IMPACT OF V2G/G2V ON VOLTAGE STABILITY IN DISTRIBUTION NETWORKS AND CYBER SECURITY IN THE SMART GRID

A Dissertation submitted in fulfillment of the requirements for the Degree of

MASTER OF ENGINEERING

in

Power Systems

Submitted by

Naman
Regd. No. 802242003

Under the Guidance of

Dr. Pratim Kundu
Assistant Professor
School of Computer and Electrical Engg.
IIT Mandi, H.P., India

Dr. Rajesh M. Pindoriya
Assistant Professor
Dept. Electrical and Instrumentation Engg.
TIET, Patiala, Punjab, India

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

2024

Department of Electrical and Instrumentation Engineering
Thapar Institute of Engineering & Technology, Patiala
(Declared as Deemed-to-be-University u/s 3 of the UGC Act., 1956)
Post Bag No. 32, Patiala – 147004
Punjab (India)

DECLARATION

I hereby certify that the work which is presented in a dissertation entitled, "Impact of V2G/G2V on Voltage Stability in Distribution Networks and Cyber Security in the Smart Grid", in partial fulfillment of the requirements for the award of the degree of Master of Engineering in Power Systems, submitted to the Department of Electrical & Instrumentation Engineering of Thapar Institute of Engineering & Technology (Deemed to be University) is as an authentic record of my own work carried under the supervision of Dr. Rajesh M. Pindoriya from TIET, Patiala and Dr. Pratim Kundu from IIT Mandi. It refers to other researcher's work duly listed in the reference section. The matter contained in this dissertation has not been submitted, neither in part nor in full to any other degree to any other university or institute except as reported in text and references.

Place: Patiala **Naman**

Date: 03-08-2024 **Roll No.: 802242003**

It is certified that the above statement made by the student is correct to the best of my knowledge and belief.

Dr. Pratim Kundu
Assistant Professor
School of Computer and Electrical Engg.
IIT Mandi, H.P., India

Dr. Rajesh M. Pindoriya
Assistant Professor
Dept. Electrical and Instrumentation Engg.
TIET, Patiala, Punjab, India

EXPERIENCE CERTIFICATE

Indian Institute of Technology Mandi
Mandi-175001, Himachal Pradesh, India

भारतीय प्रौद्योगिकी संस्थान मण्डी
मण्डी–175001, हिमाचल प्रदेश, भारत

TO WHOM IT MAY CONCERN

This is to certify that Mr. Naman s/o Mr. Pushap Raj, student of M.E. (Power System) bearing Roll No. 802242003 from Thapar Institute of Engineering and Technology, Patiala, Punjab has done a 1-year internship starting 14th June, 2023 till 14th June, 2024 at Indian Institute of Technology Mandi, Himachal Pradesh.

During the M. Tech project, he has shown rapid improvements in his ability to grasp a research problem and perform adequate literature survey. His curiosity and eagerness to look for research gaps is one of the major strengths and my assessment is that he is a sincere student.

Thank You

Dr. Pratim Kundu
Assistant Professor
School of Computing and Electrical Engineering
Indian Institute of Technology Mandi, India
Email: pratim@iitmandi.ac.in
Ph. No.: +91-1905-267111

Date: 14-06-2024

ACKNOWLEDGEMENT

I am delighted that my parents have been supportive throughout my educational career and my whole life. Without them, I would not have been able to reach the stage where I am standing today. I acknowledge them here by presenting a small piece of thanks. My mom and dad have a special place in my heart.

I wish to express my deep gratitude and appreciation to Dr. Rajesh M. Pindoriya, Department of Electrical and Instrumentation Engineering, TIET, Patiala, Prof. Bharat Singh Rajpurohit, Department of Electrical Engineering, IIT Jodhpur, and Dr. Pratim Kundu, School of Computing and Electrical Engineering, IIT Mandi, supervisors, for his valuable guidance throughout the research work. Without my supervisor's help, support, and constant encouragement, it would have been impossible for me to bring out this work. My cooperation with him has been remarkable and fruitful.

Dr. Rajesh Pindoriya has been an exceptional guide, consistently paving the way for an outstanding thesis. During my time at IIT Mandi, he proactively reached out to address any challenges I faced in my research. His support extended beyond academic issues to personal and official problems, always offering unwavering assistance. Every meeting in his office was encouraging and insightful. Dr. Pindoriya generously shared his knowledge, aiding me in writing an IEEE paper. I am deeply grateful for his belief in me and for the motivation he provided, which has been instrumental in advancing my research and completing this thesis.

I would also like to mention sincere gratitude to Dr. Sunil Kumar Singla, Head, DEIE and Dr. Nitin Naran, Associate Professor and PG Coordinator, DEIE, TIET, for allowing me to enhance my knowledge, gaining exposure to the IIT education system and coming up with innovative ideas.

Last but not least, I would like to express my deepest gratitude to my beloved parents, brothers, sisters, and family members for their continuous support and unconditional love. Truthfully, they have made many sacrifices to bring me to this stage, allowing me to pursue my studies at TIET Patiala and IIT Mandi, and enjoy a joyful and memorable academic life.

ABSTRACT

The integration of Vehicle-to-Grid (V2G) and Grid-to-Vehicle (G2V) technologies within distribution networks presents both opportunities and challenges for modern power systems. This thesis explores the impact of V2G/G2V on voltage stability and cyber security in the smart grid, aiming to enhance the resilience and reliability of electrical distribution networks.

The first part of the research focuses on voltage stability. The bidirectional power flow introduced by V2G/G2V can cause significant voltage fluctuations and instability in distribution networks. By modeling different scenarios, including varying penetration levels of Electric Vehicles (EVs), the study analyzes how V2G/G2V interactions influence voltage profiles and stability margins. Advanced control strategies and optimization algorithms are proposed to mitigate adverse effects and ensure stable operation under diverse conditions.

The second part of the thesis addresses cyber security challenges associated with the smart grid. The increasing connectivity and digitalization required for V2G/G2V operations expose the grid to potential cyber threats. This research identifies key vulnerabilities in the communication infrastructure and proposes robust security measures to safeguard against cyber-attacks. Simulation studies demonstrate the effectiveness of these measures in protecting the grid while maintaining efficient V2G/G2V functionality.

