart Grid Transient Stability and Resilience.	✓	✗	✓

Table 1.1 (continued)

A reliability perspective of the smart grid	✓	✗	✓
Impact of DER integration on the cyber security of SCADA systems—The medium voltage regulation case study	✓	✓	✓
A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy	✓	✗	✓
Stealthy cyber-attacks and impact analysis on wide-area protection of smart grid	✓	✓	✗

From Table 1.1, it can be seen that despite all these valuable contributions, there is a scarcity of research on the attack-defense analysis of any WAMPAC applications in the presence of renewable energy sources. This thesis aims to bridge the gap by conducting an attack defense study on the AGC operation of the smart grids with renewables integrated.

Thesis Motivation

The importance of security for the smart grid has rapidly gained a foundation over the past few years, especially with the recent attacks on the Ukrainian power grid in 2015 and 2016. Although information technology (IT) security has often been reliable, it is not always suitable for cyber security of ICS. This is due to the security priorities of the system data, i.e. in IT security Confidentiality is the most critical property, while in ICS security, Availability takes a higher importance. This arises the need to develop security features that go beyond the realms of traditional cyber security onto cyber physical security, where the physical characteristics of the system must be taken as essential factors. The changing nature of the grid involving increasing renewable is also an important detail to be analyzed. The study on cyber-attacks on power grid operations such as AGC in the presence of renewables has very limited exposure. Due to the increased variability in the presence of renewables, WAC operations become more important for grid stability. Also, attacks on such applications are likely to have an immediate effect due to their high frequency of operation. The impact of attacks on frequency regulation can be aggravated by the presence of non-conventional sources. This reemphasizes the grave importance of this topic.

This thesis emphasizes on the following needs:

1. Modelling of power grid with renewables integrated with adequate accuracy.
2. Development of alternate control algorithm from a cyber defense perspective.
3. Attack and defense analysis on power system with various system conditions.

Thesis Organization

The main objectives of this thesis are to analyze the effect of cyber-attacks on a power grid with renewables integrated, and to provide an effective mitigation strategy against the attack. The organization of the thesis is as follows:

1. Chapter 2 describes the attack on the AGC of the power system. It also introduces a PID based AGC algorithm and performs impact analysis on both the results.
2. Chapter 3 presents a strategy for mitigation against the attack and analyses the performance and false alert property.
3. Chapter 4 concludes the thesis and discusses scope for future study.

CHAPTER 2 **ATTACK ANALYSIS**

Overview of AGC

Automatic Generation Control (AGC) is a WAC operation used for secondary load frequency control of the power system after the primary control (i.e. governor action). The chief objectives of the operation are:

1. Balance the net generation with the net load
2. Maintain the frequency at set value (60 Hz or 50 Hz)
3. Maintain the tie-line flows between the balancing authority areas (BA)

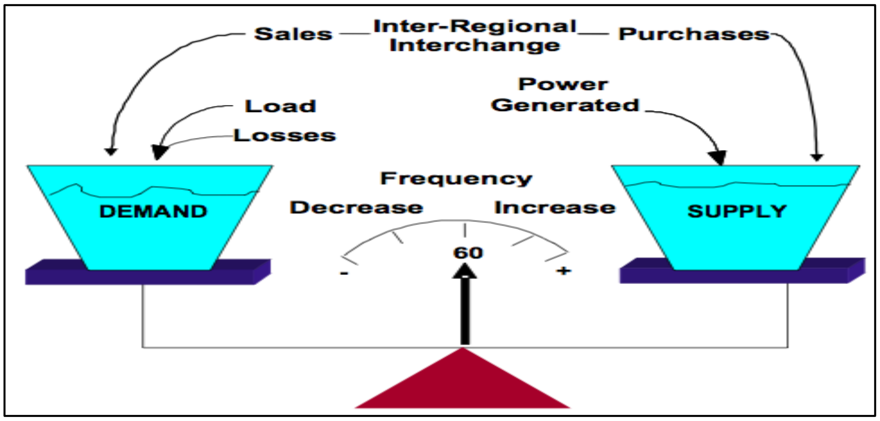

Figure 2.1 Load balancing and frequency control (Figure from NERC)

The target frequency bound in the North American grid varies with interconnection [6].

Eastern interconnection = 18 mHz

Western interconnection = 22.8 mHz

ERCOT interconnection = 30 mHz

Quebec interconnection = 21 mHz

The algorithm uses instantaneous frequency and inter-area tie line flow values to calculate the Area Control Error (ACE) every 2 to 4 seconds. It ensures that each BA is responsible for its own load changes. In the conventional AGC operation, the ACE values are added up to generate the control input.

$$\text{ACE, } E = \beta . \Delta f + \sum_{i=1}^{n} \Delta P_i \qquad (2.1)$$

where, β – frequency bias factor

Δf – frequency deviation

ΔP_i – 'ith' tie line flow deviation

$$\text{Control input, } C(t) = \sum_{t=0}^{n} E_t \qquad (2.2)$$

where, E_t – ACE value at cycle 't'

Attacks on AGC

Attacks on AGC can be classified based on different criteria.

Based on the method, the attacks can be classified as:

1. Replay attack – A copy of a previously observed packet is replayed to the target resulting in incorrect action.
2. Denial of Service (DoS) – The communication is stopped by flooding the target with packets causing a channel overuse resulting in lack of operation.
3. Data integrity attack – The values in the packet are modified by the attacker resulting in incorrect action.

4. Timing attack – The packet is captured by the attacker and released at a later instance resulting in incorrect action.

Based on the template of the attack, the classification is as follows [10]:

1. Scaling attack – A scaling parameter is used to modify the values.
2. Ramp attack – A constant value is sent to the target continuously for several cycles.
3. Pulse attack – The values are modified using temporally spaced short pulses with a fixed attack value.
4. Random attack – Using values generated by a uniform random function, the packet values are modified.

Based on the target, there are two types of attacks:

1. Attack on sensor values
2. Attack on ACE values

This thesis analyses a ramp attack on the ACE values.

Experimental Setup

The analysis was conducted on an IEEE 39-bus model using RT-LAB and Matlab/Simulink as the editor. The system is divided into two BAs as shown in Figure 2.2. Generators 1 & 8, and 2 & 3 are involved in AGC operation in BA1 and BA2 respectively.

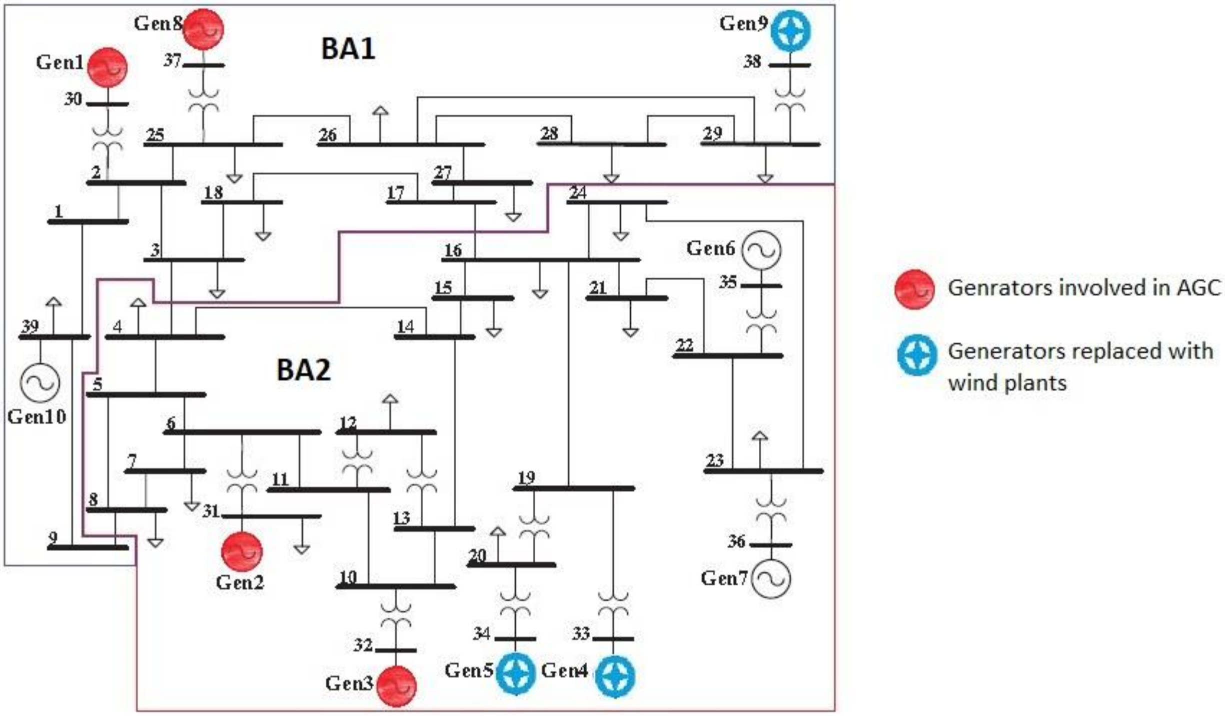

Figure 2.2 IEEE 39 bus model

The model was modified to simulate renewable energy sources. Generators 4, 5 and 9 were converted to renewables successively for simulating increasing renewable penetration. For conversion to a renewable source (Figure 2.3), the single large machine was replaced by 100 machines, each with a power rating of 1% of the original value & with an inertia of 0.1% of the single large machine. Each smaller machine was simulated with an input value subject to 1% fluctuation, to simulate the variation in the wind turbine output.

