Cyber Resilient Wind Turbine Generator Control System

Nathan Oaks Farrar

Follow this and additional works at: https://digitalcommons.memphis.edu/etd

Recommended Citation

https://digitalcommons.memphis.edu/etd/3323

This Thesis is brought to you for free and open access by University of Memphis Digital Commons. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of University of Memphis Digital Commons. For more information, please contact khgerry@memphis.edu.
Cyber Resilient Wind Turbine Generator Control System

By:

Nathan Farrar

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Major: Electrical Engineering

The University of Memphis

December 2023
This thesis is dedicated to my late mother, Victoria Farrar, whose passion for science and the unknown drove me to question the world around me, as well as my loving wife, Mallory Farrar, whose steadfast belief in my abilities has made me the person that I am today.
ACKNOWLEDGEMENT

First, I would like to thank Dr. Mohd. Hasan Ali, my thesis advisor, for the dedication and commitment to knowledge, and for passing that wisdom on to myself and my fellow students throughout my studies at the University of Memphis. I sincerely appreciate all the time and effort he has put forward in my continued education and research for my master’s studies. I am truly fortunate to have found such a knowledgeable mentor to guide me through my academic endeavors.

I would also like to thank Dr. Mohammadreza Davoodi and Dr. Myounggyu Won for assisting me with their knowledge and expertise in my research and for being a part of my thesis committee.

I would also like to thank the CfIA cyber-security team for their assistance with the research with respect to the zero-trust architecture that was implemented in my master’s thesis.

Lastly, I would like to thank my friends and family for their continued motivation and support throughout my academic career.
ABSTRACT


As wind turbine generator systems become more common in the modern power grid, the question of how to adequately protect them from cyber criminals has become a major theme in the development of new control systems. As such, Artificial Intelligence (AI) and Machine Learning (ML) algorithms have become major contributors to preventing, detecting, and mitigating cyber-attacks in the power system. In their current state, wind turbine generator systems are woefully unprepared for a coordinated and sophisticated cyber-attack. With the implementation of the internet-of-things (IoT) devices in the power control network, cyber risks have increased exponentially. In the current literature, prevention and detection of cyber-attacks have been prioritized. This includes event trigger control schemes to detect communication disruption attacks, or AI and ML algorithms to weed out manipulated data. Mitigation has largely been left to power factor correction or fault mitigation devices. Due to the importance of keeping the power system safe and dependable, especially with respect to distributed energy resources, this thesis proposes implementing a cyber secure zero-trust architecture with an AI based, wind turbine generator controller that can prevent cyber attackers from gaining access to vital control functions and mitigate any effects that communication delays or bad data could have on a grid connected wind turbine generator or wind farm. The proposed techniques have been simulated and validated utilizing the MATLAB/Simulink software to demonstrate the effectiveness of the proposed methods.
PREFACE

One paper resulting from this work was used in chapter 1, subsection 1.1.4 of the literature review of this manuscript. The paper was published in the MPDI Energies Journal on February 3, 2023. The following lists the article used in this thesis:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

Chapter 1
INTRODUCTION .................................................. 1

1.1 Background and Literature Review ................................................................. 2
  1.1.1 Wind Turbine Generator Topology and Power Extraction ......................... 2
  1.1.2 Cyber Attacks on Wind Turbine Generator Systems ................................. 5
  1.1.3 AI-Based Cyber Solutions for Wind Turbine Generator Control Systems ..... 6

1.2 Motivation ........................................................................................................... 9

1.3 The Zero Trust Concept ....................................................................................... 10

1.4 Deep Deterministic Policy Gradient Control for Wind Farms ......................... 10

1.5 Objective of The Thesis ....................................................................................... 12

1.6 Novelty ............................................................................................................... 12

1.7 Organization of Thesis ....................................................................................... 12

Chapter 2
DFIG AND CYBER ATTACK MODELING FOR WIND FARMS .................... 13

2.1 DFIG Modeling and Cyber Physical Model ..................................................... 13

2.2 DFIG Control Methodology ............................................................................. 15
  2.2.1 Grid-side and Rotor-side Converter Control .............................................. 15

2.3 Cyber Attack Modeling ....................................................................................... 20
  2.3.1 False Data Injection Attack ....................................................................... 20
  2.3.2 Denial of Service Attack ............................................................................ 21

2.4 Considered Cyber-Attack Detection Methods ................................................. 21

2.5 Conclusion ......................................................................................................... 22

Chapter 3
PROPOSED ZERO TRUST AND DDPG METHODS FOR MITIGATION OF ADVERSE IMPACTS OF CYBER-ATTACKS ON WIND FARMS .................. 23

3.1 Zero Trust Concept ........................................................................................... 23

3.2 Proposed Zero Trust Algorithm ......................................................................... 31
LIST OF FIGURES

Fig. 1: DFIG-based wind turbine generator model. ................................................................. 3
Fig. 2: Pitch Angle Controller Block Diagram. ................................................................. 15
Fig. 3: Grid-side converter block diagram. ................................................................. 16
Fig. 4: Rotor-side converter block diagram. ................................................................. 17
Fig. 5: Wind Farm Model with Cyber-Attack Points ....................................................... 22
Fig. 6: Zero Trust Logical Components. ................................................................. 27
Fig. 7: Zero Trust Flow Chart. ................................................................. 31
Fig. 8: Zero-Trust Concept in Wind Farms. ................................................................. 32
Fig. 9: Proposed multi-agent DDPG control network flow chart. ................................... 36
Fig. 10: Proposed multi-agent DDPG control network block diagram. ......................... 36
Fig. 11: (a) DDPG Actor Network for Stator idq Reference Points;(b) DDPG Critic Network for Stator idq Reference Points. ................................................................. 38
Fig. 12: (a) DDPG Actor Network for rotor idq Reference Points;(b) DDPG Critic Network for Rotor idq Reference Points. ................................................................. 40
Fig. 13: (a) DDPG Actor Network for rotor vdq Reference Points;(b) DDPG Critic Network for Rotor vdq Reference Points ................................................................. 42
Fig. 14: PI Controller Block Diagram ............................................................................. 43
Fig. 15: DoS attacks on the rotor-side converter PWM signal ......................................... 47
Fig. 16: FDIA attack on the stator current d-q set-points ................................................ 47
Fig. 17: Active power during DoS attack on rotor-side PWM signal ................................ 48
Fig. 18: Reactive power during DoS attack on rotor-side PWM signal ........................... 49
Fig. 19: Rotor Speed p.u. during DoS attack on rotor-side PWM signal ........................... 49
Fig. 20: DC-link voltage during DoS attack on rotor-side PWM signal ......................... 50
Fig. 21: Active power during FDIA on stator $i_{dq}^*$ set points ........................................ 51
Fig. 22: Reactive power during FDIA on stator $i_{dq}^*$ set points ........................................ 51
Fig. 23: Rotor speed p.u. during FDIA on stator $i_{dq}^*$ set points ........................................ 52
Fig. 24: DC-link voltage during FDIA on stator $i_{dq}^*$ set points ........................................ 52
Fig. 25: Active power during FDIA on rotor $i_{dq}^*$ set points ........................................ 53
Fig. 26: Reactive power during FDIA on rotor $i_{dq}^*$ set points .......................................................54
Fig. 27: Rotor speed p.u. during FDIA on rotor $i_{dq}^*$ set points ..........................................................54
Fig. 28: DC-link voltage during FDIA on rotor $i_{dq}^*$ set points ..........................................................55
Fig. 29: Active power during FDIA on rotor $v_{dq}^*$ set points ..........................................................56
Fig. 30: Reactive power during FDIA on rotor $v_{dq}^*$ set points ..........................................................56
Fig. 31: Rotor speed p.u. voltage during FDIA on rotor $v_{dq}^*$ set points ..............................................57
Fig. 32: DC-link voltage during FDIA on rotor $v_{dq}^*$ set points ..........................................................57
Fig. 33: Active power during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM ..............................................................................................................................................59
Fig. 34: Reactive power during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM ..............................................................................................................................................59
Fig. 35: Rotor Speed p.u. during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM ..............................................................................................................................................60
Fig. 36: DC-link voltage during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM ..............................................................................................................................................60
Fig. 37: Zero Trust Algorithm Flow Chart ...............................................................................................63
LIST OF TABLES

Table 1: AI Algorithms for Cyber Attack Detection and Mitigation ........................................... 7-9
Table 2: Simulation parameters for small scale grid connected wind farm ............................. 44-45
Table 3: Simulated Cyber Attack Scenarios. .................................................................................46
Table 4: RMSE Performance Evaluation .......................................................................................62
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>ANN</td>
<td>Artificial Neural Network</td>
</tr>
<tr>
<td>BDIA</td>
<td>Bad Data Injection Attack</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring-Your-Own-Device</td>
</tr>
<tr>
<td>CDM</td>
<td>Continuous Diagnostics and Mitigation</td>
</tr>
<tr>
<td>DT</td>
<td>Decision Tree</td>
</tr>
<tr>
<td>DDPG</td>
<td>Deep Deterministic Policy Gradient</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DER</td>
<td>Distributed Energy Resource</td>
</tr>
<tr>
<td>DFIG</td>
<td>Double-Fed Induction Generator</td>
</tr>
<tr>
<td>PKI</td>
<td>Public-Key Infrastructure</td>
</tr>
<tr>
<td>FDIA</td>
<td>False Data Injection Attack</td>
</tr>
<tr>
<td>ICAM</td>
<td>Identity, Credential, and Access Management</td>
</tr>
<tr>
<td>IGBT</td>
<td>Insulated-Gate Bipolar Transistor</td>
</tr>
<tr>
<td>IDPS</td>
<td>Intrusion Detection and Prevention Systems</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MitM</td>
<td>Man In The Middle</td>
</tr>
<tr>
<td>MaDIoT</td>
<td>Manipulation of Data via IoT</td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</td>
</tr>
<tr>
<td>NOAA</td>
<td>National Oceanic and Atmospheric Administration</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PID</td>
<td>Proportional, Integral, and Derivative</td>
</tr>
<tr>
<td>PMSG</td>
<td>Permanent Magnet Synchronous Generator</td>
</tr>
<tr>
<td>PIFPI</td>
<td>PI/fractional-order Fuzzy/PI</td>
</tr>
<tr>
<td>PAC</td>
<td>Pitch Angle Controller</td>
</tr>
</tbody>
</table>
PA  Policy Administrator
PEP  Policy Enforcement Point
PE  Policy Engine
PLC  Programmable Logic Controller
PWM  Pulse Width Modulated
RMSE  Root Mean Square Error
SIEM  Security Information and Event Management
SaaS  Software As A Service
SCADA  Supervisory Control and Data Acquisition
SVM  Support Vector Machine
VSC  Voltage Source Converter
WAMPAC  Wide Area Monitoring, Protection and Control
YAC  Yaw Angle Controller
ZT  Zero Trust
ZTA  Zero Trust Architecture
Chapter 1

INTRODUCTION

Distributed energy resources (DER) have become a major contributor to the modern power grid, with wind energy being the preferred DER implemented globally. In 2008, the US Department of Energy established a target of producing 20% of its electricity from wind resources by 2030 [1]. A report released by the International Energy Agency announced that the total renewable energy capacity of 10,800GW would be implemented by the year 2040 [2]. Due to their incredible size, many wind farms are in very remote locations or offshore, as they are subject to right-of-way constrictions of local and regional municipalities. Wind farms also require a detailed analysis of wind power flow through possible site locations, as maximum power extraction is necessary to optimize the energy produced by wind farms [3]. Due to these constraints, remote internet-of-things (IoT) devices have become a common solution to monitor, control, and manage wind farm power systems.