Overall, this thesis provides comprehensive insights into the dual aspects of voltage stability and cyber security in the context of V2G/G2V integration. The findings highlight the critical need for coordinated control and enhanced security protocols to harness the full potential of these technologies, ensuring a stable and secure smart grid.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

V2G	Vehicle to Grid
G2V	Grid to Vehicle
EV	Electric Vehicle
EVC	Electric Vehicle Charging
SOC	State of Charge
CSO	Charging Station Operator
CSS	Charging Station System
DGs	Distributed Generations
DGRs	Distributed Generations of Resources
BESS	Battery Energy Storage System
FR	Frequency Regulation
SG	Smart Grid
PG	Power Grid
TSO	Transmission System Operator
PWM	Pulse Width Modulation
ICL	Inner Current Loop
OVL	Outer Voltage Loop
SG	Smart Grid

CS	Cyber Security
AMI	Advanced Metering Infrastructure
SM	Smart Meter
MM	Manual Meter
IOT	Internet of Things
DERs	Distributed Energy Resources
CP	Communication Protocol
CIP	Critical Infrastructure Protection
SCPs	Secure Communication Protocols
DGRs	Distributed Generation of Resources
BT	Blockchain Technology
DOS- ATTACKS	Denial–of–Service Attacks
DMAs	Data Manipulation Attacks
LAN	Local Area Network
LFC	Load Frequency Controller
HAN	Home Area Network
WAN	Wide Area Network

CHAPTER 1
INTRODUCTION

1.1 Literature Survey

This study describes an optimized bidirectional Vehicle-to-Grid (V2G) operation that uses an Electric Vehicles (EVs) fleet connected to a distributed power grid [1]. EVs are more eco-friendly. Petroleum-dominated transport accounts for 25% of global energy consumption and 26% of energy-related CO_2 emissions [2]. According to China National Petroleum Corporation's "Energy Outlook 2050," transportation energy consumption will grow 23% in 2050 compared to 2015. As a result, a more efficient and clean transportation system is required to reduce fuel use and carbon emissions. EVs use electricity directly for mobility, resulting in lower emissions due to the high efficiency of energy conversion and use of renewable energy. Thus, replacing internal combustion engine vehicles with EVs may be a practical method for contributing to a low-carbon, sustainable society [3]. The block diagram of a V2G is shown in Fig. 1.1 (a). The major components of the G2V are the transformer, power converter, charging station, and control and monitoring unit.

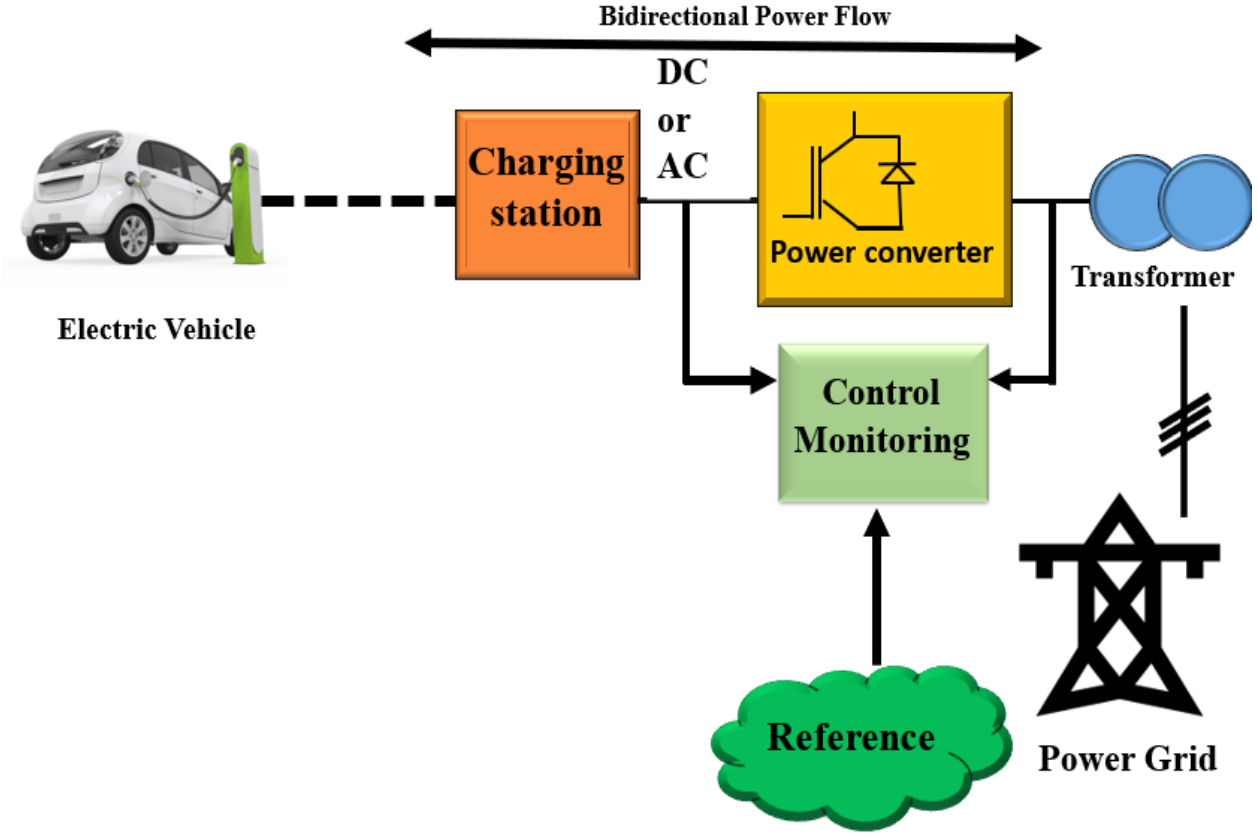

Fig. 1.1 (a). Block diagram of V2G model.