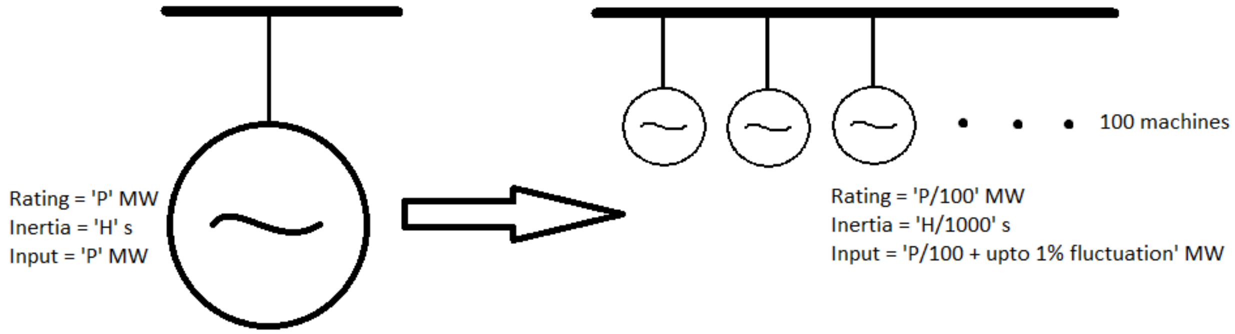

Figure 2.3 Generator conversion from conventional system to renewables

Figure 2.4 shows the modelling of the experimental setup. The generator station (substation) consists of the power system model, that sends out the observed sensor values, and the block for calculating the control signal using the ACE values. The control center consists of the block involved in performing the AGC calculations and returning the ACE values to the generators. The attack takes place on the ACE values.

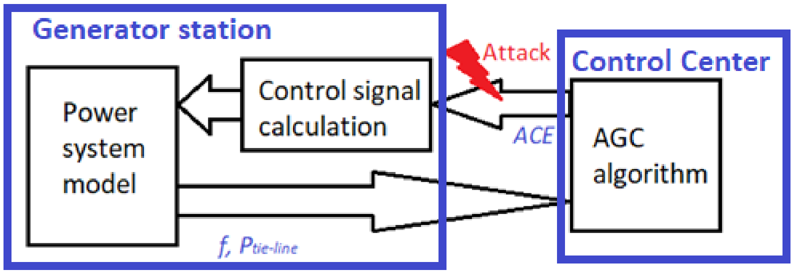

Figure 2.4 Experimental setup layout 1

Ramp Attack

A ramp attack was conducted on the system. In this case, a constant ACE value was sent to the generator station for the attack duration, resulting in a constant increase or decrease of the generator output which leads to a constant raise or drop in system frequency (Figure 2.5). This action is performed by either a replay or data integrity attack. A significant drop in frequency causes adverse frequency conditions leading to performance criteria violation, under-frequency load shedding, generation trip and loss of turbine life.

$$\text{Control signal after attack, } C(t+t_a) = C(t) + E_a * t_a \tag{2.3}$$

where, E_a – Attack magnitude

t_a – No. of attack cycles

$C(t)$ – Control signal at the start of the attack

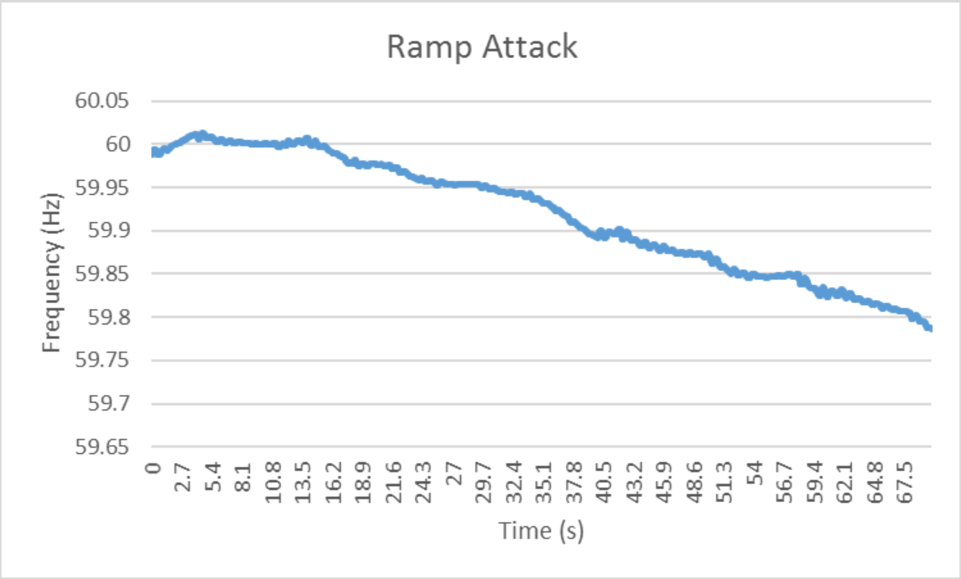

Figure 2.5 Effect of ramp attack on frequency

Case study with Conventional AGC

The attack was conducted on two cases – attack on one ACE and two ACE values, for four different conditions of renewable penetration – 0%, 10%, 20% and 30%. The increase in renewable penetration has two consequences on the grid:

1. Fluctuating output power leading to frequency fluctuations

2. Reduction in system inertia leading to faster frequency response and higher rate of change of frequency (ROCOF)

The ACE value was attacked and replaced with -5 MW for a duration of 2 minutes (120 seconds or 30 AGC cycles) causing a drop of 150 MW of generation. When both the ACE signals are attacked there is a drop of 300 MW.

From the plots in Figure 2.6, it can be inferred that with increase in renewables, due to reduction of inertia, the ROCOF is higher and the frequency drop due to the attack is faster.

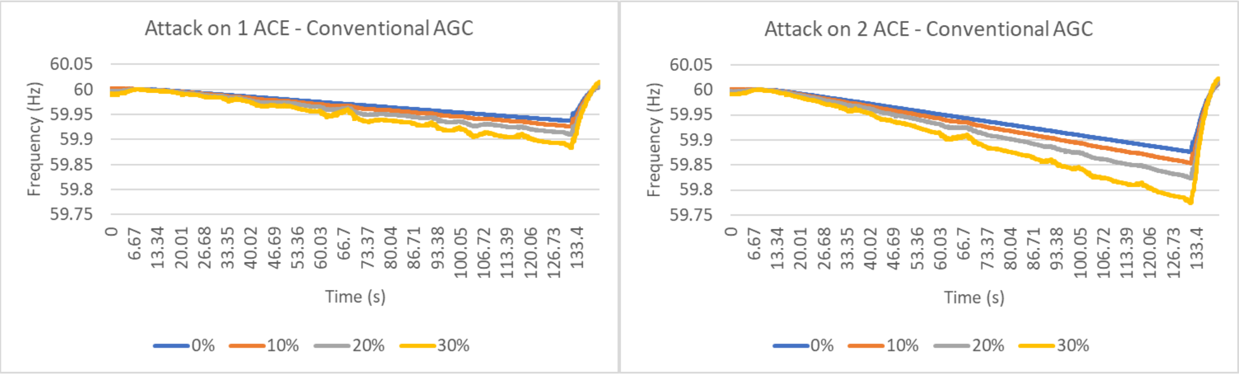

Figure 2.6 Effect of ramp attack on conventional AGC for varying levels of renewable penetration

To recover from the frequency drop, the grid responds by shedding some predetermined value of load (i.e. Under Frequency Load Shedding (UFLS)). This action is triggered at some value of frequency decided by the regulators. Typically, in the Eastern interconnection, the upper limit of this trigger point in 59.7 Hz [37]. Following this reduction in load, the frequency increases towards 60 Hz. Figure 2.7 depicts the effect of the ramp attack on one of the cases (viz. with 30% renewable penetration and attack on both ACE values) countered by UFLS. In this experiment the attack duration was for 3 minutes (45 AGC cycles). After 160 seconds, when the frequency reaches the under-frequency trigger point, 400 MW of load was shed to help recover the frequency. The attack continued for another 20 seconds causing the frequency to reduce by 50 mHz. After the attack ended, AGC was restored and the frequency condition returned to normal.

Currently, there are no measures established by regulators to help restore the frequency before UFLS occurs in the event of an attack. Thus, unless the operator manually takes an action such as load trips, using backup generators, etc., frequency recovery before 59.7 Hz is not possible.