With the increased implementation of IoT devices in wind farm control schemes, major cybersecurity risks have arisen that, if not rectified quickly, could lead to major losses in revenue for power providers, as well as unstable and unreliable power for consumers, such as the attacks presented in chapter 1, subsection 1.1.2. To reduce the occurrence and effects of these malicious attacks, researchers and engineers must continuously develop advanced control schemes to protect these vital assets to maintain a reliable power supply to consumers and prevent loss of revenue for utility providers. Before presenting information regarding the cyber security risks of wind turbine systems, this thesis will begin by introducing the importance of the topic and present the results of the literature review conducted by the authors. This will be followed by a breakdown of the topologies of wind turbine generators and the use of artificial intelligence (AI) agents in wind turbine generator control systems. This will then be followed by an introduction to the Zero Trust concept, as well as AI agents for cyber security and cybersecurity issues with wind turbine generator control systems, including the author’s proposed prevention architecture and multi-agent Deep Deterministic Policy Gradient (DDPG) control mitigation systems. Next, a simulation of the
proposed control system compared to the current system will be presented, and lastly, a conclusion of the research with a discussion of the future direction of the project.

1.1 Background and Literature Review

1.1.1 Wind Turbine Generator Topology and Power Extraction

According to Tawfiq et al. (2019), wind turbines are composed of turbine blades, a weighted rotor shaft, nacelle, generator, power electronic converters, and the tower itself [4]. Pitch and yaw actuators are utilized to adjust the turbine blades to allow each wind turbine to maximize the amount of power generated based on a given wind speed. Mechanical power is generated by the wind turbine blades by utilizing a rotor shaft that connects the blades to the generator, which is usually fed through a gearbox to allow for the generator to turn at optimal speeds. The nacelle is an aerodynamic housing that is attached to the top of the tower and contains the generator, actuators, and power electronic converters. The tower is the metallic structure the wind turbine components are mounted on and is either secured to the ground, secured to the ocean floor, or secured to a floating structure.

Depending on available resources such as location, budget and municipal regulations, different types of generators have been implemented in wind farms. In the last few decades, synchronous generators, such as the permanent magnet synchronous generator, have been used due to their high reliability; however, due to wind speeds being variable, an expensive gear box, torque converter, and speed converter are necessary to maintain the synchronous speed of the generator (Chang-Chien et al 2013) [5]. According to Adouni et al. (2016), many modern wind farms are implementing induction generators, such as the double-fed induction generator (DFIG) [6]. Induction generators are variable-speed, so they do not require a sophisticated gearbox to maintain a synchronous speed, but they do however require intelligent electronic devices such as AC/DC converters, voltage source converters inverters (VSC), a step-up gearbox, and may also use energy storage systems to remove any fluctuations in the generator frequency and to boost power output when wind speeds are low, as reported in Al-Deen et al (2021) [7]. DFIGs have become a preferable generator for wind farms, as they allow for the decoupling of real and reactive power through the independent control of torque and rotor excitation currents. Figure 1 depicts a
grid connected DFIG-based wind turbine generator model with pitch angle control, rotor-side converter, grid-side converter, DC-link capacitor, turbine blades, rotor shaft, and a set-up gearbox.

![DFIG-based Wind Turbine Generator Model](image)

Figure 1: DFIG-based Wind Turbine Generator Model.

Every wind turbine has sensors mounted to the nacelle to measure wind speed and direction, as well as the speed of the rotor shaft, the output voltage and current of the generator, and, according to Chen et al. (2019), the condition of the internal mechanical components of the generator such as the bearings and the gears [8]. The collected data is fed directly to the Supervisory Control and Data Acquisition (SCADA) controller, which then sends commands to specific devices, such as the pitch angle controller, the yaw angle controller, and Programable Logic Controllers, as depicted in Sabev et al. (2021) [2]. These devices utilize different communication schemes to relay data to the SCADA controller, such as a local area network which is hard wired directly to the controllers or sent wirelessly via a wide area monitoring, protection, and control (WAMPAC) network as described in Chen et al. (2020) [9]. At the base of each tower, a wind tower control panel (WTCP) for the specified wind turbine is available for on-site control and diagnostics.

To extract power from the wind, wind farms utilize the wind speed (V), the radius of the turbine blades (R), the air density (ρ) and the power coefficient, referenced as Cp. Equation (1)
depicts the formula for determining the wind power present to a wind turbine and equation (2)
depicts the mechanical wind power generated by a wind turbine generator in a given wind stream [10].

\[ P_{\text{wind}} = \frac{1}{2} \rho \pi R^2 V^3 \quad (1) \]

\[ P_{\text{mech}} = \frac{1}{2} \pi R^3 V^3 C_p(\lambda, \beta) \quad (2) \]

Many of the variables in equation (1) are considered constants, such as the turbine blade radius and
air density. The wind speed and power coefficient will change, depending on the wind velocity and
the blade pitch. Wind velocity of a given area is typically determined from the weather
forecasted by the National Oceanic and Atmospheric Administration; however, all wind turbine
generators are equipped with wind speed sensors, known as anemometers, to give real-time wind
speed measurements. Several AI and ML algorithms have also been proposed to predict wind
speeds to decrease computing times and allow for continuous operation if damage occurs to the
anemometer or communication line, as reported in Zhang et al. (2020) [11], and Zhang et al. (2022)
[12]. The wind velocity will then allow the SCADA to determine the proper pitch angle and yaw
of each wind turbine generator to guarantee maximum power extraction. Equation (3) depicts the
formula for determining \( C_p \) using the lambda/beta method, with equation (4) depicting the formula
for the blade tip ratio (\( \lambda \)), with \( \omega_r \) being the rotational speed of the rotor, and equation (5) depicting
the limits of the blade pitch (\( \beta \)), as reported in Khurshid et al. (2022) [10]. It is important to note
that wind power generation is limited by the Betz limit, which restricts the amount of wind power
able to be extracted from any wind stream to a maximum of 59.3% [10].

\[ C_p(\lambda, \beta) = 0.5176 \left( \frac{116}{\lambda} - 0.4\beta - 0.002\beta^{2.14} - 5 \right) e^{-\frac{21}{\lambda}} + 0.0068\lambda \quad (3) \]

\[ \lambda = \frac{\omega_r R}{V} \quad (4) \]

\[ \beta = \begin{cases} 
0^\circ \leq \beta \leq 27^\circ \\
\frac{d\beta}{dt} = 10^\circ 
\end{cases} \quad (5) \]
1.1.2 Cyber Attacks on Wind Turbine Systems

Historically, cyber-attacks on wind farms have been isolated to ransomware attacks, which involve hacking into a vendor’s wide area network (WAN) and stealing as much data as possible before severing communication lines to control devices and holding the data and devices hostage until a monetary demand is met. On November 19, 2021, a wind farm operated by the Danish wind turbine manufacturer Vestas was attacked by a LockBit ransomware attack that stole sensitive proprietary data and employee personal information [13]. Thanks to the quick response of Vestas’s cyber response team, no third-party vendors were affected, and no damage was reported in any wind farms [13]. In March 2022, the wind farm operator Enercon lost control of the satellite communication with approximately 5,800 wind turbine generators [13]. The staff was forced to shut down the entire wind farm system, effectively removing 11,000 MW of power from the interconnected power grid. As of March 15, 2022, only 15%, roughly 900 wind turbine generators, had been restored [13]. In this case, no damage was reported to any wind turbine generators.

Again, in March 2022, the wind farm operator Nordex SE was hit with a Conti ransomware attack that forced the entire platform offline [13]. The attack only affected the internal IT infrastructure, and no third-party assets were affected [13]. No wind turbine generator damage was reported as a result of this attack. Lastly, on April 11, 2022, the wind farm operator Deutsche Windtechnik AG was attacked by a ransomware attack and lost control of 2,000 wind turbine generators [13]. The incident forced the responders to switch off the remote data monitoring connections to the wind turbine system, effectively shutting the turbines down for 48 hours [13]. No wind turbine generator damage was reported due to this incident. Though these attacks have caused a loss in revenue for utility providers as well as a loss in power generation, they have been limited in scope and only marginally successful in the grand scheme of cyber incidents.

From the literature review, there are two types of attacks that researchers focus on. These attacks are denial of service (DoS) and false data injection attack (FDIA) / bad data injection attack (BDIA). According to Chen et al. (2020), a DoS attack is when a hacker overwhelms the communication lines of the control system for a wind farm, causing complete loss of control in the system and adding significant delay to automated control processes of the wind farm [9]. A FDIA/BDIA is an attack where the hacker penetrates the control network of a wind farm and maliciously manipulates sensor data or reference set points, causing instability or damage to the wind turbines.
When these two attacks are conducted simultaneously, severe damage can be caused to a wind generator or the entire wind farm that could also have disastrous effects on the interconnected power grid.

According to Carvalho et al. 2019, the other types of cyber-attacks that could be implemented to disrupt or disable wind turbine systems are brute force, man in the middle, spoofing, jamming, crash override, tripping [14], manipulation of data via IoT (Shekari et al. 2022) [15], and zero-dynamics attacks, according to Wang et al. (2023) [16]. Any combination of these attacks can have detrimental impacts to the affected wind farm as well as the interconnected power grid. Even though these types of attacks haven’t been utilized in the past to disrupt wind farms, it is important to take them into consideration when designing a cyber resilient wind turbine control system.