This is shown in Fig. 1.1 (b). The major components of the G2V are the transformer, power converter, charging station, control, electric vehicle, and monitoring unit.

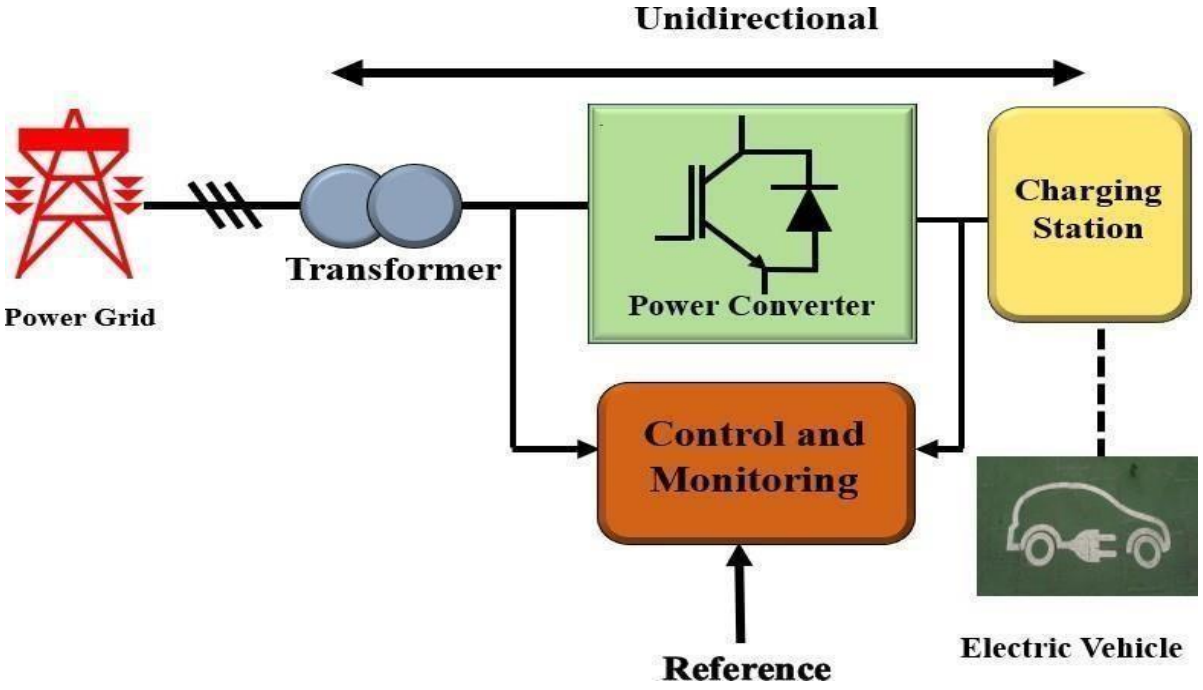

Fig. 1.1 (b). Block diagram of G2V model.

Diagram 1.1 (b). illustrates how power moves through electric cars, specifically the chargingsystem. Let's break down each component one by one.

- **Power Grid:** The power grid is the foundation of any electrical energy system since it provides the system with electricity.
- **Transformer:** Power converters can benefit from the step-up and step-down processes. The system's subsequent stage receives the desired voltage level.
- **Power converters:** Their fundamental function is to convert AC energy into DC, which is compatible with EV batteries and guarantees that the energy is perfectly stored in the batteries.
- **Charging station:** An electric car can receive DC electricity from a charging station, which connects it to the charging infrastructure.
- **Electric Vehicle:** The vehicle's electric motor is powered by energy stored in the battery, which is sourced from the charging station.
- **Control and Monitoring:** By controlling every step of the charging process, it keeps an eye on the power flow in a way that is efficient, safe, and controlled. The system

performs and is more stable now.

- **Reference:** It displays different current and voltage levels as well as the length of time needed to charge. It guarantees that the system is operating correctly.
- **Unidirectional flow:** This denotes that power only travels in one way, such as from an electric vehicle to the power grid. In this case, bidirectional flow is prohibited and it is regarded as the standard setting for EV charging systems.

1.2 Circuit Topology of V2G/G2V Operation

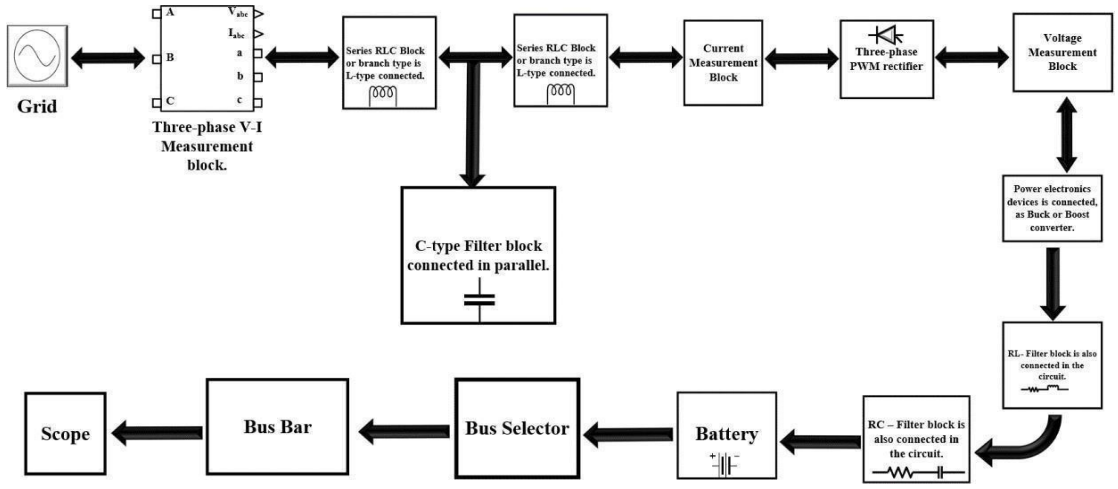

Fig. 1.2. Block diagram of V2G/G2V circuit topology operation.