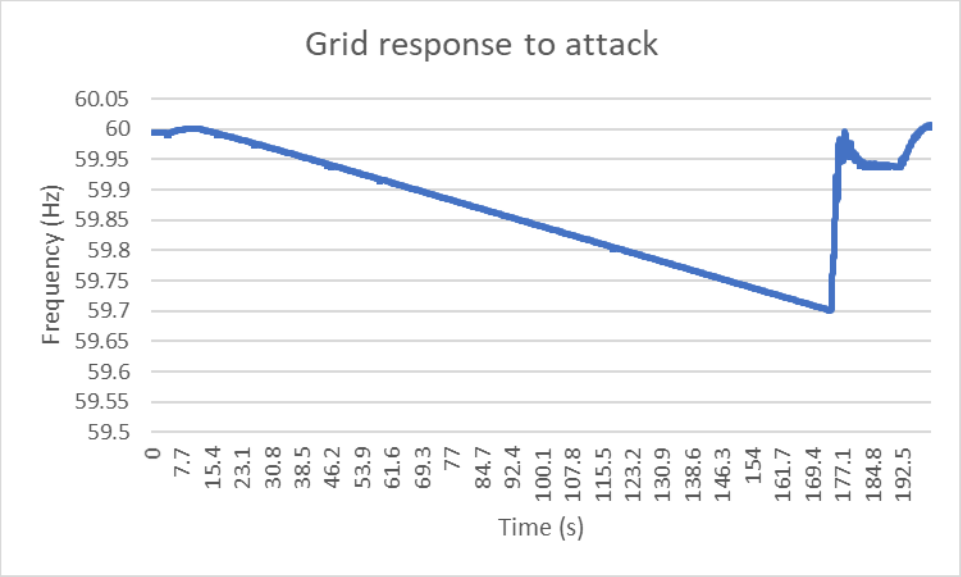

Figure 2.7 Effect of ramp attack countered by UFLS

Impact of high renewable penetration

From the above experiments, it was observed that increasing renewable shares may lead to higher impact during a cyber-attack. This raises concerns with respect to integrating more renewables. Due to reduction in inertia and increasing variability, any attack that causes a disturbance or change in system frequency is likely to have a faster impact. For example, a system with extremely high share of renewables might face an even faster drop in frequency during a ramp attack, and hence load shedding might be necessary sooner and/or even multiple times. Also, due to higher variability with a high renewable presence, a simple DoS attack would be capable of destabilizing the system. One preventive measure is inertial emulation, using power electronic controllers to simulate inertial action similar to conventional generation. Another method is using superior governor control to reduce frequency fluctuations.

One advantage with higher renewables is the faster frequency recovery due to any restoration techniques because of higher ROCOF. This can be observed from the plot in which the frequency recovery due to UFLS occurs within 3 seconds.

PID Based AGC

To help reduce the impact of the attack, a PID based control algorithm was developed. This involves modifying the control signal algorithm to help reduce the impact while retaining the AGC performance.

Conventional AGC defines control signal,

$$C(t) = E_0 + E_1 + E_2 + \cdots + E_t$$

This can be rearranged in a PID format as,

$$C(t) = 1 * E_t + 1 * (E_0 + E_1 + \cdots + E_{t-1}) \tag{2.4}$$

where, $1 * E_t$ – represents the proportional component

and, $1 * (E_0 + E_1 + \cdots + E_{t-1})$ – represents the integral component.

By modifying the formula to include a derivative component and variable PID parameters, the control signal is derived as,

$$C(t) = K_P * E_t + K_I * (E_0 + E_1 + \cdots + E_{t-1}) + K_D * (E_t - E_{t-1}) \quad (2.5)$$

PID parameter selection

From equation 2.5, it can be inferred that changing the values of the PID parameters will vary the effect of the ramp attack. Thus, to reduce the effect, the parameters should have values lesser than 1. However, it is necessary to ensure that the AGC performance is not compromised. The values of the PID parameters are selected to help reduce the impact and maintain satisfactory performance. The best way to do this is to let K_P remain as '1' to ensure the most recent updates in the control are provided during that ACE value's first cycle. A small value of around '0.01' is assigned to K_D to provide the derivative control action based on the rate of change of ACE. The main component that can help reduce the effect of attack is K_I. Through a set of experiments, it was observed that the ideal value is around '0.5' as it retains satisfactory load frequency control. This helps reduce the damage due to the ramping by approximately half.

Case Study with PID Based AGC

The same 8 experiments were repeated for the same attack duration and signal magnitude. But, due to the PID based AGC, by the end of 2 minutes the reduction in generation was only 77.5 MW for attack on 1 ACE, and 155 MW for attack on 2 ACE values. The following observations were made:

1. Attack on PID based AGC has lesser impact due to limiting the control signal which in turn limits generation drop (Figure 2.9).
2. The plot on the left in Figure 2.8 shows that for attack signals of relatively lesser magnitude, with PID based AGC, the effect due to inertial loss is reduced, making the impact due to

change in renewables up to a certain level almost negligible. This is because, for small magnitude of attack there is marginal difference in time taken to attain the frequency level targeted by the generation change for the different conditions of renewable penetration. If the attack signals have a higher magnitude, an impact of similar nature but lesser in magnitude, is observed as shown in the plot on the right in Figure 2.6.

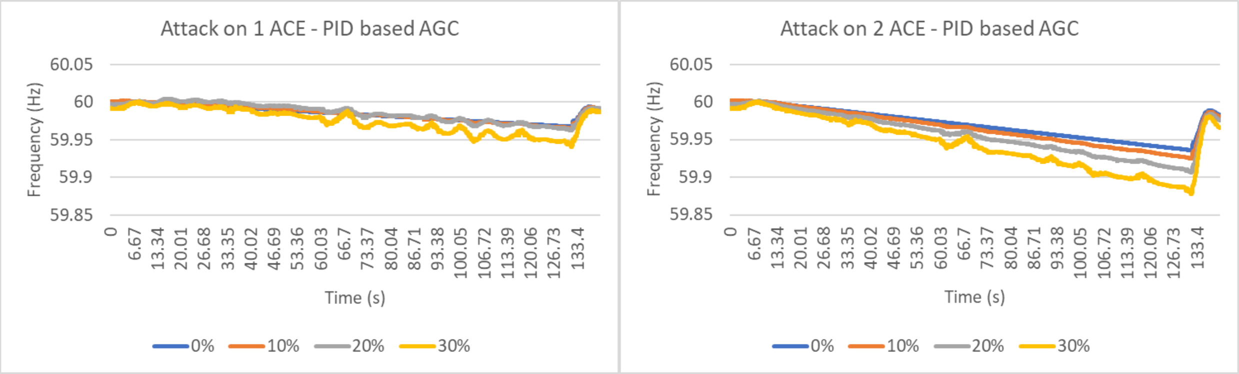

Figure 2.8 Effect of ramp attack on PID based AGC for varying levels of renewable penetration

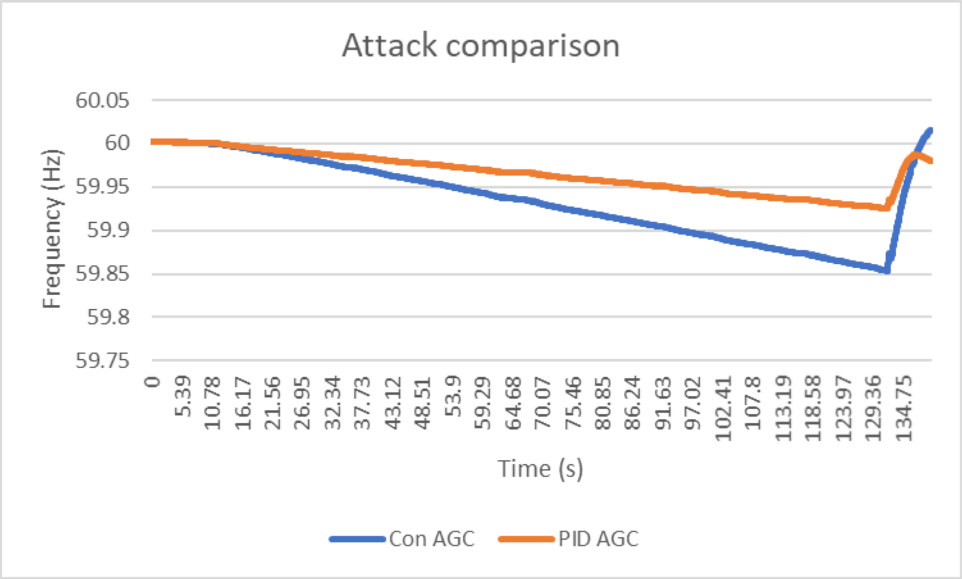

Figure 2.9 Comparison of attack impacts

The experimental results of the attack on the two AGC algorithms shown in Table 2.1 support the conclusions derived in sections 2.5 & 2.7.

Table 2.1 Results of ramp attack

% Renewable Penetration	Frequency drop (Hz)			
	Attack on 1 ACE		Attack on 2 ACE	
	Conventional AGC	PID based AGC	Conventional AGC	PID based AGC
	Generation drop = 150 MW	Generation drop = 77.5 MW	Generation drop = 300 MW	Generation drop =155 MW
0	0.062	0.032	0.122	0.063
10	0.072	0.033	0.143	0.073
20	0.086	0.034	0.172	0.089
30	0.106	0.048	0.214	0.11

AGC performance evaluation

The plots in Figure 2.10 show the AGC performance for both the algorithms under different conditions of renewables in the absence of an attack. The blue and green lines indicate the permissible upper limit (UL) and lower limit (LL) for frequency. It was observed that the PID based AGC algorithm provides a satisfactory performance that is as good as the conventional algorithm, since it manages to maintain the steady state frequency error within the regulation requirements (18 mHz in this case).