1.1.3 AI-Based Cyber Solutions for Wind Turbine Generator Control Systems

Since the implementation of wind turbine generators, countless articles have been written about hypothetical control schemes for wind farms. For a deeper look into the different AI control and monitoring methods, this thesis recommends the following articles 17 - 30. With respect to wind turbine generators, detection has been the focus in the academic world. Due to the clear lack of novel mitigation methods, this thesis focuses its attention on this area. The following table 1 lists the detection and mitigation methods reviewed while formulating the novel control approach presented in this thesis.
Table 1: AI Algorithms for Cyber Attack Detection and Mitigation

<table>
<thead>
<tr>
<th>References</th>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>[31]</td>
<td>1.) An event-triggered scheme is proposed in the presence of DoS attacks, which are carried out by a class of periodically detectable jammers. 2) By taking the event-triggered scheme under DoS attacks and deception attacks into consideration, a new model for LFC multiarea power system is constructed as a switched system. 3) On the basis of the new model, the exponentially mean-square stability of LFC multiarea power system is obtained by virtue of Lyapunov stability theory.</td>
<td>The network transmission times are decreased, and the stability of the network transmission times are decreased, and the stability of system is guaranteed under the hybrid cyber-attacks. system is guaranteed under the hybrid cyber-attacks.</td>
<td>Only considers different types of jamming attacks.</td>
</tr>
</tbody>
</table>
| | **using forecast information.**

| **[9]** | **Rules based control method using PDC data (Wide Area Damping Control - WADC) to detect and mitigate FDIA\(\text{\textregistered}\)s w/ RPi in WAMPAC platform.** | **Not sensitive to variable load demand and harmonics introduced from sensors.** | **Threshold could be better configured if a more comprehensive approach taken such as exponential weighted moving average.**

| &nbsp; | **Cheaply implemented.** | **Quick response time.** | **Only 3 phase-to-ground faults considered.**

| &nbsp; | **Bad Data traceback to determine compromised device.** | **Relies on neighboring relay controls for fault state.** |

| **[33]** | **1. A dynamic model is improved for LFC considering cyber-attacks, load disturbance, and the influence of variable wind speeds of a wind farm.**

2. A cooperative control strategy against cyber-attacks for power systems with a high proportion of windfarm is proposed.

3. The parameters of the PI controller and the PID compensation When collaborative control is introduced, the amplitude of frequency deviation is lower, and the convergence is faster. Collaborative has better control effect on the fluctuation caused by wind speed change.

The cooperative controller with parameters obtained by the PSO algorithm can restore its stability when the system faces different |

| &nbsp; | Only considers FDIA and DOS attacks. |
of the cooperative controllers are optimally tuned by the PSO algorithm in order to minimize the deviation of the load frequency.

degrees of attack and wind speed conditions.

| [34] | Consensus based, distributed control of modular multilevel converter (MMC) submodules (SMs) to prevent bad data attacks. Kalman Filter based FDIA detection method. | Flexibility, scalability, and modularity. Doesn’t require high computational burden. | Only considers FDIA. Doesn’t consider attack on central controller. Doesn’t differentiate between cyber attacks and faults in the system. |
| [35] | Pearson correlation coefficient data points w/ autoencoder/decoder and time sequence machine learning algorithm approach finds outliers efficiently to detect FDIA/BDIA and DoS. | High accuracy when detecting outliers. 97% accuracy, 96% precision, and 95.4% recall. | Doesn’t discuss mitigation strategies. |

1.2 Motivation

Based on a thorough literature review, very few AI-based control methods have been utilized to mitigate cyber-attacks on wind farms. Although there are many methods used for monitoring and control of wind turbine generators, as well as a plethora of methods to detect cyber-attacks on wind farms, the clear lack of mitigation methods other than removing the entire wind farm from the power grid leads to room for improvement in the current control methodology.
Specifically, a control method that can not only mitigate data injection attacks to controller set-point values, but also manage the wind turbine generators during network attacks is lacking, and therefore more research in this area is necessary to protect wind farm assets. Based on the National Institute of Standards and Technology (NIST) special publication 800-207, new cyber architectures for access control with respect to wind turbine generators is necessary to prevent cyber-attacks on the energy management system. Therefore, this thesis will also develop a novel zero trust algorithm for use in wind turbine generator access control.

1.3 The Zero Trust Concept

According to Rose et al. (2020) [36], “Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture.” The main goal of ZT is to prevent unauthorized access to data and services that is coupled with access control enforcement that is as granular as possible [36]. In order to minimize uncertainties, the focus is on authentication, authorization, and making the implicit trust zone as small as possible, while maintaining availability and minimizing delays in the authentication mechanism [36].

ZT employs seven tenets, as the concept of removing wide-area perimeter defenses is heavily stressed, and most of the definitions continue to define themselves in relation to the perimeters, such as micro-segmentation or micro-perimeters, as part of the functional capabilities of a ZT architecture [36]. These tenets cover the ideal goal of ZT, and it must be acknowledged that not all tenets may be fully implemented for a given strategy [36].

1.4 Deep Deterministic Policy Gradient Control for Wind Farms

Many different approaches for controlling wind farms have been proposed in the literature, as shown in the next section. In this thesis, a multi-agent DDPG controller was chosen for cyber-
attack mitigation due to several key factors. Firstly, wind farm control often involves making continuous adjustments to the pitch angles of wind turbine blades and other parameters. A DDPG agent is designed for solving problems with continuous action spaces, making it well-suited for such tasks. Other networks such as deep-Q networks (DQN), or artificial neural networks (ANN), are designed for discrete action spaces, and while the data can be discretized, it may be insufficient to capture all the features of the action space. DDPG also uses a deterministic policy, which can lead to more stable training and better convergence in continuous control tasks. In wind farm control, stability is crucial to ensure the turbines operate efficiently and safely. DQN, on the other hand, uses a stochastic policy and can be less stable in continuous action spaces.

Another key feature of DDPG algorithms is that it incorporates experience replay, which helps in breaking correlations between consecutive experiences, making the learning process more stable. This is important in scenarios where data can be highly correlated, such as wind data. DQN also uses experience replay, but it's more critical in continuous action spaces, leading to longer training times and can be less likely to converge. Also, DDPG employs target networks for both the actor and critic networks. This stabilizes the learning process by making the target values less volatile. This is particularly beneficial for wind farm control, where actions can have delayed and long-term effects on the stability of the system. DQN also uses target networks, but ANNs typically do not.

Another key feature of DDPG is that it utilizes an actor-critic method. This means it maintains two separate neural networks, one for estimating the value function (critic) and one for estimating the policy (actor). This separation of tasks makes it easier to optimize the policy in complex environments, such as wind farms. Wind farm control also requires a balance between exploration and exploitation. DDPG incorporates noise in the action space for exploration, which allows it to explore different control actions systematically. DDPG is known for being more sample-efficient than DQN and in wind farm control, where collecting data can be costly or time-consuming, DDPG typically requires fewer samples to achieve better performances, where ANNs, without a reinforcement learning framework, may struggle with the exploration-exploitation balance. Lastly, wind farm control often involves optimizing the controller for long-term rewards, such as maximizing energy production over extended periods of time. A DDPG agent is convenient for
this because it considers the cumulative future rewards, while networks such as ANNs may not naturally capture this long-term perspective.

1.5 Objective of The Thesis

The overall goal of this thesis is to explore new and effective control schemes for wind turbine generators to mitigate adverse effects of cyber-attacks on DFIG control systems, as well as cyber architectures for managing cyber-physical access to energy management systems. To achieve this goal, this thesis proposes to conduct the following research in-depth.

- A grid-connected DFIG model that consists of multiple wind turbine generators, and a communication network that can simulate cyber-attacks on the system.
- New solutions in the form of multi-agent DDPG controller that can mitigate the effects of FDIA and DoS attacks on wind turbine generator controllers has been developed to alleviate the effects of cyber-attacks on a wind farm and the interconnected power grid.
- A novel Zero Trust algorithm for managing cyber-physical access to energy management systems utilizing the NIST special publication 800-207.

1.6 Novelty

Novelty of this thesis stands on the following facts:

- Mitigation strategies for cyber-attacks on grid-connected DFIG-based wind turbine generators has not been explored in full detail.
- The zero-trust concept has not been fully utilized in grid connected wind turbine generator energy management systems.
- This work proposes a novel cyber architecture for wind turbine generator energy management system (EMS), and also a novel control system for mitigation of cyber-attacks on grid-connected wind turbine generator control systems.

1.7 Organization of Thesis

This thesis is organized as follows:
- Chapter-2: Describes the mathematical modeling of a DFIG as well as the interconnected control system. The zero-trust concept is also applied to wind turbine generator energy management systems. Cyber-attack modeling is included.
- Chapter-3 Describes the proposed Zero Trust algorithm with respect to wind farms as well as the proposed multi-agent DDPG control scheme.
- Chapter-4: Shows and describes the simulation results of the proposed control system.
- Chapter-5: Provides the conclusion for this work as well as the future scope of the thesis.

## Chapter 2

### DFIG AND CYBER ATTACK MODELING FOR WIND FARMS

2.1 DFIG Modeling

As mentioned in the previous section, DFIGs have become the go to generator for wind turbine applications as they allow for the decoupling of the torque and the rotor excitation currents (Douiri et al. 2018) [37]. When modeling the DFIG, the generator convention method was used, meaning the currents are seen as outputs and the real and reactive power are positive with respect to being fed into the grid. The stator and rotor voltages and currents are modeled using Parks direct-quadrature, $dq0$, transform method, which allows for complex mathematical equations of the electromagnetic force (EMF) to be reduced to simple algebraic equations. The stator $d$-$q$ voltages ($v_{ds}$, $v_{qs}$) are depicted in equations (6) and (7) and the rotor $d$-$q$ voltages, ($v_{dr}$, $v_{qr}$) are depicted in equations (8) and (9) [37].

\[
\begin{align*}
    v_{ds} &= r_s i_{ds} - \omega_s \lambda_{qs} + \frac{\lambda_{ds}}{dt} \\
    v_{qs} &= r_s i_{qs} - \omega_s \lambda_{qs} + \frac{\lambda_{qs}}{dt} \\
    v_{dr} &= r_r i_{dr} - s\omega_s \lambda_{qr} + \frac{\lambda_{dr}}{dt}
\end{align*}
\]
\[ v_{dr} = r_i i_{dr} - s \omega_s \lambda_{qr} + \frac{\lambda_{dr}}{dt} \quad (9) \]

The flux linkages (\( \lambda \)) are given by the following equations (10), (11), (12), and (13) [37].

\[ \lambda_{ds} = L_s i_{ds} + L_m (i_{ds} + i_{dr}) \quad (10) \]

\[ \lambda_{qs} = L_s i_{qs} + L_m (i_{qs} + i_{qr}) \quad (11) \]

\[ \lambda_{dr} = L_r i_{dr} + L_m (i_{ds} + i_{dr}) \quad (12) \]

\[ \lambda_{qr} = L_r i_{qr} + L_m (i_{qs} + i_{qr}) \quad (13) \]

By utilizing equations 1-8, the active (P) and reactive (R) power generated by the DFIG can be modeled, as depicted in the following equations (14) and (15) [37].

\[ P = v_{ds} i_{ds} + v_{qs} i_{qs} + v_{dr} i_{dr} + v_{qr} i_{qr} \quad (14) \]

\[ Q = v_{ds} i_{ds} - v_{qs} i_{qs} + v_{dr} i_{dr} - v_{qr} i_{qr} \quad (15) \]

Next, as equations 5-15 represent the electrical side of the generator, the mechanical side should also be modeled to give us a robust and dynamic system. The following equation (16) yields the electro-mechanical torque generated by the DFIG [37].