Fig. 1.4. shows a power system including grid integration, measuring blocks, filters, power electronics, and a battery storage system is depicted in this block diagram. Below is a detailed breakdown of each component:

- **Grid:** This is where the three-phase AC power comes from.
- **Three-phase V-I Measurement Block:** This block measures the grid's three-phase AC power's voltage and current. Composed of series resistor (R), inductor (L), and capacitor (C) components, the series RLC block is an L-type linked circuit. The powersignal's high-frequency components are filtered and dampened by this block.
- **Current Measurement Block:** This component gauges the system's current flow.
- **Three-phase PWM Rectifier:** This device uses the Pulse Width Modulation (PWM) method to convert three-phase AC power into DC power. Usually, this rectifier is utilized to enhance power quality and regulate the output voltage.
- After rectification, the voltage is measured by the voltage measurement block.
- **Power Electronics Devices (Boost/Buck Converter):** These devices either step up or step down the DC voltage to regulate it.

- **RL Filter Block:** A filter to smooth out the DC voltage that is made up of resistors (R) and inductors (L).
- **RC Filter Block:** An additional filter to further smooth the voltage, made up of resistors (R) and capacitors (C).
- **Battery:** Holds the controlled DC power in reserve for potential use or backup power.
- **Bus Selector:** Chooses the right bus so that power is distributed to various system components.
- **Bus Bar:** A standard connector used to deliver electricity across multiple components.
- **Scope:** Used to track and examine the system's voltage and current waveforms.
- **C-type Filter Block:** A parallel filter to eliminate particular harmonics or undesired frequency components from the power stream is a C-type filter block (connected in parallel).
- Starting with the grid, power, and signal measurement moving through measurement and filtering blocks, rectification, voltage regulation, and battery storage. Additionally, the system has parts for keeping an eye on and guaranteeing power quality all along the way.

1.3 EV's Charging and Discharging

The system plans EV charging and discharging for the following day to lower EV ownership charging costs and provide frequency and voltage regulation services. To provide voltage and frequency regulation, the suggested system responds to real-time data on EV utilization and optimizes EV use. According to the results, the system may support frequency and voltage while EV charging costs are reduced [4]. Using a fleet of electric vehicles (EVs), the study proposes an optimized bidirectional Vehicle-to-Grid (V2G) operation that reduces EV ownership charging costs and aids in frequency regulation. Frequency regulation is maintainingan electrical power system's frequency at its specified level. Deviations in frequency from the nominal frequency can damage machinery and reduce the efficiency of power systems [1, 5].

While V2G/G2V technologies can also be employed, frequency regulation is often handled by power plants. In contrast to G2V EVs, which can charge their batteries from the grid, V2G EVscan discharge their batteries to the grid. By discharging EVs during high frequency and charging them during low frequency, this two-way energy flow may alter frequency. Amultitude of V2G/G2V control approaches are available for frequency adjustment. Each EV isfree to make its own decisions thanks to decentralized control systems [6]. The "when" and "where" of vehicle charging is a persistent worry for electric vehicle owners. Finding the "appropriate" Charging Station (CS) is

therefore essential. Numerous researchers have offereda variety of solutions to address this issue. However, the majority of them believed that the only factor in choosing the right CS for matching was the distance vehicle [7].

1.4 Charging Station Operators

Nonetheless, the most important factor to take into account while choosing a suitable CS is the presence of open charging slots in CS. Therefore, to assist in selecting the proper CS, this factoris covered in this article along with others like the shortest distance and reduced battery energyusage. The second significant issue is the charging schedule, which comes after assigning pertinent CS to the appropriate vehicles. Additionally, managing EV charging effectively is always very challenging. A lot of writers are focusing on the G2V mode's EV charging method.How the extra energy from EVs might be utilized to enhance the grid and bring in a new era ofintelligent electric cars is another significant issue [8].

Developing a new realistic pricing strategy that considers the requirements of numerous stakeholders is one of this paper's most important contributions. To address the specialcharging method, the study builds several EV charging models that rely on charging schedulespushed by EV owner behavior to assess the charging impact of EVs. The new charging strategy classifies distribution corporations and charging station operators (CSOs) as distinct enterprises. Distribution operators have little issue handling EV data, and CSOs for electric vehicles are aware of the locations of all the different EVs inside the power system. The novelapproach takes into account a typical battery and blends stochastic algorithms with a maximized extensive index to model the traveling behavior of large-scale EVS over extended periods. The transformer, power converter, charging station, control, electric vehicle, and monitoring unit are the main parts of the G2V and V2G.