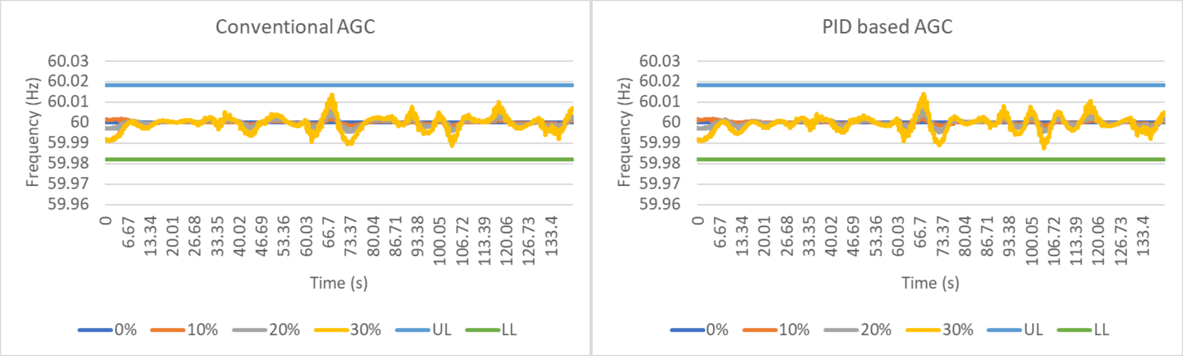

Figure 2.10 AGC performance comparison

Conclusions

The main conclusions obtained from the experiments were:

1. With increase in renewable penetration, there is a reduction in system inertia and thus for the same attack vector, the change in frequency is faster. In this case, the ramp attack leads to a faster drop in frequency with increase in renewable content.
2. PID based AGC that limits the control signals will suffer lesser impact due to an attack than conventional AGC, while maintaining satisfactory performance.

CHAPTER 3 **MITIGATION ANALYSIS**

Mitigation Overview

This chapter discusses a mitigation algorithm that can prevent the attack from affecting the system beyond certain limits. Since the thesis considers attack on the ACE signals, the mitigation algorithm is operated at the terminals of the generating station. Figure 3.1 shows the placement of the mitigation block in the experimental setup. The algorithm validates the ACE value that it receives using several conditions before allowing them through to the control signal calculator.

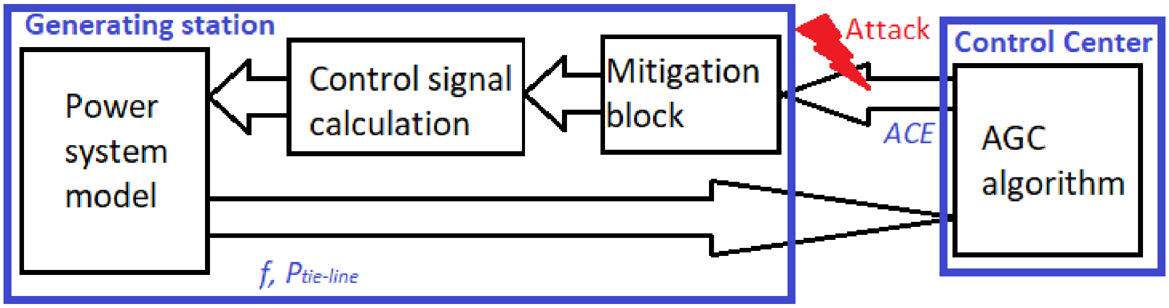

Figure 3.1 Experimental setup layout 2

The algorithm for mitigation is shown in the flowchart in Figure 3.2. After obtaining the ACE value, two conditions are checked:

1. The values are checked to be within a pair of bounds.
2. The sign of ACE is checked with the frequency value to ensure the ACE helps to improve frequency conditions, i.e. for a system frequency < 60 Hz, only a positive ACE value (ramp up signal) will be allowed, and vice-versa.

If either condition is violated, the ACE value is dropped and replaced with 0.

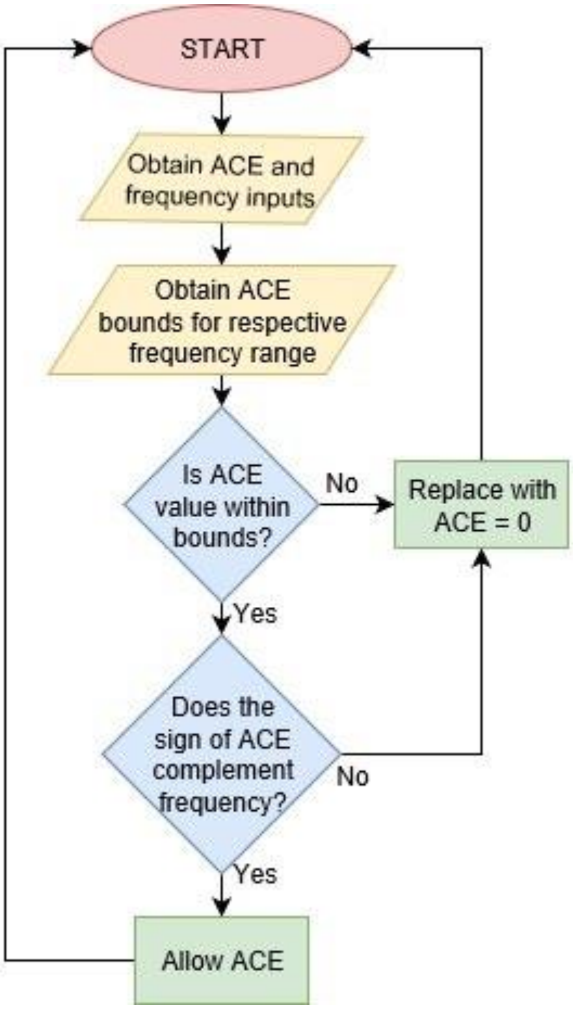
START
Obtain ACE and frequency inputs
Obtain ACE bounds for respective frequency range
Is ACE value within bounds?
No
Replace with ACE = 0
Yes
Does the sign of ACE complement frequency?
No
Yes
Allow ACE

Figure 3.2 Attack detection and mitigation procedure

Assumptions

This mitigation strategy assumes that the generating stations have access only to frequency values and thus cannot use tie-line flow values as a secondary parameter for ACE verification.

Calculating the ACE bounds

The bounds are determined using the data used by regulators for determining the performance parameters of the AGC (viz. Control Performance Standard - CPS1 and the Balancing Authority ACE Limits (BAAL)) [6]. The data consists of one-minute average values of frequency and ACE for a total period of 12 months which are updated every month. These values also include readings obtained for system events such as contingencies, faults, etc. The bounds for each frequency range are the maximum and minimum ACE values observed for that range in the past 12 months. Figure 3.3 describes the method for deriving the ACE bounds.

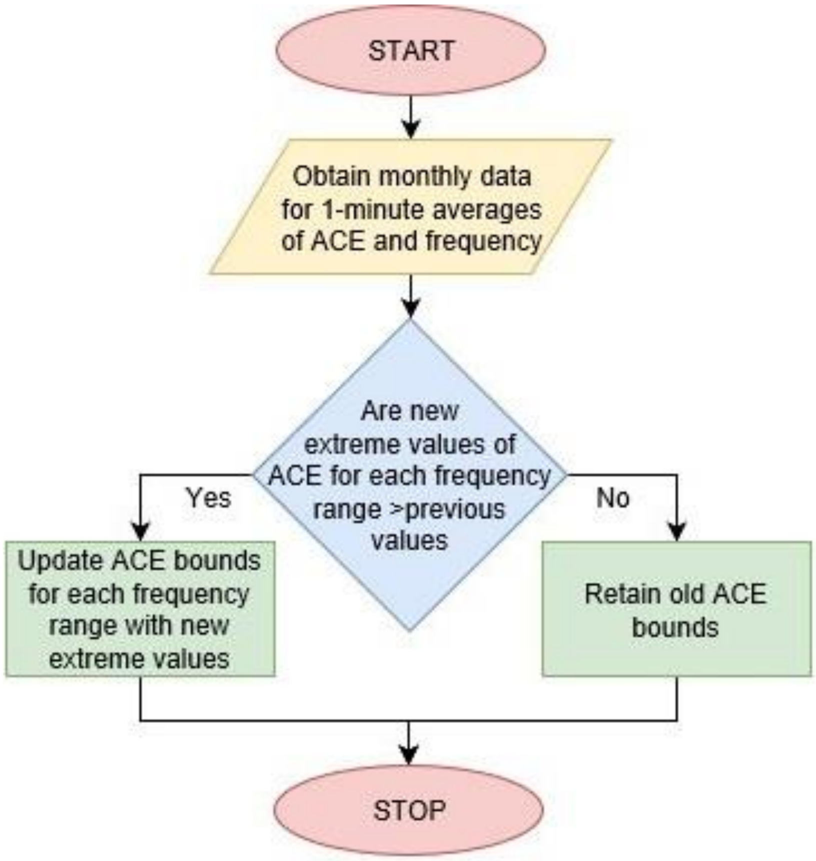
START
Obtain monthly data for 1-minute averages of ACE and frequency
Are new extreme values of ACE for each frequency range >previous values
Yes
No
Update ACE bounds for each frequency range with new extreme values
Retain old ACE bounds
STOP

Figure 3.3 Procedure to determine ACE bounds for mitigation

Table 3.1 provides an example of how the ACE bounds are derived and updated. Let the frequency ranges be divided in blocks of 5 mHz. The bounds used during a month, say June, are obtained from the data of previous 12 months updated by the end of May (i.e. June of previous year to May of current year). While obtaining the bounds for July, the data is updated with the values obtained during the month of June, and the minimum and maximum values of ACE for each frequency range is determined, and the respective bounds are updated with the new values. For example, since the ACE in the range 59.99-59.995 has a new minimum value of -32, the minimum ACE bound is updated with that value. Similar changes can be seen in other parts of the table. For the values that haven't changed, it is assumed that the respective extreme values obtained from the data of June to May is the same as that obtained from July to June.