\[ T_{em} = \lambda_{ds} i_{qs} - \lambda_{qs} i_{ds} = \lambda_{dr} i_{dr} - \lambda_{dr} i_{qr} = L_m (i_{qs} i_{dr} + i_{ds} i_{qr}) \quad (16) \]

Lastly, we find the mechanical torque of the generator by dividing the power extracted by the DFIG by the mechanical frequency of the generator (\( \omega_m \)). The differences in the electrical and mechanical torque can then be calculated utilizing the equation of motion for a generator, depicted in equation (17), in which \( J \) is the inertia constant of the generator and \( T_m \) is the mechanical torque [37].
\[
\frac{\partial \omega_m}{\partial t} = \frac{1}{2j} (T_m - T_em)
\]  

(17)

2.2 DFIG Control Methodology

As mentioned in the previous section, dual fed induction wind turbine generators require a sophisticated control system utilizing AC/DC converters and DC/AC inverters to manage the speed of the rotor, the wind power extracted, the reactive power generated by the DFIG, and the DC link voltage. By controlling these parameters, the control systems maintain proper currents and voltages through the generator, as well as the output lines of the generator and the grid side of the system. The pitch angle controller also comes into play, as the amount of power a wind turbine generator can produce is directly proportional to the amount of power the turbines can extract from a given wind stream. Figure 2 depicts a block diagram of a conventional pitch angle controller, with proportional (P) and proportional-integral (PI) gain controllers used to process the error signals with respect to the rotor shaft speed and its reference value, \((\omega_r - \omega_{ref})\), and the measured power and its reference value, \((P_{meas} - P_{ref})\) [10]. This signal is then passed to the actuator and rate limiter to adjust the pitch angle to a specific degree.

![Pitch angle Controller Block Diagram](image)

2.2.1 Grid-side and Rotor-side Converter Controls

The grid-side and rotor-side converters, known as back-to-back converters in this application, are an essential part of any variable speed generator, as they allow for the electronic control of the rotor, which affects the frequency and power output by the wind turbine generator, as well as direct control of the reactive power that will be generated due to the inductive nature of...
DFIGs [38]. The rotor-side converter, as the name implies, has direct control over the speed of the rotor, which directly affects the electronic torque of the wind turbine generator, as well as the overall active power output from the DFIG. The grid-side converter controls the DC-link voltage that exists between the two converters and allows for direct control of the reactive power present in the system. Due to these features, the torque, and the active and reactive power control is decoupled, allowing for better controllability and power quality delivered to the interconnected power grid [38]. Figure 3 depicts the block diagram for the grid-side converter, and figure 4 depicts the block diagram of the rotor-side converter.

Figure 3: Grid-side converter block diagram.

Figure 4: Rotor-side converter block diagram.
In this thesis, both converters are voltage source converters (VSC) utilizing insulated gate bipolar transistor (IGBT)/diode-based converters, in which a series of gates and diodes control the flow of electricity, depending on the duty cycle (D) or modulation index. In the simulation, two voltage-fed, pulse width modulated (PWM) converters are wired to the rotor and stator circuits, which connects the slip ring terminals to the AC supply network electrically [38]. This allows for the direct control of both the magnitude and direction of the power flow between the rotor circuit and the supply side. The grid-side converter is known as an inverter, as it inverts the DC-link voltage to AC voltage. The inverter switching functions and the zero-sequence voltages are derived in the following equations (18), (19), and (20), as reported in Mehdipour et al. (2016) [38].

\[ v_{a0} = \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t) \]  
\[ v_{b0} = \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t - 120^\circ) \]  
\[ v_{c0} = \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t + 120^\circ) \]  

The inverter line to line voltages are depicted in the following equations (21), (22), and (23) [38].

\[ v_{ab} = \sqrt{3} \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t + 30^\circ) \]  
\[ v_{bc} = \sqrt{3} \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t - 90^\circ) \]  
\[ v_{ca} = \sqrt{3} \frac{V_d}{2} \sum_{n=1}^{\infty} A_n \sin(n \omega t + 150^\circ) \]  

To calculate the inverter phase voltages, the zero-sequence voltage \( v_{n0} \) is depicted in the following equation (24) [38].

\[ v_{n0} = \frac{v_{a0} + v_{b0} + v_{c0}}{3} \]
The phase voltages were then obtained as depicted in the following equations (25), (26), and (27) [38].

\[ v_{an} = v_{a0} - v_{n0} \]  
\[ v_{bn} = v_{b0} - v_{n0} \]  
\[ v_{cn} = v_{c0} - v_{n0} \]  

The rotor-side converter works on the same principles as the grid-side inverter; however, it converts AC to DC and is known as a rectifier. The AC equations listed above also apply to the rectifier, however the DC-link voltage must also be modeled. The equation for the DC-link voltage is depicted in the following equation (26) [38].

\[ C \frac{d u_{dc}}{dt} = d_a i_a + d_b i_b + d_c i_c \]  

Where \( \{d_a, d_b, d_c\} \) are the duty-cycles of the converters [38].

To accomplish a decoupled control of both the active and reactive power, several considerations have been made. For the rotor side control, the DFIG is associated with a steady-state grid, as the frequency and amplitude of the grid voltage is assumed steady. The magnetizing current of the stator is determined by the grid. Lastly, the stator flux vector is aligned with the d-axis of the stator. These assumptions allow for the rotor-side converter voltage to be modeled in terms of the rotor current, which is depicted in the following equations (27) and (28) [38].

\[ i_{dr}^* = \frac{-\omega_s L_{ss} i_{ds} - R_s i_{qs} + v_{qs}}{\omega_s L_m} \]  
\[ i_{qr}^* = \frac{R_s i_{ds} - \omega_s L_{ss} i_{qs} - v_{ds}}{\omega_s L_m} \]  

Where \( L_{ss} = L_s + L_m \) and \( L_{rr} = L_r + L_m \). The active and reactive power produced by the stator is then found to be the following equations (29) and (30), respectively [38].
\[ P_s = \frac{3}{2} v_{sd} i_{sd} \]  
\[ Q_s = -\frac{3}{2} v_{sd} i_{sq} \] (29) (30)

The grid-side converter utilizes the vector-control methodology with a reference frame oriented along the stator voltage vector position. This enables independent control of the active and reactive power flowing from the supply and the grid-side converter. The PWM for the grid-side converter is regulated, with the d-axis current used to control the DC-link voltage and the q-axis current to regulate the reactive power. The voltage balance across the inductors in the stator is modeled in the equation (31) found below [38].

\[
\begin{bmatrix}
    v_a \\
v_b \\
v_c,
\end{bmatrix} = R \begin{bmatrix}
    i_a \\
i_b \\
i_c
\end{bmatrix} + L \frac{d}{dt} \begin{bmatrix}
    i_a \\
i_b \\
i_c
\end{bmatrix} + \begin{bmatrix}
    v_{a1} \\
v_{b1} \\
v_{c1}
\end{bmatrix}
\] (31)

Where L and R are the line inductance and the resistance. In the \(dq\) reference frame, the \(v_d\) and \(v_q\) vector of the grid voltage is depicted in the following equations (32) and (33) [38].

\[ v_d = R i_d + L \frac{dv_d}{dt} - \omega_e L i_q + v_{d1} \] (32)

\[ v_q = R i_q + L \frac{dv_q}{dt} - \omega_e L i_d + v_{q1} \] (33)

With the reference \(dq\) voltages for the grid side converter as follows in equations (34) and (35) [38].

\[ v_{d1}^* = \omega L i_{qs} + v_{ds} \] (35)

\[ v_{q1}^* = -\omega L i_{ds} \] (35)

Lastly, the angular position of the grid-side voltage is calculated in the following equation (36) [38].
\[ \theta_e = \int \omega_e dt = \tan^{-1} \frac{v_{gs}}{v_{ds}} \]  

(36)

2.3 Cyber Attack Modeling

In this thesis, the focus of the research was the detection and mitigation of DoS and FDIA attacks on wind turbine systems. The attacks were implemented utilizing MatLab function blocks, and communication controlled multi-switches. When the cyberattack occurred, the multi-switches would change channels and allow for either false data to be injected into the control blocks for the reference set points of specific controllers, or the communication lines would have delay implemented in the measured values or control signals, such as the measurement data used to control the PWM signal of the converter control system.

2.3.1 False Data Injection Attack

To model a false data injection attack in MatLab, the MatLab function block was utilized to implement the formulas found in equations (43) and (44). The formula found in equation (43) represents a scaling attack, in which the attacker manipulates the data measured by a sensor, \( P_i \), and multiplies that value by a scaling factor, \( 1 + \gamma_{scale} \) [32]. This will cause the measurements to increase and force the energy management control system to respond inappropriately, with the worst-case scenarios causing damage to electronic equipment, damage to mechanical components, or disconnection of the wind farm from the interconnected power grid.

\[ P_{scale} = P_i (1 + \gamma_{scale}) \]  

(43)

The second attack modeled in this thesis is a BDIA, in which the communication line of the sensor or controller is blocked, and the attacker injects a malicious measured value or command that will cause a poor response from the control system. In equation (44), the bad data injection attack is modeled, with \( \tilde{y}(t) \) being the parameter or control signal being attacked, \( y(t) \) being the true signal value, \( t_0 \) being the initial sampling time, \( t_{attack} \) is the time in which the data is injected, and \( \alpha(t) \) is the malicious input by the attacker [39].
\[ y(t) = \begin{cases} y(t), & t_0 < t_{\text{attack}} \\ \alpha(t), & t_0 \geq t_{\text{attack}} \end{cases} \] (44)

### 2.3.2 Denial of Service Attack

To implement a DoS attack, a hacker gains access to a control or measurement communication line and sends thousands of empty packets to bottleneck and eventually stop communication between devices. When this occurs, the stability of a wind turbine system can become compromised, as power flow and quality control devices are unable to respond to dynamic fluctuations of the control parameters of the system. In equation (45), a periodic jamming DoS attack is modeled, where \( n \in \mathbb{N} > 0 \) is the period number, \( T \in \mathbb{R} > 0 \) is the period of the jammer, \( T_{\text{off}} \) represents the sleeping time of the jammer, with the lower time bounded by \( T_{\text{off}}^{\min} \) in each jamming signal period, where \( T_{\text{off}}^{\min} \leq T_{\text{off}} < T \) [39]. Within one period of \( T \), the interval \([0, T_{\text{off}})\) denotes the sleeping interval of the jamming signal and the interval \([T_{\text{off}}, T)\) represents the active interval of jamming signal. In this representation, the communication line operates correctly in the interval \([0, T_{\text{off}})\) and is blocked in interval \([(n-1)T, nT]\) [39].

\[ \tau_{\text{DOS}} = \begin{cases} 0, & t \in ([n-1]T, (n-1)T + T_{\text{off}}] \\ 1, & t \in ((n-1)T + T_{\text{off}}, nT] \end{cases} \] (45)

### 2.4 Considered Cyber-Attacks Detection Method/Methods

In this thesis, an event trigger was utilized to detect the DoS attack. To detect a FDIA, the system utilizes the change in the DC-link voltage to determine if the reference set points for the converters has been manipulated as both converters are linked electrically through the DC-link, and magnetically through the generator. The parameters for the event trigger and the DC-link variation are defined in chapter 4, and the correlation between the DC-link voltage and manipulation of set points for the converters is validated in the simulations included in chapter 4. These methods were chosen over other methods as the computational burden to find the ripple in the DC-link voltage and the time difference in two consecutive samples is far less than other.
methods utilized in the literature review. In the following figure 5, a wind farm model is presented with the cyber-attack locations considered in this thesis.