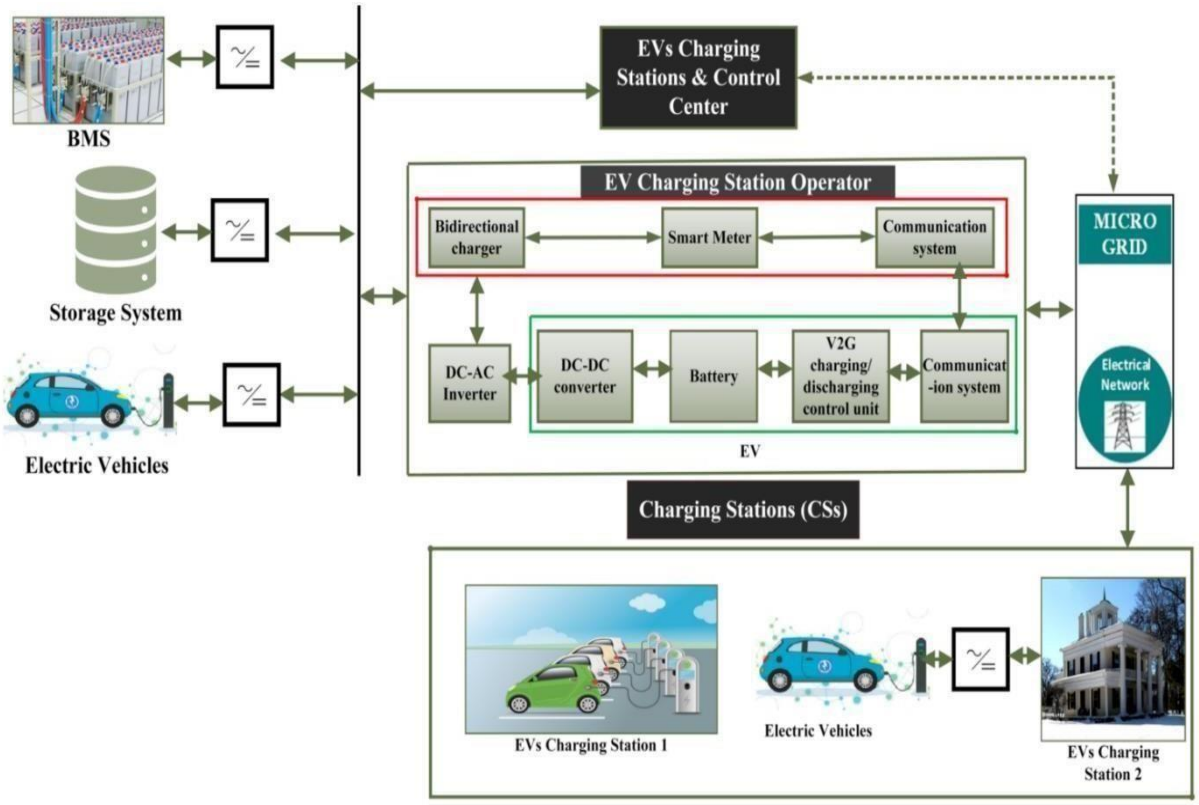

Fig. 1.4. An overview of a V2G charging station linked to the grid.

1.5 V2G/G2V Control Schemes: Benefits and Drawbacks for Frequency Regulation

There are a few benefits and drawbacks to various V2G/G2V frequency regulation control methods.

Benefits:

- **Better frequency control:** V2G/G2V may offer quick and adaptable frequency regulation services, which can support the grid's stability.
- **Enhanced integration of renewable energy:** By enabling the storage and discharge of excess energy when required, V2G/G2V can facilitate the integration of renewable energy sources into the grid.
- **Decreased reliance on fossil fuels:** V2G/G2V can contribute to a reduction in the use of fossil fuels for power generation by offering a sustainable and clean alternative.
- **Economic benefits:** By selling electricity back to the grid, EV owners can benefit from V2G/G2V.

Drawbacks:

Increased battery deterioration: V2G and G2V can shorten the life of EV batteries by hastening this process.

Communication problems: The grid controller and EV batteries must have a stable communication system for V2G/G2V to function.

Cybersecurity risks: Cyberattacks could disrupt power grid operations by targeting V2G/G2V equipment.

Cost: The installation and upkeep of V2G/G2V hardware and software can be expensive.

The charger or discharger needs to be set to a positive power setting to charge the EV battery from the grid. To guarantee that the battery is charged safely and effectively, the charger/discharger is managed by the grid's voltage and frequency. While the EV battery is being discharged to the grid, the charger/discharger is set to a negative power setting. To guarantee that the battery is discharged safely and effectively, the charger/discharger is managed by the grid's voltage and frequency. One of the services for frequency regulation is the charger/discharger, which is designed to control the frequency of the grid. To maintain a steady grid frequency, the battery is charged or discharged as necessary [9].

CHAPTER 2
PROBLEM FORMULATION AND CONTROL TOPOLOGY

2.1 V2G AND G2V SYSTEMS

The growing interest in G2V and V2G technology is a result of the expansion of renewable energy sources, like wind and solar power. While G2V enables EVs to charge their batteries from the grid, V2G allows EVs to discharge their batteries back to the grid. By utilizing this two-way energy flow, frequency regulation services, integration of renewable energy sources into the grid, and removal of the need for fossil fuel power plants can all be achieved. Developing and implementing control systems to optimize EV charging and discharging to meet grid and EV owner needs is one of the issues with V2G/G2V operation. Making durable, affordable, and user-friendly V2G/G2V hardware and software is another challenge. Fig. 2.1 displays the control block diagram that is utilized in both front-end bi-directional buck-boost converters. The bi-directional buck-boost converter's control block diagram manages the power transfer between the input source (such as the grid or battery) and the output load. Several feedback loops that cooperate to maintain a steady output voltage and current while guaranteeing the converter operates efficiently make up the control block diagram in most cases.

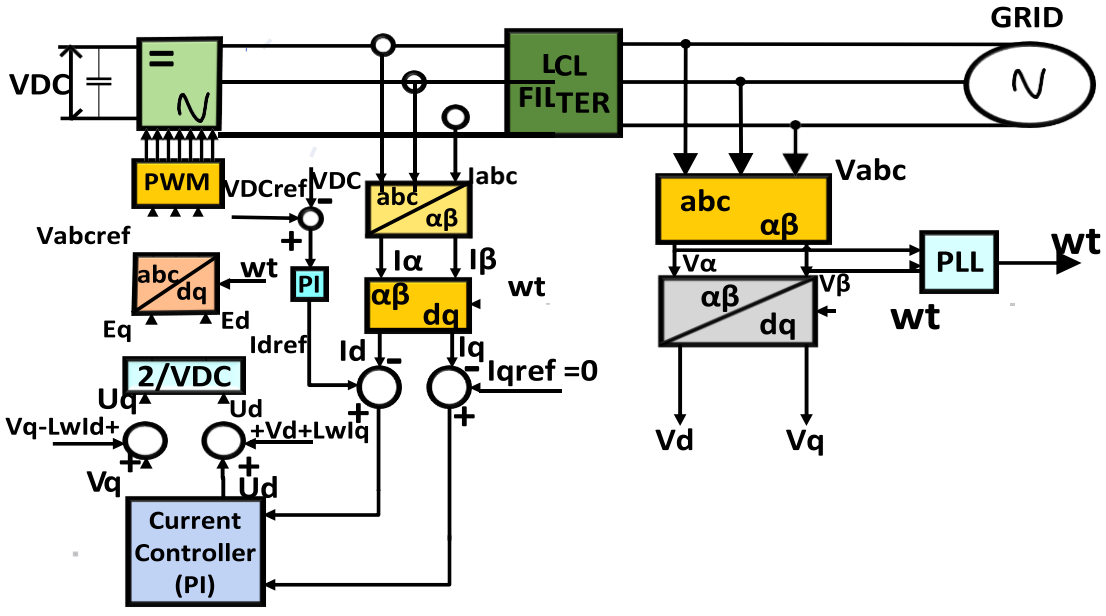

Fig. 2.1. Control block diagram used in both the front-end bi-directional buck-boost converter.