Table 3.1 Monthly updating of ACE bounds

Bounds for June			**Data obtained in June**		**Bounds for July**		
Frequency range (Hz)	**Min ACE**	**Max ACE**	**Frequency 1-min avg**	**ACE 1-min avg**	**Frequency range (Hz)**	**Min ACE**	**Max ACE**
59.98–59.985	-35	+50	59.994	-32	59.98–59.985	-35	+50
59.985-59.99	-30	+45	60.004	-33	59.985-59.99	-30	+45
59.99–59.995	-30	+40	60.004	-38	59.99–59.995	-32	+40
59.995-60	-25	+35	60.009	+23	59.995-60	-27	+39
60-60.005	-35	+20	59.998	-27	60-60.005	-38	+20
60.005-60.01	-45	+20	59.996	+39	60.005-60.01	-45	+23
60.01–60.015	-50	+25	59.997	+38	60.01–60.015	-50	+25
60.015-60.02	-55	+30	60.007	-43	60.015-60.02	-55	+30

Case Study

The ramp attack was conducted with the mitigation algorithm in place for both the AGC methods, with varying conditions of renewables, and with attacks on single and multiple ACE values. The magnitude and duration of the attack were the same as in sections 2.5 & 2.7. The plots in Figure 3.4 show the result of the attack with mitigation in place for the four cases of attack and AGC. The following observations were made:

1. The attack was prevented during the AGC cycles for which condition 2 wasn't satisfied. Condition 1 wasn't violated as the attack magnitude was small. This resulted in the

possibility of the attack being rarely successful and the successful ones having negligible impact.

2. The impact would be lesser when the mitigation was used with the PID based AGC, as this method reduces the effect of the previous ACE values (or attack signals) on the control signals.
3. Although the ramp attack was mitigated, due to the absence of AGC function during attack, the frequency regulation is essentially lost. This can lead to adverse frequency conditions during extreme load and renewable generation variations when faced with an attack.

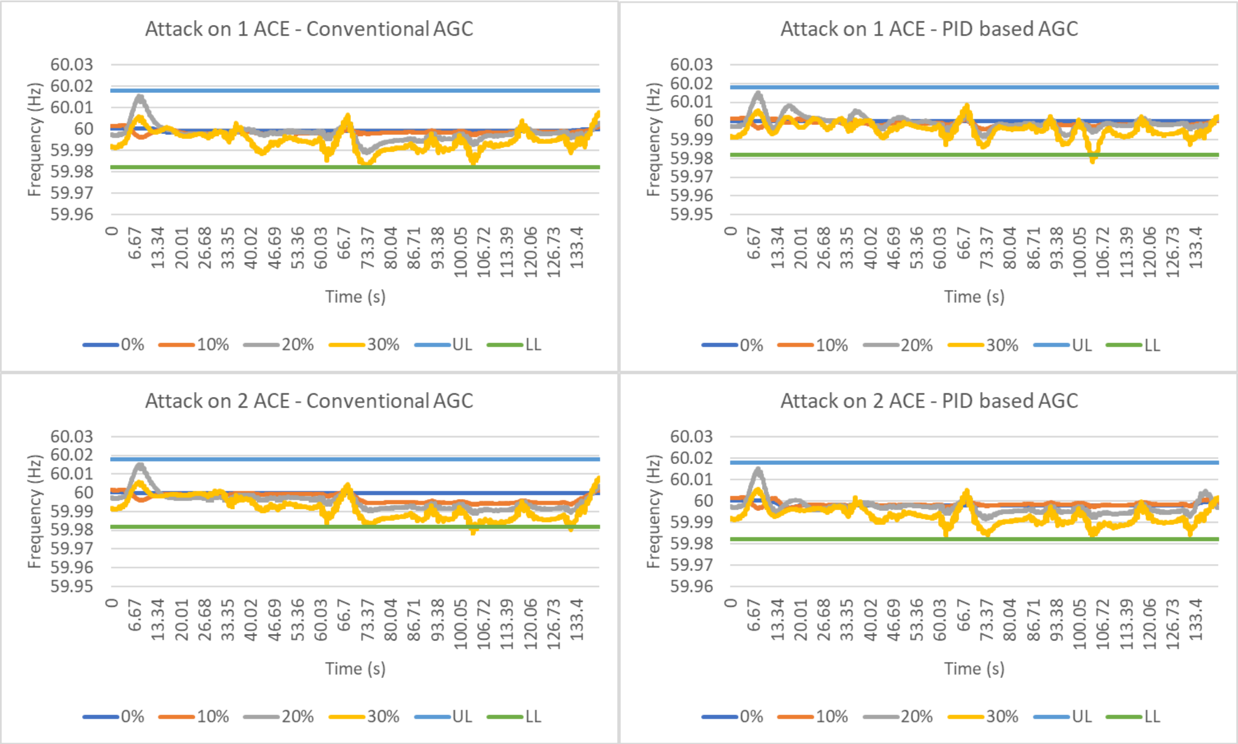

Figure 3.4 Effect of ramp attack with mitigation

Overall, the attack was successfully mitigated, and system frequency contained within the necessary limits for a majority of the attack duration.

Effect of mitigation on AGC performance

From the algorithm, it is evident that an alert would be generated whenever the ACE signals have opposite signs. This will result in a high incidence of false positives as this condition in ACE is observed most of the time. So, it is important to ensure that the normal AGC operation isn't adversely affected by the mitigation.

The AGC operation was simulated with the mitigation in place for both AGC algorithms and different conditions of renewables. Due to frequency being the primary factor in the algorithm, the system tends to restore frequency without any hindrance, despite the false positives. The plots in Figure 3.5 show that the AGC operations exhibit satisfactory performance with the mitigation installed for the simulated system conditions.

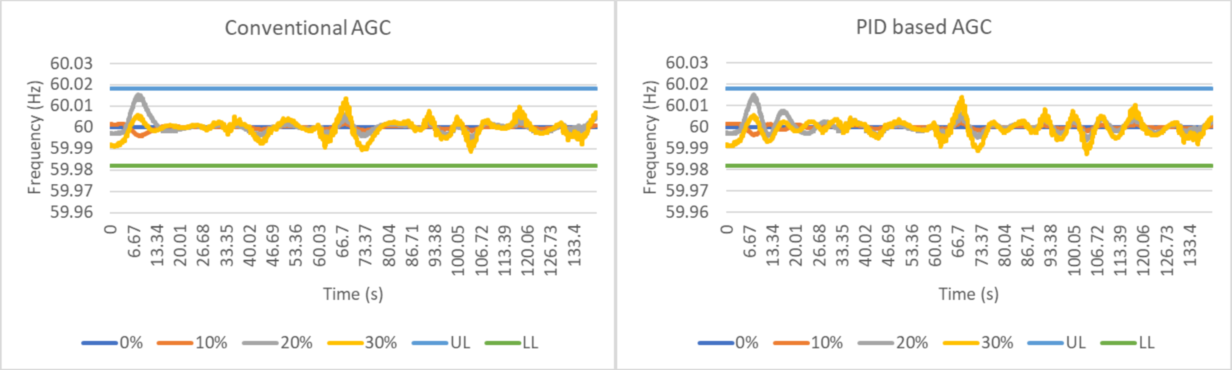

Figure 3.5 Effect of mitigation on AGC performance

An analysis of the performance of tie-line flow restoration was conducted by means of a step change in two of the loads. One load in BA1 and one in BA2 were subject to an increase and decrease of 50 MW of load respectively as shown in Figure 3.6. This was done to achieve an extreme condition of around 60 Hz, but with the maximum possible tie-line flow deviation for a given load change. This is because both the BAs would have ACE values similar in magnitude but with opposite signs, i.e. both BAs need to achieve a ramp up and ramp down in their generation by an equal amount, while being allowed to do only one at a time and needing longer time for restoration. It was observed that the system performance was satisfactory with the mitigation algorithm in place. The plot on the left in Figure 3.7 shows the frequency restoration. Even though the frequency performance appears to be inferior, there is a very less possibility of violation. This seemingly inferior performance is because at any instant, the machines in the grid are allowed to either ramp up or down, but not both. However, because of condition 2 in the mitigation algorithm the frequency deviation in any direction will always be facing an aggressive opposition. This would cause relatively greater frequency swings as compared to the system without mitigation. From the plot on the right, it was observed that the tie line restoration occurs at fairly the same duration with or without mitigation.