![Wind Farm Model with Cyber-attack Points](image_url)

Figure 5: Wind Farm Model with Cyber-attack Points

2.5 Conclusion

In this chapter, the mathematical modeling of the rotor-side converter and grid-side converter of the DFIG is presented. The mathematical modeling of the considered cyber-attacks in this thesis are also presented. The communication structure of the inverter management system is also displayed.
Chapter 3
Proposed Zero Trust and DDPG Methods For Mitigation of Adverse Impacts of Cyber-Attacks on Wind Farms

3.1 Zero Trust Concept

In this thesis, a zero trust architecture was designed and with adherence to the following seven basic tenets, in accordance with NIST SP 800-207 [36].

1. **All data sources and computing services are considered resources.** A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service, systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

2. **All communication is secured regardless of network location. Network location alone does not imply trust.** Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.

3. **Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted.** Access should also be granted with the least privileges needed to complete the task. This could mean only “sometime recently” for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.
4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.** An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For zero trust, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include, but are not limited to, automated subject analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application. Environmental attributes may include such factors as requestor network location, time, reported active attacks, etc. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least privilege principles are applied to restrict both visibility and accessibility.

5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** This is a constant cycle of obtaining access, scanning, and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management and asset management systems in place. This includes the use of multifactor authentication for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined, and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.

7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

When applying a ZT architecture to the digital structure of an enterprise, there are some basic assumptions for network connectivity. These assumptions include enterprise-owned network infrastructure, and some apply to enterprise owned resources operating on non-enterprise owned network infrastructure, such as public Wi-Fi or public cloud providers [36]. These assumptions are used to direct the formation of a ZTA, and the network in the enterprise implementing a ZTA should be developed utilizing the tenets outlined above along with the following assumptions, as reported in NIST SP 800-207 [36].

1. **The entire enterprise private network is not considered an implicit trust zone.** Assets should always act as if an attacker is present on the enterprise network, and communication should be done in the most secure manner available (see tenet 2 above). This entails actions such as authenticating all connections and encrypting all traffic.

2. **Devices on the network may not be owned or configurable by the enterprise.** Visitors and/or contracted services may include non-enterprise owned assets that need
network access to perform their role. This includes bring-your-own-device policies that allow enterprise subjects to use non-enterprise owned devices to access enterprise resources.

3. **No resource is inherently trusted.** Every asset must have its security posture evaluated via a PEP before a request is granted to an enterprise-owned resource (like tenet 6 above for assets as well as subjects). This evaluation should be continual for as long as the session lasts. Enterprise-owned devices may have artifacts that enable authentication and provide a confidence level higher than the same request coming from non-enterprise owned devices. Subject credentials alone are insufficient for device authentication to an enterprise resource.

4. **Not all enterprise resources are on enterprise-owned infrastructure.** Resources include remote enterprise subjects as well as cloud services. Enterprise-owned or -managed assets may need to utilize the local (i.e., non-enterprise) network for basic connectivity and network services (e.g., DNS resolution).

5. **Remote enterprise subjects and assets cannot fully trust their local network connection.** Remote subjects should assume that the local (i.e., non-enterprise owned) network is hostile. Assets should assume that all traffic is being monitored and potentially modified. All connection requests should be authenticated and authorized, and all communications should be done in the most secure manner possible (i.e., provide confidentiality, integrity protection, and source authentication). See the tenets of ZTA above.

6. **Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture.** Assets and workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise networks (i.e., remote users). This also includes workloads migrating from on-premises data centers to non-enterprise cloud instances.
A ZTA is composed of numerous logical components that can be deployed in an enterprise [36]. These components may be operated as an on-premises service or through a cloud-based service and can use a separate control plane to communicate, while application data is communicated on a data plane. In figure 6, the basic relationship between the components and their interactions is displayed, with a breakdown of the components and their description following the image, found in NIST SP 800-207 [36].

![Figure 6: Zero Trust Logical Components.](image)

- **Policy engine**: This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm (see Section 3.3 for more details) to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.

- **Policy administrator**: This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It would generate any session-specific authentication and authentication token, or
credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service; here, it is divided into its two logical components. The PA communicates with the PEP when creating the communication path. This communication is done via the control plane.

- **Policy enforcement point:** This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone (see Section 2) hosting the enterprise resource.

Along with the core components in an enterprise implementing a ZTA, there are several data sources provided as input and policy rules used by the PE when making decisions. These include local data sources as well as external data sources that are included in the NIST SP 800-207 publication [36]. These can include:

- **Continuous diagnostics and mitigation system:** This gathers information about the enterprise asset’s current state and applies updates to configuration and software components. An enterprise CDM system provides the policy engine with the information about the asset making an access request, such as whether it is running the appropriate patched operating system, the integrity of enterprise-approved software components or presence of non-approved components and whether the asset has any known vulnerabilities. CDM systems are also responsible for identifying and potentially enforcing a subset of polices on non-enterprise devices active on enterprise infrastructure.
• **Industry compliance system**: This ensures that the enterprise remains compliant with any regulatory regime that it may fall under (e.g., FISMA, healthcare or financial industry information security requirements). This includes all the policy rules that an enterprise develops to ensure compliance.

• **Network and system activity logs**: This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.

• **Data access policies**: These are the attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in (via management interface) or dynamically generated by the policy engine. These policies are the starting point for authorizing access to a resource as they provide the basic access privileges for accounts and applications/services in the enterprise. These policies should be based on the defined mission roles and needs of the organization.

• **Enterprise public key infrastructure**: This system is responsible for generating and logging certificates issued by the enterprise to resources, subjects, services and applications. This also includes the global certificate authority ecosystem and the Federal PKI,4 which may or may not be integrated with the enterprise PKI. This could also be a PKI that is not built upon X.509 certificates.

• **ID management system**: This is responsible for creating, storing, and managing enterprise user accounts and identity records (e.g., LDAP server). This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets. This system often utilizes other systems (such as a PKI) for artifacts associated with user accounts. This system may be part of a larger federated community and may include non-enterprise employees or links to non-enterprise assets for collaboration.
- **Security information and event management system**: This collects security centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets.

Depending on the workflows that an enterprise chooses to implement, there can be several ways to enact a ZTA. These approaches vary depending on the components used in the main source of policy rules for an organization. In each case, all tenets of ZT will be implemented; however, only one or two will be used as the main driver of the policies. A full ZT solution include elements of all three approaches and include enhanced identify governance-driven, logical, micro-segmentation, and network-based segmentation [36]. Depending on the approach, an organization may find that its chosen use case and existing policies point to one approach over others, but that does not mean the other approaches will not work but rather that the other approaches may be more difficult to implement or may require a more fundamental change to how the enterprise currently conducts business flows [36].

When it comes to zero trust and wind farms, several of the tenets from the zero-concept section will be utilized. The following six bullet points offer a guideline for utility providers that operate wind farms when attempting to provide adequate security for their assets.

- Identify and classify all assets and resources, including hardware, software, and data in the Energy Management System.
- Strong Authentication and access control measures should be utilized i.e., every user, device and/or application that requests access to the control system should be authorized – based on level of access privilege. (MFA, ACL, RBAC).
- Strict network segmentation – control systems should be divided into smaller segmented zones that are isolated from each other and controlled independently.
- All traffic should be monitored and analyzed for suspicious activity or anomalies. (IDPS and SIEM).
- Encryption and data protection measures for sensitive data in control systems. (Such as AES-256).
• Continuously test and evaluate the security posture of the system including regular security assessments, penetration testing, and vulnerability scanning. (Remediation plans should be in place).

The flow chart depicted in figure 7 illustrates the guidelines presented in the bullet points listed above.

![Zero Trust Concept Flow Chart]

**Figure 7: Zero Trust Concept Flow Chart**

### 3.2 Proposed Zero Trust Algorithm

In this thesis, a perimeter-based zero trust model is recommended, in which the traditional network perimeter is dissolved, and all network traffic is treated as untrusted. Access controls and authentication mechanisms are applied at a granular level based on user and device attributes, regardless of their location network boundary. This model ensures that every access request is evaluated and authenticated individually, regardless of the network type, such as satellite communication. This model was chosen for wind farms, as many are located in remote locations, require satellite communication for monitoring, control, and even some diagnostic functions.
This thesis also recommends utilizing the Partner/Third-Party zero trust model which focuses on extending the zero trust principles to external entities, such as third-party vendors or partners, who require access to the system. This model treats these entities as untrusted and applies access controls and authentication mechanisms to verify their identities and enforce the principle of least privilege. This ensures that third-party vendors can access only specific resources and perform only the necessary tasks for monitoring and maintaining the system. This method was chosen for wind farms, as third-party vendors typically monitor and maintain the wind farm components, including the wind turbine generators and the electrical control devices. It is important to apply the least privilege principle to vendors so that if they have a data breach, there will be limited information and access to wind farm control system available to the attackers.

The following figure 8 depicts the zero-trust concept as a preventative measure for wind farm cyber security, and appendix A depicts the zero-trust concept in algorithm form, written in the computer language Python, and written on the platform GoogleColab. One important note, the encryption algorithm is a well-known algorithm not written by the authors and was created using an example code created by IBM [41].

![Figure 8: Zero-Trust Concept in Wind Farms.](image)

3.3 Deep Deterministic Policy Gradient

As detailed in chapter 1, subsection 1.1.4, DDPG is an optimal candidate for wind turbine generator control. The DDPG algorithm is a model-free, online, off-policy reinforcement learning
method, that utilizes an actor-critic reinforcement learning agent that can search for an optimal policy that can maximize the expected cumulative long-term reward [40]. The DDPG algorithm utilizes two neural networks, known as actor-critic networks, where the actor, denoted as \(\pi(S; \theta)\), with parameters \(\theta\), takes an observation, \(S\), and returns the corresponding action that maximizes the long-term reward [40]. The critic, denoted as \(Q(S, A; \phi)\) with parameters \(\phi\), takes an observation, \(S\), and an action, \(A\), and returns the long-term expected value [40]. The DDPG also leverages a target actor and a target critic. The target actor, denoted as \(\pi_\tau(S; \theta_\tau)\), is used to improve the stability of the optimization, by allowing the agent to periodically update the target actor parameters, \(\theta_\tau\), using the latest actor parameter values [40]. The target critic, denoted as \(Q_\tau(S, A; \phi_\tau)\) is also used to stabilize the optimization, as the agent periodically updates the target critic parameters, \(\phi_\tau\), using the latest critic parameter values [40].