2.2 Equivalent Circuit Diagram Topology

Fig. 2.2. illustrates battery charging from and discharging to the grid (V2G and G2V operation).For V2G and G2V activities, a bidirectional buck-boost converter is a common circuit layout. This dynamic converter design makes it simple to transition between V2G and G2V modes andpermits both battery draining and charging. The bi-directional buck-boost converter is suitablefor a range of applications since it can adjust the voltage between the grid and the battery. In G2V mode, the converter lowers the battery voltage to equal the grid voltage by acting as abuck converter. The battery's power is released into the grid.

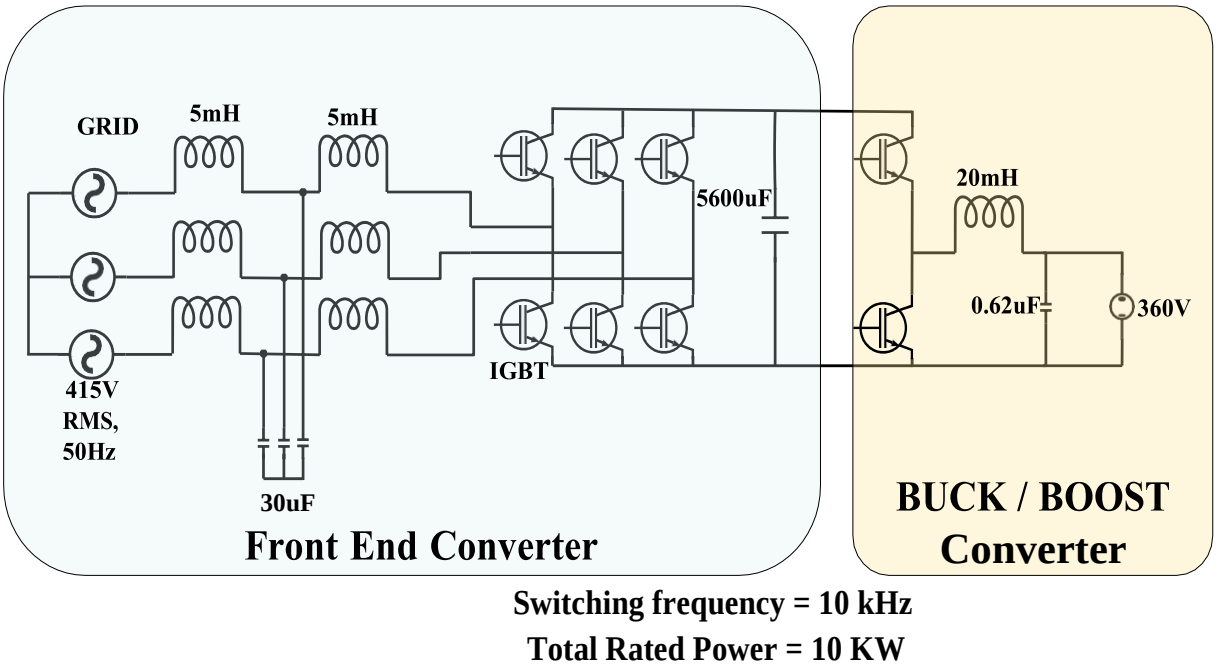

Fig. 2.2. Battery charging from the grid and discharging to the grid (V2G and G2V operation).

Fig. 2.2 illustrates the bi-directional buck-boost converter's battery charging and discharging. The control block diagram of a bidirectional buck-boost converter is essential for controlling the flow of power between the output load and the input source (grid or battery). Often, this design consists of many feedback loops that cooperate to ensure efficient operation and maintain a constant output voltage and current. Power flow control is greatly influenced by theduty cycle of the converter's switching components. More power is transmitted from the input source to the output load when the duty cycle is higher; less power is transferred when the dutycycle is lower.

2.3 EV Associated Terms

Inner Current Loop (ICL): The inner current loop maintains a proportionality between the reference current and the output current. To compare the actual output current to the reference current, a Current Error Amplifier (CEA) is utilized. An error signal proportionate to the current differential is produced by the CEA. The duty cycle of the switching components in theconverter is thus managed using this error signal.

Outer Voltage Loop (OVL): To guarantee that the output voltage is proportionate to the reference voltage, there is an outside voltage loop or OVL. To compare the actual output voltage to the reference value, a Voltage Error Amplifier (VEA) is utilized. An error signal corresponding to the voltage differential is produced by the VEA. Next, this error signal is used to regulate the duty cycle of the switching elements in the converter.

Modulation of Duty Cycle: One of the most important factors in managing power flow is the duty cycle of the converter's switching components. More power is transmitted from the input source to the output load when the duty cycle is higher; less power is transferred when the duty cycle is lower.

V2G/G2V Communication: When in V2G/G2V mode, the PI controller is set up to manage the output voltage and current to the appropriate levels. The direction of power flow is determined by the sign of the reference current. When the reference current is positive, electricity flows from the grid to the battery; conversely, when it is negative, electricity flows from the battery to the grid. The control block diagram then automatically modifies the duty cycle of the switching elements to maintain the required output voltage and current. The intended power transfer between the battery and the grid is therefore accomplished. To maintain stability and govern power flow, a complex control strategy is needed in both V2G and G2V modes. A mixture of voltage and current feedback loops is often used in the control approach to guarantee that the battery charges or drains at the appropriate rate.