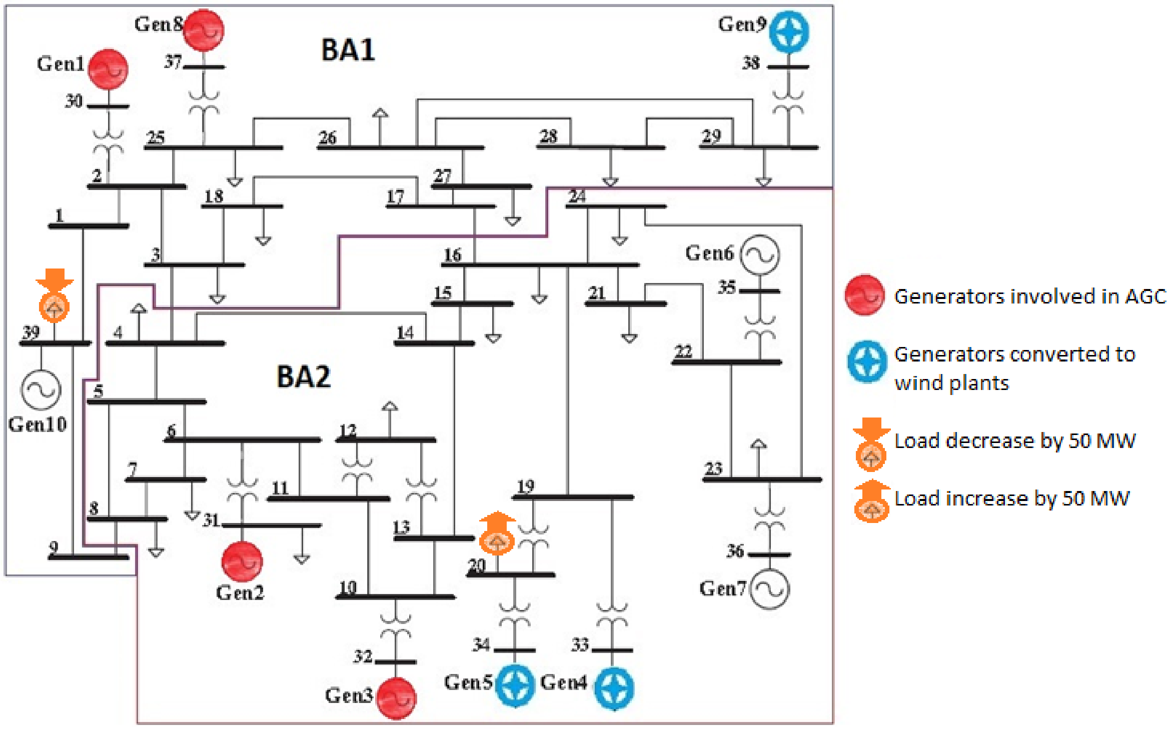

Figure 3.6 IEEE 39 bus model – AGC analysis with mitigation

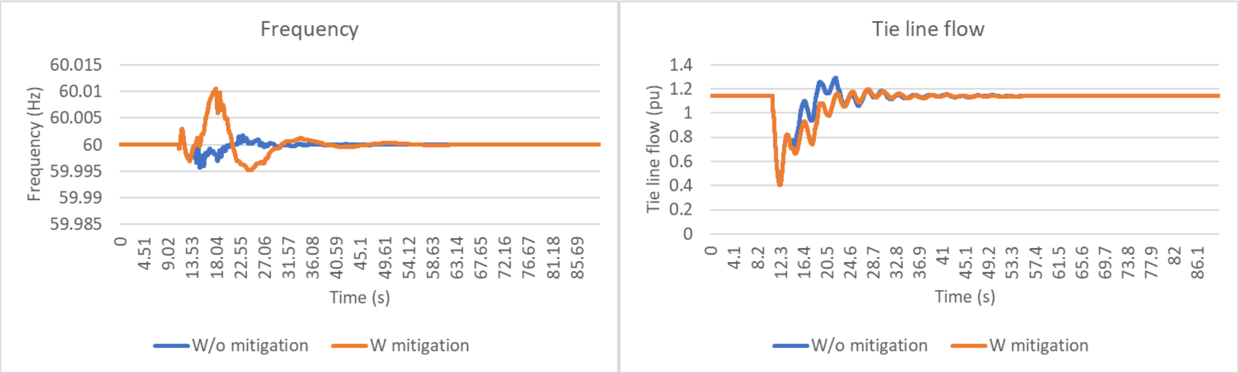

Figure 3.7 Effect of mitigation on frequency and tie line restoration

Effect of mitigation on contingency response

Current NERC regulations defined by BAL-002 standards, require the grid to restore its ACE to zero or a pre-disturbance value within 15 minutes following any disturbance [38]. This basically means that the grid is required to restore normal operation within 15 minutes following any event. During such situations, the ACE values could possibly be higher than those observed during normal operation. This operation might be at a risk if the mitigation algorithm is used as condition 1 limits the ACE to bounds based on values that were previously observed. Thus, it is necessary to analyze the impact of the mitigation on contingency restoration. Since, it is required by each BA to maintain sufficient reserves to address at least the Most Severe Single Contingency (MSSC) in its own area, the availability of resources to handle the event is not a concern. Rather, the issue lies in the mitigation's handling of higher ACE values and the effect of condition 1.

For the analysis, three types of contingencies have been considered as shown in Figure 3.8. From [38], it was found that on an average more than 100 events have occurred from 2010 to 2014 in the Eastern interconnection alone. So, in our analysis, we assume that the data used for generating the ACE bounds contain values observed during a contingency.

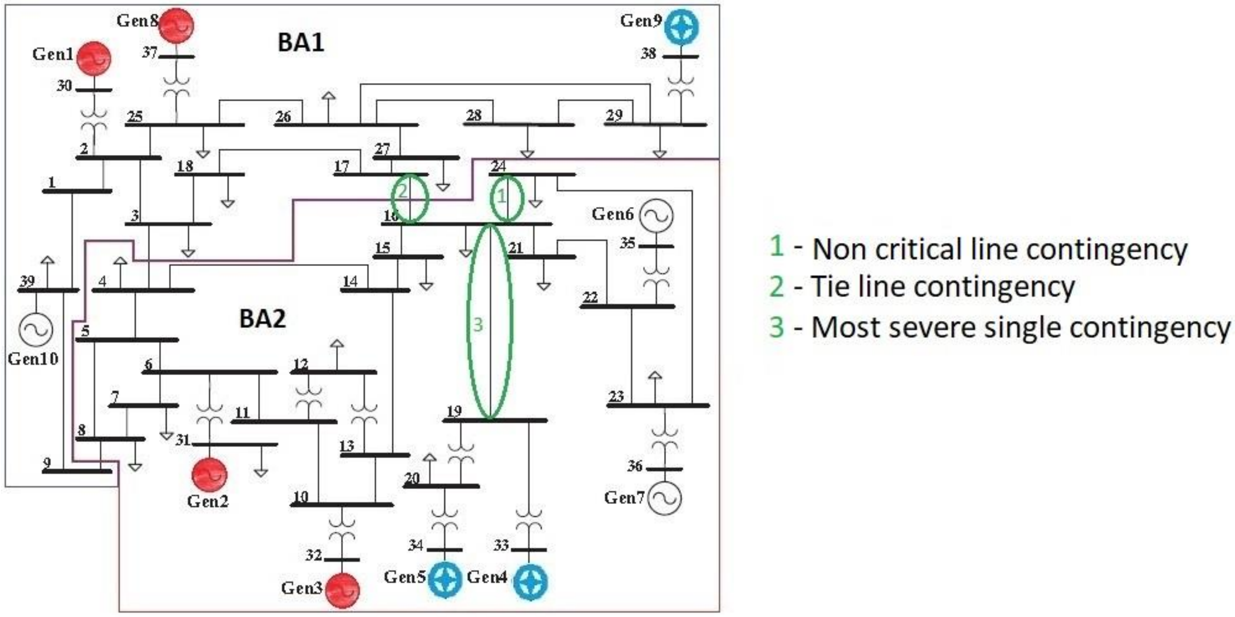

Figure 3.8 IEEE 39 bus model – Contingency analysis with mitigation

Contingency on a non-critical line

A non-critical line is one which when subject to an event doesn't cause any observable drop in load or generation. For such scenarios, the ACE values aren't expected to be very high. A contingency was simulated by disconnecting the line indicated in Figure 3.8, and the system response for restoring the normal operation of the grid was observed. The experiment was conducted for the system with and without the mitigation algorithm. Figure 3.9 shows the plots that depict the performance of the grid during the above-mentioned scenarios. Going with the assumption that the algorithm considers data due to events, it was observed that for simple contingencies such as the one on a non-critical line, presence of the mitigation doesn't impact the contingency recovery as shown in plot.

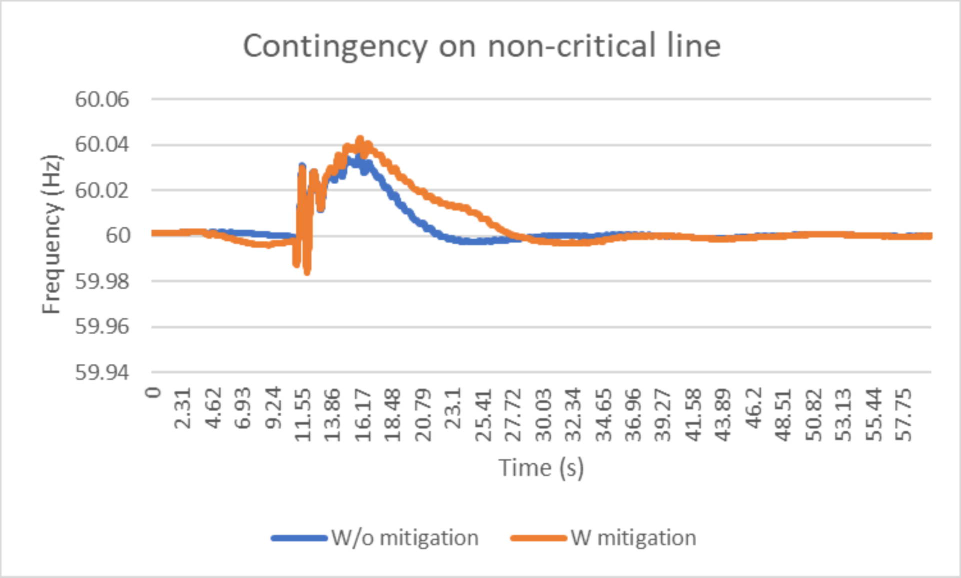

Figure 3.9 Contingency analysis on a non-critical line

Contingency on a tie-line

The second analysis was a contingency on one of the tie-lines indicated in Figure 3.8. In such situations, a significant tie-line error and hence a higher ACE value can be expected. The analysis was conducted on two cases – system that has a history of such a contingency in the past 12 months (i.e. the data used to generate the ACE bounds contained values due to such a contingency), and a system without history of such an event. In the second case, we assume history of a simple contingency. The contingency on the tie-line was simulated on both the cases with and without mitigation.