The training algorithm, depicted on MathWorks [40], begins by initializing the critic with random parameter values and then initializes the target critic with the same parameter values. This is also done with the actor and target actor parameters, respectively. For each training time step, there are 8 steps that will be completed and are listed as follows [40]:

1. For the current observation \(S\), select an action \(A = \pi(S; \theta) + N\), where \(N\) is the stochastic noise.
2. Execute action \(A\). Observe the reward and next observation \(S'\).
4. Sample a random mini-batch of \(M\) experiences \((S_i, A_i, R_i, S'_i)\) from the experience buffer.
5. If \(S'_i\) is a terminal state, set the value function target \(y_i\) to \(R_i\). Otherwise, set it to equation (37).

\[
y_i = R_i + \gamma Q_\tau(S'_i, \pi_\tau(S'_i; \theta_\tau); \phi_\tau)
\]

The value function target is the sum of the experience reward, \(R_i\), and the discount future reward. To compute the cumulative reward, the agent first computes the next action by passing the next observation, \(S'_i\), from the sampled experience to the target actor. The agent then finds the cumulative reward by passing the next action to the target critic [40].

6. Update the critic parameters by minimizing the loss, \(L\), across all sampled experiences, as depicted in the following equation (38).
\[ L = \frac{1}{2M} \sum_{i=1}^{M} (y_i - Q(S_i, A_i; \phi))^2 \]  

7. Update the actor parameters using the following sampled policy gradient to maximize the expected discounted reward, as depicted in equations (39), (40), and (41).

\[ \nabla_{\theta} J \approx \frac{1}{M} \sum_{i=1}^{M} G_{ai} G_{\pi i} \]  

(39)

\[ G_{ai} = \Delta_{A} Q(S_i, A_i; \phi) \quad \text{where} \quad A = \pi(S_i; \theta) \]  

(40)

\[ G_{\pi i} = \nabla_{\theta} \pi(S_i; \theta) \]  

(41)

8. Update target actor and critic parameters depending on the target method.

The target update method has 3 options: smoothing, periodic, and periodic smoothing [40].

- **Smoothing** – Update the target parameters at every time step using smoothing factor, \( \tau \). The equations for updating the target parameters utilizing the smoothing factor is depicted in equations (42) and (43).

\[ \phi_t = \tau \phi + (1 - \tau) \phi_t \quad \text{(for critic parameters)} \]  

(42)

\[ \theta_t = \tau \theta + (1 - \tau) \theta_t \quad \text{(for actor parameters)} \]  

(43)

- **Periodic** – Update the target parameters periodically without smoothing.

- **Periodic Smoothing** – Update the target parameters periodically with smoothing.

3.4 Proposed DDPG Control Methodology

In this thesis, a multi-agent DDPG algorithm is leveraged to predict the stator and rotor current reference values, \( \{i_{ds}^*, i_{qs}^*, i_{dr}^*, i_{qr}^*\} \) for the grid-side and rotor-side converters. These values are then be used to predict the \( d-q \) \( \{v_{dr}^*, v_{qr}^*\} \) reference rotor voltages that are then passed
to the PWM controller to determine the proper duty cycle for the rotor-side converter. If an FDIA/BDIA is launched against the reference values for the controllers, the effect will be seen on the DC-link voltage, and the DDPG controller will then replace the missing reference values to prevent the system from reacting to the attack. If a DoS attack occurs and communication between the SCADA and the converter system is blocked or jammed, the packet sampling time $t_{\text{received}}$ will violate the minimum and maximum allowed sampling times, which are based on the specific network communication structure. The affected communication line will then be disconnected from the system, and the specific DDPG agent will assume control of the affected system until a cyber team can assess and respond accordingly to the situation. In this thesis, the sampling time will be based on the simulation sampling time, which is 50 microseconds per sample.

By integrating these algorithms into a controller that is physically attached to the converters, the PWM signals will be consistently updated in the event of a sophisticated cyber-attack conducted against the communication network of a wind turbine generator or wind farm, as there will be no wireless nodes to be attacked in the DDPG network. The following figure 9 displays the flow chart of the proposed control algorithm, with figure 10 depicting the block diagram of the proposed multi-agent DDPG converter controllers.
Figure 9: Proposed multi-agent DDPG control network flow chart.

Figure 10: Proposed multi-agent DDPG control network block diagram.
3.4.1 Stator Active and Reactive Power Measurement and Set Points

According to Douiri et al. (2018), the direct (d) part of the stator current is directly related to the real power of the stator and the quadrature (q) part of the stator current is related to the reactive power of the stator [13]. Thus, by utilizing these values, the real and reactive power of the stator can be found mathematically in real time. Equations (29) and (30), referenced earlier in the thesis, are utilized to calculate these values. The data points are created using a small-scale wind farm, consisting of six wind turbine DFIGs, and the AI controller is trained during a live simulation; therefore, the training should closely resemble real world parameters. The set points for the system are determined by the generators utilized in the wind farm and are considered constants under best case scenarios. In this thesis, the stator active power set point is 9 MW, and the reactive power set point is 0 MVAR.

3.4.2 Stator Current Reference Point Sub-system

The stator current is predicted utilizing the active and reactive power measurements of the stator, as well as the measured DC-link voltage, and the reference DC-link voltage. The real and reactive power measurements, as well as the DC-link measured voltage, along with their respective reference points are used as observations in this network, and the outputs of the network are compared to the conventional system for the reward calculation during live training. In the conventional wind turbine generator control system, a PI controller is utilized to adjust the gains to maintain stability in the system.
Figure 11: (a) DDPG Actor Network for Stator $i_{dq}$ Reference Points; (b) DDPG Critic Network for Stator $i_{dq}$ Reference Points
The first fully connected layer of the actor network consists of 20 nodes, with the relu activation function. The second fully connected layer of the actor network consists of 10 nodes with the relu activation function. The final fully connected layer of the actor network consists of 6 nodes, with the relu activation function, and the final output node outputs the predicted $i_{ds}$ and $i_{qs}$ measurements.

The critic network has the same structure for the observation side; however, the action side consists of a layer of 10 nodes, and then a layer of 6 nodes, both using the relu activation function. The output of the observation node and action nodes are then added together in a fully connected node, with the output yielding the predicted reward of the step, based on the state-action pair.

### 3.4.3 Rotor Current Set Point Sub-system

By using the measured stator current d-q values along with the measured stator voltage d-q values, the rotor reference d-q current values can be found. Used along with the rotor speed $\omega_r$ as observations, the DDPG agent can quickly and accurately predict the reference set points for the rotor current d-q values. In the conventional system, this process is done by a PI controller, which again will be removed from the system in the event of a cyber-attack, so that the DDPG agent can replace any missing set-point values and maintain a steady-state of the system until cyber analysts can resolve the breach. In the following figure 12, the actor and critic networks for the rotor current d-q predictions are depicted.
Figure 12: (a) DDPG Actor Network for rotor $i_{dq}$ Reference Points; (b) DDPG Critic Network for Rotor $i_{dq}$ Reference Points
The network is structured in the same way as reported in the first sub-section.

3.4.4 Rotor Voltage Set Point Sub-System.

The d-q reference values for the rotor voltage is found by using the rotor current d-q measured values and the rotor current d-q reference values. Also, the rotor speed, $\omega_r$, is utilized as an input in this agent. Typically, a PI controller would have the error of the reference values compared to the measured values as inputs, and then a specified gain would be applied to keep the system stable and output the reference d-q voltage values. In this thesis, the measured rotor d-q currents, the rotor speed, $\omega_r$, and reference rotor d-q current values are used as inputs to the DPPG agent, and the output of the conventional PI controller system is used to determine the reward for the current state/action pair. The DDPG agent was trained during a live simulation, so the agent will be better equipped to handle real world scenarios. When a cyber-attack occurs, the DDPG agent will be utilized to replace the missing set-points, or in the event of a DoS attack, both rotor DDPG agents will control the entire system until a cyber defense team can quarantine the effected unit. The following figure 13 depicts the actor and critic networks of the rotor voltage set-point DDPG controller.
Figure 13: (a) DDPG Actor Network for rotor $v_{dq}$ Reference Points; (b) DDPG Critic Network for Rotor $v_{dq}$ Reference Points
3.5 **Conventional PI Controller**

In this thesis, the performance of the proposed multi-agent DDPG controller has been compared to the performance of the conventional PI controller during the considered cyber-attacks. Therefore, a description of the PI controller and its structure is described and depicted below. The conventional PI controller takes a specified measured signal and utilizes a feedback loop from its output to determine the error of output versus the input. The error is fed through the controller and finds the integral of the error with respect to time as well as a proportional gain. These values are then added together and become the output of the system, which as was stated before, is fed back into the input and is subtracted from the measured value. The PI controller can be tuned utilizing several different methods, such as the root locust method to ensure proper stability of the system; however, in this thesis, the PI controller was tuned only for normal operation, and not for the mitigation of cyber-attacks. The following figure 14 depicts the conventional PI controller, with $k_1$ being the tuned proportional gain, and $\frac{k_2}{s}$ being the tuned integrated gain. The inputs and outputs considered in this thesis for the PI controllers can be found in the RSC and GSC block diagrams, found in chapter 2, and the gain values are listed in the simulation parameter table found in chapter 4.

![Figure 14: PI Controller Block Diagram.](image)

3.6 **Conclusion**

In this chapter, the zero-trust concept is presented, along with the proposed zero trust algorithm for wind farm EMS. The proposed multi-agent DDPG network is also presented along with the methodology for creating the algorithm. Lastly, the conventional PI control scheme is presented and displayed to give a better understanding of how the conventional system operates.
In this chapter, the effectiveness of the proposed controller has been presented to prove the effectiveness of the system, as well as validate the approach. The effectiveness of the system will be determined by the visual performance of the system, as well as a numerical score based on the controller’s ability to control the system during a cyber-attack, when compared to the conventional controller. The root mean square error (RMSE) of the conventional controller and the DDPG controller was computed and then compared to validate the proposed control system and will be included in the final chapter.