CHAPTER 3
SIMULATION & RESULTS

The MATLAB/Simulink environment is used to implement the V2G and G2V systems. Figure 3.1. illustrates the system's operation in V2G mode (+30), using the system. Here, we are injecting power into the grid since the voltage and current are both in phase. The current is positive, and the waveforms for voltage and current are in phase. This indicates that the grid is receiving power from the system. We can therefore infer that the system in the graph is operating in V2G mode. Since it enables electric vehicles to contribute to the grid and help stabilize the power system, this is a desirable mode of operation. It's also critical to understand that sophisticated control systems are frequently used to oversee V2G activities. The safe and effective transfer of power between the grid and the batteries of an electric car is ensured by this control system.

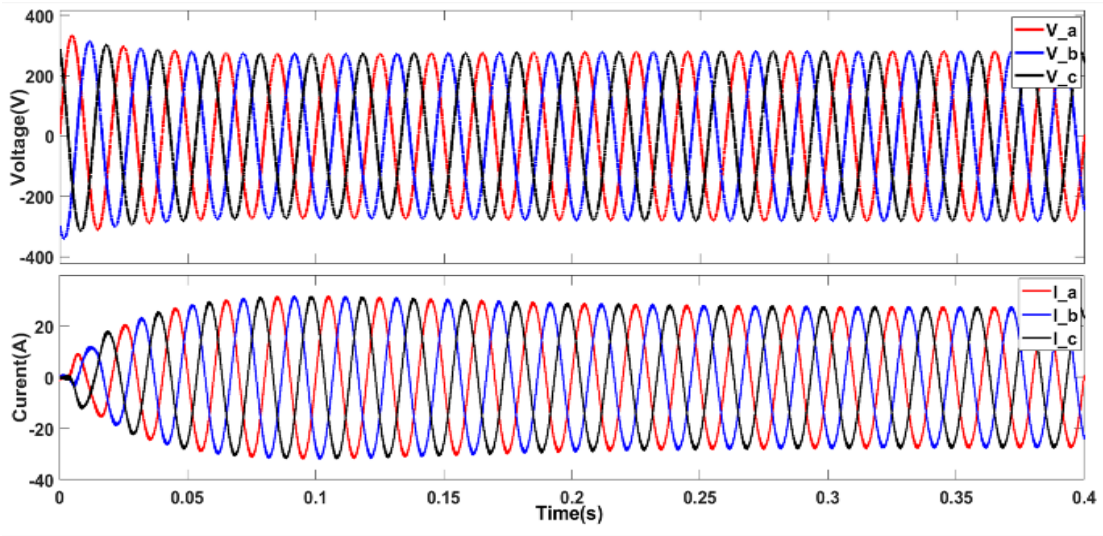

Fig. 3.1. Voltage and Current waveforms in V2G mode.

A graph depicting a battery's voltage, current, and state of charge (SOC) over time is shown inFig. 3.2. Time (s) is labeled on the x-axis of the graph, voltage (V) for the voltage line, current (A) for the current line, and SOC (%) for the charge line's state. The battery's state of charge (SOC) is shown by the red line on the graph. The SOC represents the portion of the battery's capacity that is still usable. The SOC on the graph begins at 100% and gradually drops as the battery drains. The current (A) passing through the battery is shown by the green line on the graph.

When the battery is charging, the current is negative, and when it is discharging, it is positive.The battery is depleted because the graph's current is positive. The voltage (V) of the battery isshown by the blue line on the graph. As a battery empties, its voltage drops. As the battery empties, the voltage on the graph drops from approximately 400 volts to approximately 300 volts.

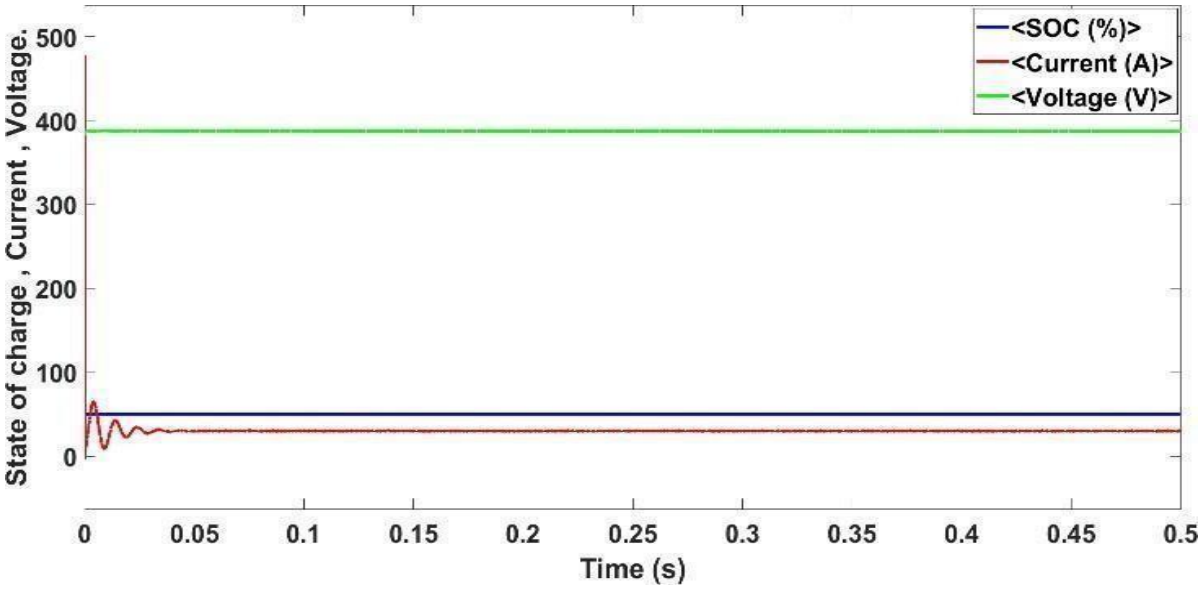

Fig. 3.2. SOC, Current, and Voltage waveforms in V2G mode.