The performance of the system is shown in the plots in Figures 3.10 and 3.11. From the plots, it was observed that the presence of the mitigation algorithm doesn’t impact the contingency response of the grid for the considered tie-line loss, regardless of history of contingencies. This can be due to the fact that for the contingency considered, there wasn’t any significant drop in generation or load. Although with history of a tie-line contingency, the frequency deviation was lesser, the steady state conditions were achieved at fairly the same duration.

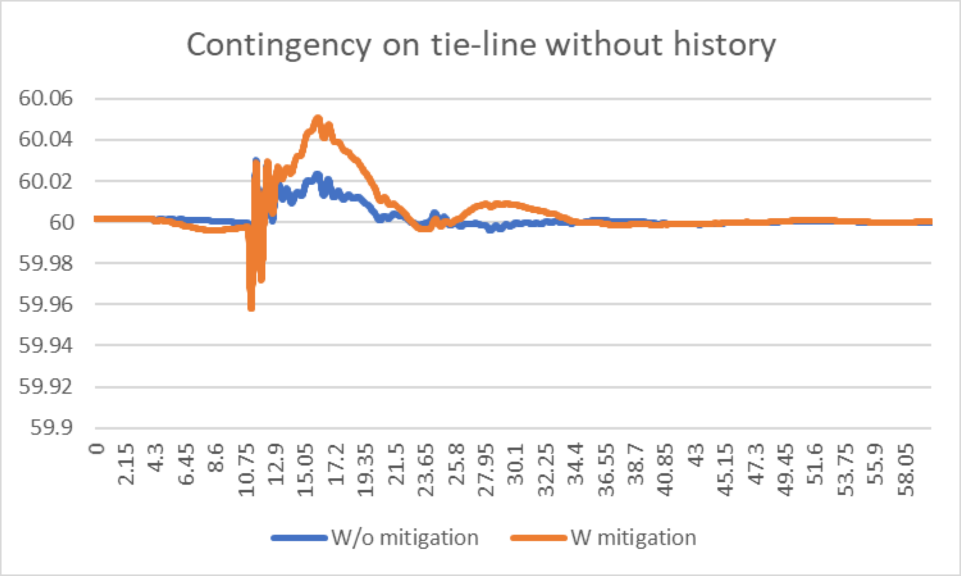

Figure 3.10 Contingency analysis on a tie-line without history

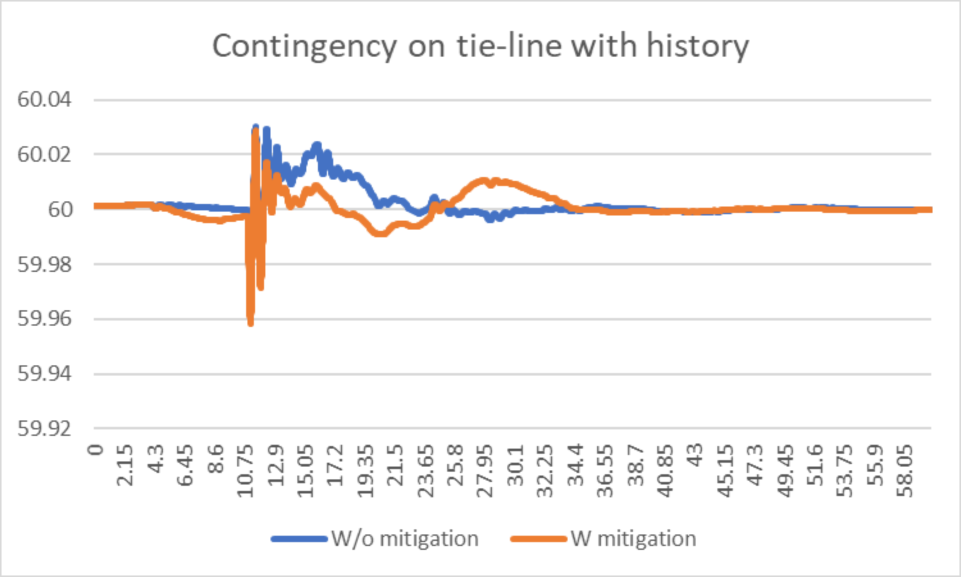

Figure 3.11 Contingency analysis on a tie-line with history

Most Severe Single Contingency

The final analysis was performed for the Most Severe Single Contingency (MSSC) of the system. Such a contingency would cause the maximum possible impact on the system due to a single event. From Figure 3.8, it can be seen that the loss of the indicated line would disconnect Generators 4 and 5 causing a severe drop in system generation and hence frequency. Such a situation would require extremely high values of ACE, which are rarely observed, to restore normal operation. The analysis was conducted for the system with and without mitigation, and with and without history of the considered contingency (assuming history of simple contingencies).

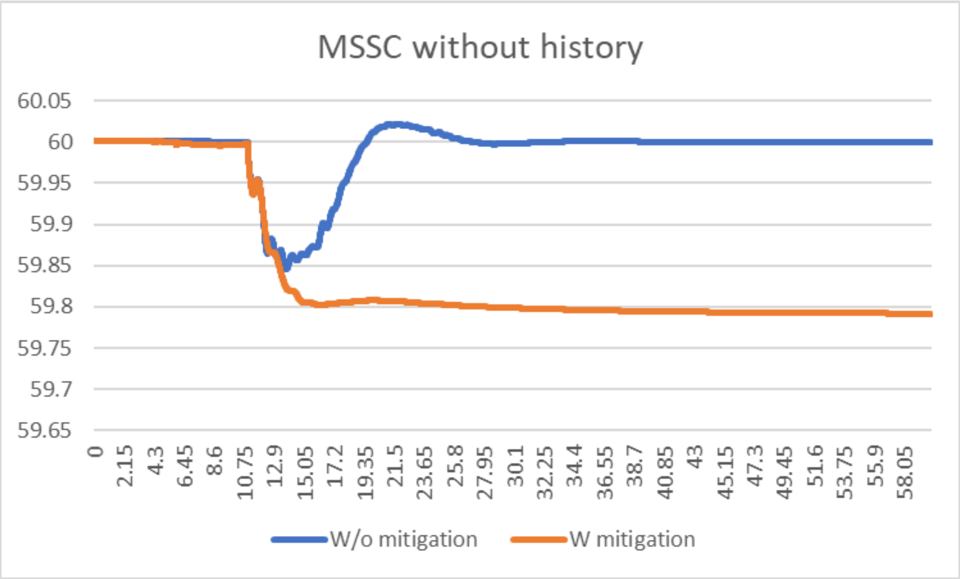

Figure 3.12 Analysis of MSSC without history

From the plots in Figures 3.12 and 3.13, it was observed that for a system without history, it is not possible to respond to an MSSC. This is obviously because of the high ACE values required for restoration, which aren’t normally observed during simple contingencies. If a system has history of a MSSC, recovery is possible within the required duration as shown in Figure 3.13.

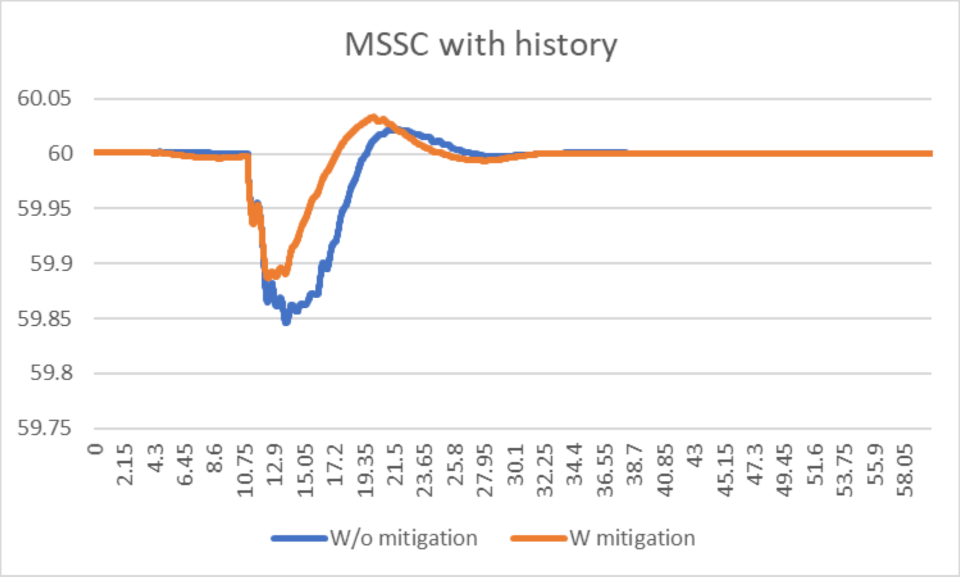

Figure 3.13 Analysis of MSSC with history

Conclusions

The designed mitigation strategy helps avoid the large drop in frequency due to attacks and to some extent mitigates the attack. But, due to absence of AGC, the load frequency control is lost. From the false positive analysis for the mitigation, it was observed that the AGC performance was not adversely affected for the tested system conditions. An analysis was also performed on the impact of mitigation on the contingency restoration, and it was observed that for contingencies that do not cause a significant change in generation or load, the response wasn't affected. Also, for contingencies that do cause such a change, the response wasn't affected provided the system has a history of similar contingencies in the past 12 months.