4.1 Simulation Parameters

The simulation for this thesis was conducted using the MATLAB/Simulink software. The simulation uses a pre-built wind farm provided by MathWorks. In the simulation, a grid-connected, 9 MW wind farm consisting of 6 DFIG-based wind turbines is used to train and test the performance of the control system. The following table 4 presents the parameters for the grid-connected wind farm used in the simulation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal Power - $P_{nom}$</td>
<td>10 MVA</td>
</tr>
<tr>
<td>Line-to-line Nominal Voltage - $V_{l-l,nom}$</td>
<td>575 $v_{rms}$</td>
</tr>
<tr>
<td>Nominal Rotor Voltage - $V_{r-nom}$</td>
<td>1975 $v_{rms}$</td>
</tr>
<tr>
<td>Nominal Frequency - $F_{nom}$</td>
<td>60 Hz</td>
</tr>
<tr>
<td>Stator Resistance - $R_s$</td>
<td>0.023 p.u.</td>
</tr>
<tr>
<td>Stator Inductance - $L_{ls}$</td>
<td>0.18 p.u.</td>
</tr>
<tr>
<td>Rotor Resistance - $R_r$</td>
<td>0.016 p.u.</td>
</tr>
</tbody>
</table>

Table 2: Simulation parameters for small scale grid connected wind farm.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotor Inductance - $L_{ir}$</td>
<td>0.16 p.u.</td>
</tr>
<tr>
<td>Mutual Inductance - $L_m$</td>
<td>2.9 p.u.</td>
</tr>
<tr>
<td>Inertia Constant - $H$</td>
<td>0.685 s</td>
</tr>
<tr>
<td>Friction Factor - $F_\mu$</td>
<td>0.01 p.u.</td>
</tr>
<tr>
<td>Number of Pole Pairs - $P_#$</td>
<td>3</td>
</tr>
<tr>
<td>RSC PWM Frequency - $PWM_{freq-rsc}$</td>
<td>1620 Hz</td>
</tr>
<tr>
<td>GSC PWM Frequency - $PWM_{freq-gsc}$</td>
<td>2700 Hz</td>
</tr>
<tr>
<td>DC-Link Nominal Voltage - $V_{dc-nom}$</td>
<td>1150 V</td>
</tr>
<tr>
<td>DC-Link Capacitor - $C_{dc-link}$</td>
<td>10 mF</td>
</tr>
<tr>
<td>Nominal Mechanical Power - $P_{mec-nom}$</td>
<td>9 MW</td>
</tr>
<tr>
<td>DC PI Gains - $K_{p-dc}, K_{l-dc}$</td>
<td>[8, 400]</td>
</tr>
<tr>
<td>GSC PI Gains - $K_{p-gsc}, K_{l-gsc}$</td>
<td>[0.83, 5]</td>
</tr>
<tr>
<td>RSC PI Gain - $K_{p-rsc}, K_{l-rsc}$</td>
<td>[0.6, 8]</td>
</tr>
<tr>
<td>Rotor Speed PI Gains - $K_{p-\omega}, K_{l-\omega}$</td>
<td>[3, 0.6]</td>
</tr>
<tr>
<td>Reactive Power PI Gains - $K_{p-var}, K_{l-va}$</td>
<td>[0.05, 20]</td>
</tr>
<tr>
<td>Pitch Controller P Gain - $K_p$</td>
<td>150</td>
</tr>
<tr>
<td>Pitch Compensation PI Gains - $K_p, K_l$</td>
<td>[3, 30]</td>
</tr>
<tr>
<td>Max Pitch Angle</td>
<td>27°</td>
</tr>
<tr>
<td>Max Pitch Rate of Change</td>
<td>10°/s</td>
</tr>
<tr>
<td>Sampling Time - $T_s$</td>
<td>50 μs</td>
</tr>
</tbody>
</table>
4.1.1 Cyber Attack Scenarios

In the simulation, a DoS attack, an FDIA, and a combination of both attacks were implemented on the wind turbine generator control system. In all case studies, if the communication signal violated the time sampling bounds of 50 μs, or if the DC-link voltage fluctuated greater than 5% of the nominal voltage, the controller then checked if the specific set points changed more than 5% of their original values, and if this is found to be the case, the specified DDPG agent will be commanded on.

In the first scenario, the PWM signal to the rotor-side converter will be hit with a DoS attack in the form of a jamming attack. The signal to the converter will be extremely delayed, with the jamming signal pushing a ‘0’ value to the controllers, effectively disabling them. In the second, third, and fourth scenarios, the set points for the current and voltage d-q parameters will be adjusted with a scaling attack. This will cause an increase or decrease in the set-point values, causing over-voltage or under-voltage conditions. In the fifth scenario, a combination of both attacks will occur on the rotor-side control system. The following table 5 depicts each attack scenario along with the specific parameters being manipulated, and figures 15 and 16 depict the conventional PI controllers under a DoS attack on the rotor-side controller PWM signal and an FDIA attack on the stator current set points. These figures clearly show the need for a mitigation strategy when cyber-attacks occur on wind turbine generator control systems.

<table>
<thead>
<tr>
<th>Case Study Number</th>
<th>Attack Type</th>
<th>Parameter Manipulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Study 1</td>
<td>DoS</td>
<td>Rotor-side Converter Sampling time for PWM, $T_s$</td>
</tr>
<tr>
<td>Case Study 2</td>
<td>FDIA</td>
<td>Stator Current Set Points $i_{dqs}^*$</td>
</tr>
<tr>
<td>Case Study 3</td>
<td>FDIA</td>
<td>Rotor Current Set Points $i_{dqr}^*$</td>
</tr>
<tr>
<td>Case Study 4</td>
<td>FDIA</td>
<td>Rotor Voltage Set Points $v_{dqr}^*$</td>
</tr>
<tr>
<td>Case Study 5</td>
<td>DoS + FDIA</td>
<td>Rotor-side converter sampling time for PWM and rotor voltage set points, $T_s$ and $i_{dqr}^*$</td>
</tr>
</tbody>
</table>
4.1.2 Case Study 1

The first scenario simulated in this thesis involves jamming the communication line to the rotor-side converter so that the pulse width modulation (PWM) signal becomes intermittent. In this case, the rotor speed will become oscillatory, and the effects will be seen on the active power.
measurement of the system. The system will become damaged if proper action isn’t taken. The jamming attack will start at $T = 1$ second and will repeat every 2 seconds, in on for one second, off for two second intervals until 8 seconds. The following figures 17, 18, 19, and 20 depict the active power, reactive power, rotor speed, and DC-link voltage, respectively, of the conventional PI controller versus the DDPG controller during the DoS attack.

Figure 17: Active power during DoS attack on rotor-side PWM signal.
Figure 18: Reactive power during DoS attack on rotor-side PWM signal.

Figure 19: Rotor Speed p.u. during DoS attack on rotor-side PWM signal.
As depicted in the figures above, the DoS attack has devastating impacts on the wind turbine generator control system. The active and reactive power become extremely unstable, and the rotor speed becomes oscillatory. There are spikes in the DC-link voltage that has a difficult time recovering. Damage to the wind turbine generator components would likely occur due to this attack if a proper cyber mitigation plan isn’t utilized.

4.1.3 Case Study 2

In this scenario, the current set points for the stator will be attacked with a scaling FDIA. In this case, the reactive power will become unstable and will likely collapse if proper action isn’t taken quickly and it will influence the DC-link voltage. The effects of this attack will also be seen on the active power and the rotor speed. The ramping signal will utilize equation 43 and utilize a scaling value of 0.2. The ramping attack will start at $T = 2$ seconds and will repeat every 2 seconds, in on for one second, off for two second intervals until 9 seconds. The following figures 21, 22, 23, and 24 depict the active power, reactive power, rotor speed, and DC-link voltage, respectively, of the conventional PI controller versus the DDPG controller during the FDIA attack.
Figure 21: Active power during FDIA on stator $i_{dq}^*$ set points.

Figure 22: Reactive power during FDIA on stator $i_{dq}^*$ set points.
Figure 23: Rotor speed p.u. during FDIA on stator $i_{dq}^*$ set points.

Figure 24: DC-link voltage during FDIA on stator $i_{dq}^*$ set points.
From the figures, it is clear that the ramping FDIA has detrimental effects on the wind turbine generator control system. In this scenario, the DDPG agent for the stator current reference points vastly outperforms the conventional controller during the attack. Without a proper cyber mitigation controller, the wind generators in this wind farm would be badly damaged.

### 4.1.4 Case Study 3

In this scenario, the current set points for the rotor will be attacked with a scaling FDIA. In this case, the rotor speed will become oscillatory and will likely cause damage to the system if proper action isn’t taken quickly. The effects will also be seen on the active power of the system, as well as the reactive power and the DC-link voltage. The ramping attack will start at \( T = 2 \) seconds and will repeat every 2 seconds, in on for one second, off for two second intervals until 9 seconds. The following figures 25, 26, 27, and 28 depict the active power, reactive power, rotor speed, and DC-link voltage, respectively, of the conventional PI controller versus the DDPG controller during the FDIA attack.

![Active Power during FDIA on rotor](image)

**Figure 25:** Active power during FDIA on rotor \( i_{dq}^* \) set points.
Figure 26: Reactive power during FDIA on rotor $i_{dq}^*$ set points.

Figure 27: Rotor speed p.u. during FDIA on rotor $i_{dq}^*$ set points.
As shown in the figures, the scaling FDIA on the rotor-side converter $i_{dq}^*$ set points is just as detrimental to the system as the scaling attack on the stator $i_{dq}^*$ set points. From this case, it is clear why the AI controller for cyber mitigation is necessary for mitigating FDIAs on wind turbine generator control systems.

### 4.1.5 Case Study 4

In this scenario, the voltage set points for the rotor will be attacked with a scaling FDIA. In this case, the rotor speed will again become oscillatory and will likely cause damage to the system if proper action isn’t taken quickly. The effects will also be seen on the active power as well as the reactive power and the DC-link voltage of the system. The ramping attack will start at $T = 2$ seconds and will repeat every 2 seconds, on for one second, off for two second intervals until 9 seconds. The following figures 29, 30, 31, and 32 depict the active power, reactive power, rotor speed, and DC-link voltage, respectively, of the conventional PI controller versus the DDPG controller during the FDIA attack.
Figure 29: Active power during FDIA on rotor $v_{dq}^*$ set points.

Figure 30: Reactive power during FDIA on rotor $v_{dq}^*$ set points.
Figure 31: Rotor speed p.u. voltage during FDIA on rotor $v_{dq}^*$ set points.

Figure 32: DC-link voltage during FDIA on rotor $v_{dq}^*$ set points.
In this case, the FDIA causes the rotor speed to become extremely erratic. The effects can be seen on both the active and reactive power of the system, as well as the DC-link voltage. The DDPG agent performs as designed, keeping the system in a steady state condition until a cyber forensics team can determine which controller was affected and remove it from the system. In this scenario, the rotor components would likely be damaged due to the extreme oscillations.