CHAPTER 4 **CONCLUSION AND FUTURE WORK**

Conclusion

With the electric power grid advancing towards a greener, reliable and smarter future, the importance of cyber security is of paramount importance. With increasing dependence on critical applications, such as WAMPAC, using sophisticated state-of-the-art equipment like synchrophasors over the Wide Area Network (WAN), there is an ever-increasing need for research in the various cyber threats that can pose a risk to the critical infrastructure. Also, as the nature of the grid changes with more renewable sources, distributed generation, electric vehicles, etc. it is essential to conduct studies using more realistic and practical power grid simulations.

To address some of the issues faced, this thesis makes two contributions.

1. First, an analysis was conducted on cyber-attacks on the power grid with renewables integrated. A ramp attack was carried out on the AGC operation under different conditions and the ill-effects that increasing renewable penetration posed in the face of an attack were observed. An alternative algorithm employing a PID based approach, with the aim of diminishing the impact of cyber-attacks was introduced, and its performance analyzed under different scenarios. A faster drop in frequency was observed with increase in renewable penetration level.
2. Secondly, a two-step mitigation strategy was developed and validated in terms of defense effectiveness and efficiency of system operation. Although the load frequency control was suspended for the duration of the attack, the damage caused by the attack in the previous case was greatly avoided. An analysis on the effect of false positives generated by the mitigation on the AGC performance was conducted, and satisfactory performance was

observed. An analysis of the effect on contingency response was also performed, and it was observed that, for contingencies resulting in a significant drop in load and/or generation, the response was poor unless the system had experienced similar event during the previous 12 months. Satisfactory response was observed for events that were less damaging.

Future Work

Further development on this topic would include:

1. Analysis of various developments for renewables, like battery storage integration, distributed generation, AGC participation by wind turbines, inertial emulation, renewable dispatch, etc. will be helpful in generating more cutting-edge results in the area. Inclusion of such technology will influence the performance of the renewables integrated system and might result in reducing some of the adverse impacts of renewable integration. As a result, the conclusions obtained from this thesis might be exaggerated for such a grid.
2. Development and analysis of new types of attacks on renewables and related features such as the ones mentioned above. An intelligent attacker might opt for a more stealthy and coordinated attack, which while having negligible immediate impact might result in severe long-term consequences. Also, while considering the technological advances as mentioned in the first point, it is important to realize the probable increase in attack surface which opens further options for the attacker. Thus, a scrutinizing analysis of the vulnerability and impact evaluation of a more modern power grid is of tremendous importance.

3. Improvement of mitigation algorithm to a resilient algorithm that can help the system to correct its frequency deviations, using data from forecast, governor response data, peer-to-peer interaction, etc. is an absolute necessity. As seen from the results, the mitigation algorithm, while capable of reducing the impact in the event of an attack, completely neglects the load frequency control (LFC) action needed for system stability. Also, from the contingency analysis, it was observed that the system tends to have an inferior performance while responding to contingencies resulting in a significant generation loss. In these cases, additional information obtained from real time load forecast, weather patterns, and other system data can assist the mitigation algorithm in performing effective LFC. These data when combined with state-of-the-art applications such as machine learning, can help in predicting accurate control and protective actions.

REFERENCES

[1] FERC Docket no. RR09 - Three-year electric reliability organization performance assessment report. North American Electric Reliability Corporation (NERC). July 20, 2009.

[2] Yih-Huei Wan. Wind Power Plant Behaviors: Analyses of Long-Term Wind Power Data. Technical report. National Renewable Energy Laboratory (NREL). September 2004.

[3] Y. Wan. A Primer on Wind Power for Utility Applications. Technical report. National Renewable Energy Laboratory (NREL). December 2005.

[4] 2013 Special Reliability Assessment: Maintaining Bulk Power System Reliability While Integrating Variable Energy Resources – CAISO Approach. Technical report. North American Electric Reliability Corporation (NERC) and California Independent System Operator Corporation (CAISO). November 2013.

[5] Balancing and Frequency Control. Technical document. North American Electric Reliability Corporation (NERC). January 26, 2011.

[6] BAL-001-2 – Real Power Balancing Control Performance Standard. North American Electric Reliability Corporation (NERC). February 2013.

[7] Standard BAL-001-2 – Real Power Balancing Control Performance. North American Electric Reliability Corporation (NERC).

[8] A. M. Annaswamy, M. Amin, C. L. DeMarco and T. Samad. IEEE Vision for Smart Grid Controls: 2030 and Beyond. IEEE Standards Association. June 2013

[9] A. Ashok, P. Wang, M. Brown and M. Govindarasu. Experimental evaluation of cyber-attacks on automatic generation control using a cps security testbed. IEEE Power Energy Society General Meeting 2015. July 15, 2015.

[10] S. Sridhar and M. Govindarasu. Model-based attack detection and mitigation for automatic generation control. IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580-591, March 2014.

[11] S. Sridhar and M. Govindarasu. Data Integrity Attacks and their Impacts on SCADA Control System. IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580-591, March 2014. IEEE Power Energy Society General Meeting 2015. September 30, 2010.

[12] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang and M. Govindarasu. Testbed-based performance evaluation of Attack Resilient Control for AGC. Resilience Week (RWS) 2016. September 22, 2016

[13] A. Ashok, M. Govindarasu and J. Wang. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. Proceedings of the IEEE, vol. 105, issue. 7. July 2017

[14] R. Tan, H. H. Nguyen, E. Y. S. Foo and X. Dong. Optimal False Data Injection Attack against Automatic Generation Control in Power Grids. 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS).

[15] A. K. Bejestani, A. Annaswamy and T. Samad. A Hierarchical Transactive Control Architecture for Renewables Integration in Smart Grids: Analytical Modeling and Stability. IEEE Transactions on Smart Grid, Vol. 5, No. 4, July 2014.

[16] C. Zhang, T. Liu and D. J. Hill. Distributed Load-Side Frequency Regulation for Power System. Power Systems Computation Conference (PSCC), 2016.

[17] A. Kehyani and A. M. Annaswamy. A New Automatic Generation Control with Heterogeneous Assets for Integration of Renewables. Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES.

[18] G. Delille, B. Francois and G. Malarange. Dynamic Frequency Control Support by Energy Storage to Reduce the Impact of Wind and Solar Generation on Isolated Power Systems Inertia. IEEE Transactions on Sustainable Energy, Vol. 3, No. 4, October 2012.

[19] M. Ayar, S. Obuz, R. D. Trevizan, A. S. Bretas and H. Latchman. A Distributed Control Approach for Enhancing Smart Grid Transient Stability and Resilience. IEEE Transactions on Smart Grid, vol. pp, issue. 99. June 13, 2017.

[20] J. Schlauwitz and Petr Musilek. Smart Renewable Energy Management System for Consumer Applications. 2016 IEEE Congress on Evolutionary Computing (CEC). November 21, 2016

[21] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. IEEE Transactions on Smart Grid, vol. 1, issue 1, pp. 57–64, June 2010.

[22] G. Dondossola, F. Garrone, G. Proserpio, and C. Tornelli. Impact of DER integration on the cyber security of SCADA systems—The medium voltage regulation case study. Integration of Renewables into the Distribution Grid, CIRED Workshop, May2012, pp.1–4.

[23] B. J. Kirby, J. Dyer, C. Martinez, R. A. Shoureshi, R. Guttromson and J. Dagle. Frequency Control Concerns in The North American Electric Power System. CERTS – Real-time Grid Monitoring and Management. December 2002.

[24] Gesche Krause. From Turbine to Wind Farms – Technical Requirements and Spin-Off Products. Chapter 6. April 2011

[25] Interconnection Requirements for Variable Generation. Technical Document. North American Electric Reliability Corporation (NERC). September 2012.

[26] 20% Wind Energy by 2030 – Increasing Wind Energy's Contribution to U.S. Electricity Supply. U.S. Department of Energy – Energy Efficiency and Renewable Energy. May 2008.

[27] Accommodating High Levels of Variable Generation. Technical Report. North American Electric Reliability Corporation (NERC). April 2009.

[28] M. Moness, A. M. Moustafa. A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy. IEEE Internet of Things Journal, vol. 3, no. 2, pp. 134-145, April 2016.

[29] Cyber Attack Task Force. Final Report. North American Electric Reliability Corporation (NERC). May 2012.

[30] Interconnection Criteria for Frequency Response Requirements. Technical Report. North American Electric Reliability Corporation (NERC). August 2011.

[31] Allen J. Wood, Bruce F. Wollenberg, and Gerald B. Sheble. Power Generation, Operation and Control, 3rd edition.

[32] Siddharth Sridhar. Cyber risk modeling and attack-resilient control for power grid. Doctoral Dissertation, Iowa State University, 2015

[33] M. Govindarasu and P. W. Sauer. Smart grid Security, [Guest Editorial]. IEEE Power and Energy Magazine, vol. 10, pp. 17-17, 2012.

[34] V. Kumar Singh, A. Ozen and M. Govindarasu. Stealthy cyber-attacks and impact analysis on wide-area protection of smart grid. 2016 North American Power Symposium (NAPS), Denver, CO, 2016, pp. 1-6.

[35] P. Fairley. A December attack on Ukraine’s grid was a wake-up call. IEEE Spectrum, April 20,2016.

[36] Grid integration of large-capacity Renewable sources and use of large-capacity Electrical Energy Storage. White paper, IEC, Geneva, Switzerland 2012

[37] Frequency Response Initiative Report – The Reliability Role of Frequency Response. Technical Report. North American Electric Reliability Corporation (NERC). October 2012.

[38] BAL-002-2 - Disturbance Control Performance - Contingency Reserve for Recovery from a Balancing Contingency Event Standard Background Document - North American Electric Reliability Corporation (NERC). July 2015.