4.1.6 Case Study 5

In the last scenario, the rotor-side converter PWM signal will be attacked by a jamming attack, while the current set points for the rotor are also attacked with a scaling FDIA. In this case, the rotor speed will again become very oscillatory and will cause damage to the system if proper action isn’t taken quickly. The effects will also be seen on the active and reactive power of the system. The DoS attack will start at T = 1 second and will repeat every 2 seconds, in on for one second, off for two second intervals until 8 seconds, with the FDIA being delayed 0.5 seconds, making its interval T = 1.5 seconds until T = 8.5 seconds. The following figures 33, 34, 35, and 36 depict the active power, reactive power, rotor speed, and DC-link voltage, respectively, of the conventional PI controller versus the DDPG controller during the combination DoS and FDIA.
Figure 33: Active power during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM.

Figure 34: Reactive power during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM.
Figure 35: Rotor Speed p.u. during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM.

Figure 36: DC-link voltage during combination DoS and FDIA on rotor $v_{dq}^*$ set points and rotor-side PWM.
In what is the worst-case scenario for a control system, both the communication lines are blocked, and the data has been manipulated, causing the system to react very poorly and likely damage the electrical and mechanical components of the DFIG. These effects would be seen on the interconnected power grid, and the wind farm would likely be removed from the system, causing a reduction in the amount of available power for consumers. As can be seen by the figures, the active and reactive powers as well as the DC-link voltage and the rotor speed become extremely erratic. The DDPG agents work in unison to mitigate the effects of the attack.

### 4.1.7 Error-based Performance Evaluation of Proposed Controller

In this thesis, the performance evaluation was conducted by finding the root mean square error (RMSE) of the conventional controller and the proposed DDPG controller, and then comparing the two. The RMSE is a standard metric used in model evaluation, as it is the optimal metric for “normal” errors and determines how the model “fits” the data [42]. In the power system, and with respect to wind energy generation, there is an acceptable amount of deviation from the optimal set points that will still allow the system to remain in a steady state condition. Due to this feature, RMSE is a better option than mean absolute error. To determine the RMSE, the formula depicted in the following equation 46 was utilized.

\[
RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (\hat{y}_i - y_i)^2}
\]  

(46)

Where \( n \) is the number of observations, \( y_i \) is the theoretical value and \( \hat{y}_i \) is the experimental value. In this this, the \( y_i \) values are the set points for the specific measured value and \( \hat{y}_i \) is the simulated value obtained by the AI controller. The following table 6 depicts the RMSE evaluation of the conventional controller and the DDPG agents.
### Table 4: RMSE Performance Evaluation

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Attack Type</th>
<th>Active Power RMSE</th>
<th>Reactive Power RMSE</th>
<th>Rotor Speed RMSE</th>
<th>DC-Link Voltage RMSE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DoS</td>
<td>FDIA</td>
<td>PI</td>
<td>DDPG</td>
<td>PI</td>
</tr>
<tr>
<td>1</td>
<td>✓</td>
<td>-</td>
<td>5.029</td>
<td>0.075</td>
<td>1.393</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>✓</td>
<td>25</td>
<td>0.480</td>
<td>154</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>✓</td>
<td>8.205</td>
<td>0.477</td>
<td>6.783</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>✓</td>
<td>10</td>
<td>0.045</td>
<td>6.949</td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>17</td>
<td>0.074</td>
<td>38</td>
</tr>
</tbody>
</table>

From the case studies presented in the table, the performance of the DDPG agents during a cyber-attack is clearly better than its conventional counterpart, as denoted with the green highlighting. With more training and fine tuning of the inputs, the DDPG agent could perform even better. Also, implementing an agent to predict the stator rotor voltage set points could also help alleviate cyber-attacks on the grid-side converter.

#### 4.1.8 ZT Based Test Results

As the zero-trust concept will be applied to the development phase of the EMS, the zero-trust algorithm’s effectiveness will be seen in the implementation of the system, and therefore results cannot be presented at this time. Since the zero-trust algorithm was created using guidance from NIST SP 800-207 [36], the architecture of the algorithm is designed to prevent cyber criminals from gaining access to the EMS by giving every entity in the cyber-physical system a status of least trust. This leaves the decision of who is given access to a specific resource to the policy enforcement point, as was displayed in figure 8. The following figure 37 depicts the flow chart of the proposed algorithm, which mirrors the seven tenets of zero-trust perfectly.
4.2 Conclusion

This chapter compares the conventional controller and the DDPG controller during 5 different case studies. The DDPG controllers vastly outperform the PI controllers in the system during cyber-attacks and can mitigate any of the effects of the cyber-attack on the control system, as shown in the figures for each sub-section.
Chapter 5
CONCLUSION AND FUTURE WORKS

5.1 Conclusion

This work researches the effects of different types of cyber-attacks on the control system of a grid-connected wind farm. This thesis can be concluded as follows:

- This work provides detailed modeling of a DFIG-based wind turbine generator including its control system.
- A ZT architecture is proposed to prevent cyber-attacks on vital EMS.
- A multi-agent DDPG AI controller has been designed and leveraged to mitigate the effects of cyber-attacks on the EMS of a wind turbine generator.
- The proposed system can mitigate the attack regardless of which set point is manipulated or if the PWM signal to the rotor-side converter is blocked.

5.2 Contribution of this thesis

- This research proposes a novel mitigation method for cyber-attacks on wind farms, which from the literature review, is severely lacking.
- The controller is dynamic and can mitigate cyber-attacks in several locations of the EMS, making it robust.
- The worst-case scenarios (DDoS, FDIA, and the combination) for cyber-attacks on wind turbine generators have been considered.
- Implementing the proposed control scheme will ensure stability in the system during cyber-attacks.

BROAD IMPACT OF THIS WORK

This research will provide a new approach to distributed energy resource control and will have impacts on society beyond just from a power generation perspective.
• Emergency services, such as hospitals and police, require power to provide lifesaving services during emergencies. The military also needs reliable energy production to operate military bases all over the world. This thesis offers a solution to prevent cyber-attacks from causing chaos in these industries.

• Basic consumers will have more reliable power, and cyber-attacks will impact their lives less than they currently do.

• Autonomous energy generation has become a practical approach to control for power generation, and this research has a positive contribution to the respective field.

5.3 Future scope of this thesis

This work could be extended to the following tasks:

• The stator voltage controller can be replaced by a DDPG agent, allowing for the PWM signal to be replaced for the grid-side converter during a cyber-attack, like what was presented for the rotor side control system.

• The method can be utilized for other DERs, such as ocean/wave energy production.

• The effects of a battery energy storage system on the DC-link circuit could be investigated to determine if better stability can be achieved.

• Exploring new AI detection and mitigation techniques based on the works presented in the thesis could be explored.
Appendix A: Zero Trust Algorithm for Wind Farms

def ZT_algorithm(user, resource, network_fprint, second_factor):
    # Authenticate the user
    if not authenticate_user(user):
        return "Access denied"

    # Perform multifactor authentication
    if not multifactor_authentication(user, second_factor):
        return "Access denied"

    # Authorize the user
    if not authorize_user(user, resource):
        return "Access denied"

    # Apply additional access controls
    if not apply_access_controls(user, resource, network_fprint):
        return "Access denied"

    # Log the user's access
    log_access(user, resource, network_fprint)

    # Grant access to the resource
    return "Access granted"

# Start sample code
# Example Encryption Algorithm

def encrypt_data(key, data):
    # Generate a random initialization vector (IV)
    iv = os.urandom(16)

    # Create a cipher using AES in CBC mode with the generated IV
    cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
                    backend=default_backend())

    # Encrypt the data
    encryptor = cipher.encryptor()
    padder = padding.PKCS7(128).padder()
    padded_data = padder.update(data) + padder.finalize()
    ciphertext = encryptor.update(padded_data) + encryptor.finalize()

    # Return the IV and ciphertext
    return iv + ciphertext

# Example decryption algorithm
def decrypt_data(key, encrypted_data):
    # Extract the IV from the encrypted data
    iv = encrypted_data[:16]
    ciphertext = encrypted_data[16:]

    # Create a cipher using AES in CBC mode with the extracted IV
    cipher = Cipher(algorithms.AES(key), modes.CBC(iv), backend=default_backend())

    # Decrypt the data
    decryptor = cipher.decryptor()
    decrypted_data = decryptor.update(ciphertext) + decryptor.finalize()

    # Remove the padding
    unpadder = padding.PKCS7(128).unpadder()
    unpadded_data = unpadder.update(decrypted_data) + unpadder.finalize()

    # Return the decrypted data
    return unpadded_data

# End sample code

def authenticate_user(user):
    # Retrieve user credentials from a database or storage
    stored_user_credentials = retrieve_user_credentials(user)

    # Check if the user exists and retrieve the stored password
    if stored_user_credentials is None:
        return False

    stored_password = stored_user_credentials['password']

    # Compare the user-provided password with the stored password
    if verify_password(user.password, stored_password):
        return True

    return False

def multifactor_authentication(user, second_factor):
    # Validate the second factor
    if not validate_second_factor(user, second_factor):
        return False

    # Perform additional checks or verifications
    if not additional_checks(user):
        return False
return False

# Grant access if all factors are successfully verified
return True

def authorize_user(user, resource):
    # Retrieve user roles or permissions from a database or storage
    user_roles = retrieve_user_roles(user)
    user_permissions = retrieve_user_permissions(user)

    # Check that user has the necessary role for accessing the resource
    if role_authorization(user_roles, resource):
        return True

    # Check that user has the necessary permission for accessing the resource
    if permission_authorization(user_permissions, resource):
        return True

    return False

def apply_access_controls(user, resource, network_fprint, encryption_key):
    # Encrypt the network fingerprint
    encrypted_network_fprint = encrypt_data(encryption_key, network_fprint)

    # Retrieve the access control policies for the resource
    access_control_policies = retrieve_access_control_policies(resource)

    # Evaluate the access control policies
    for policy in access_control_policies:
        # Check that user satisfies the policy's conditions
        if user_match(user, policy):
            # Check that encrypted network fingerprint matches the policy's expected encrypted network profile
            if encrypted_fingerprint_match(encrypted_network_fprint, policy):
                return True

    # If no matching policy is found, access is denied
    return False

def log_access(user, resource, network_fprint, encryption_key):
    # Encrypt the network fingerprint
encrypted_network_fprint = encrypt_data(encryption_key, network_fprint)

# Retrieve the current timestamp
timestamp = get_current_timestamp()

# Create a log entry with user, resource, timestamp, and encrypted network fingerprint
log_entry = {
    'user': user,
    'resource': resource,
    'timestamp': timestamp,
    'encrypted_network_fprint': encrypted_network_fprint
}

# Save the log entry to a log storage or database
save_log_entry(log_entry)
References


[29] Zhang, Yagang, and Ruixuan Li. "Short term wind energy prediction model based on data decomposition and optimized LSSVM." Sustainable Energy Technologies and Assessments 52 (2022): 102025.


[36] Scott Rose Oliver Borchert Stu Mitchell Sean Connelly https://doi.org ...,


[41] “AES with CBC mode example,” libica: AES with CBC mode example, 

[42] T. O. Hodson, “Root-mean-square error (RMSE) or mean absolute error (mae): When to use them or not,” Geoscientific Model Development, 