Table .3. Simulation Components of V2G/G2V

Parameters	**Values**
Phase-to-phase voltage	415V
Current	30A
Rated power	10kW
Capacitance (F)	30μF
Buck filter inductance	20mH
Output Capacitance	0.625μF
Switching frequency of both converters (Buck/boost)	10kHz
Frequency	50Hz
Battery nominal voltage	360V
Battery rated capacity	300Ah
SOC (state-of-charge)	50%

The power curve of a device using the Vehicle-to-Grid (V2G) mode is displayed in Fig. 3.3. The term "V2G" describes a method that allows electric cars (EVs) to communicate with the electrical grid. The grid can either charge the EV battery or it can discharge energy back into the grid. This two-way power flow can lessen the system's dependency on peak power plants and aid in grid stabilization. On the y-axis of the graph in the picture is power (W), and on the x-axis is time (s). Positive and negative values can be seen fluctuating in the power curve, with positive values probably indicating power being provided to the device and negative values perhaps showing power being discharged from it. This is incompatible with V2G functioning, as during discharge the power transfer from the EV to the grid would normally be unidirectional. Based on the time scale, the graph most likely shows a device's power output over a brief interval of time (a fraction of a second). At a very high frequency, the power alternates between positive and negative values. This can mean that the gadget is alternating between the charging and draining phases quite quickly. This is incompatible with V2G functioning, as during discharge the power transfer from the EV to the grid would normally be unidirectional. Based on the time scale, the graph most likely shows a device's power output

over a brief interval of time (a fraction of a second). At a very high frequency, the power alternates between positive and negative values. This can mean that the gadget is alternating between the charging and draining phases quite quickly.

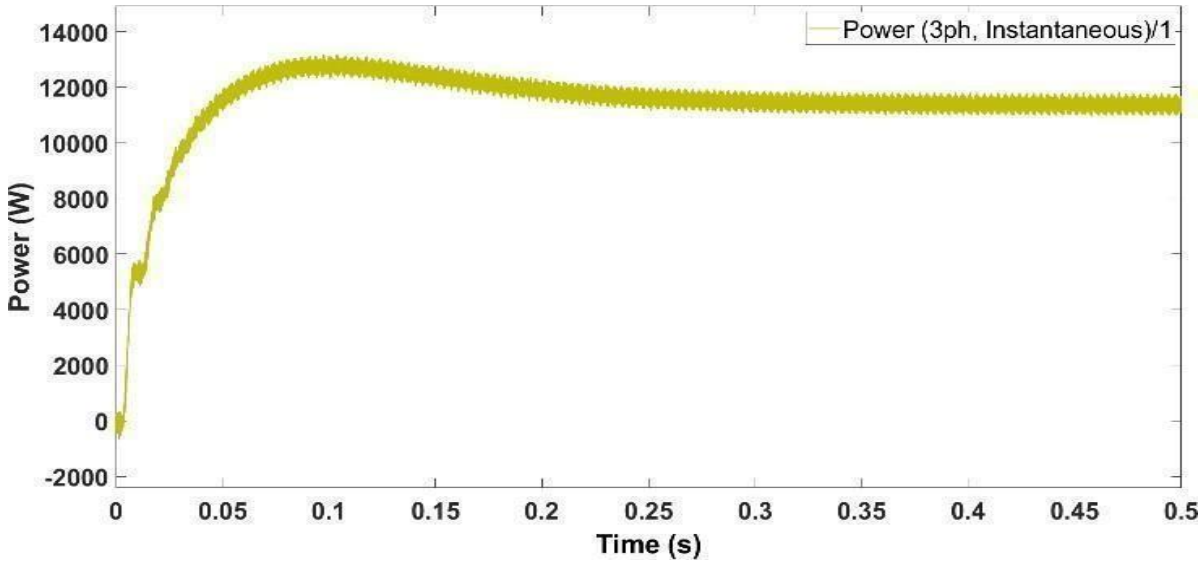

Fig. 3.3. Power and time waveform in V2G mode operation.

Instead of power, Fig. 3.4 displays a graph with a voltage-to-current curve. Electric current is shown on the y-axis with the label "Current (A)," while time is shown on the x-axis with the label "Time (s)." The y-axis does not provide a power (watt) indicator. Positive numbers likely indicate current entering the battery and negative values represent current leaving the battery. A graph of the current plotted over time is displayed in Figure 3.4. Considering the timescale on the x-axis, it seems to represent a little time (fraction of a second). The short vertical lines are probably spikes or bursts of electricity.

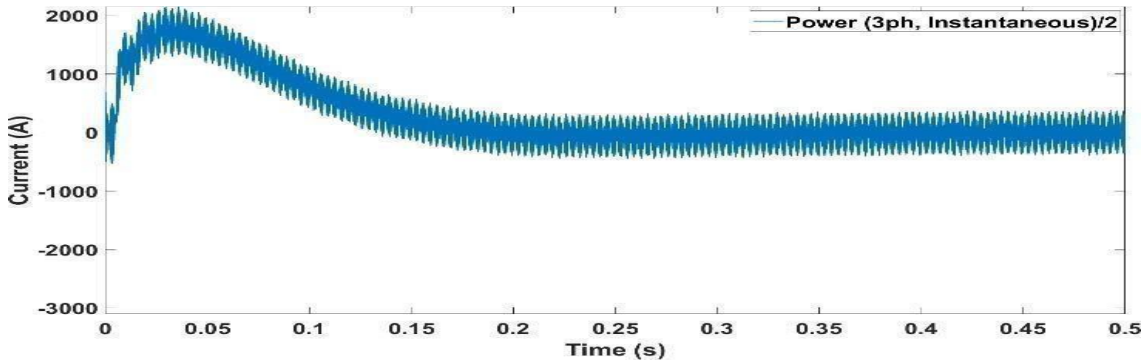

Fig. 3.4 Current and time waveforms in G2V mode operation.

CHAPTER 4
CYBER SECURITY IN SMART GRID

4.1 Brief Overview

In its ability to improve the efficiency of conventional power system grids, smart grid technology has the potential to completely transform today's businesses. Smart is a digital communication technology-based energy supply network [10]. As stated in "the increasing loadand consumption demand increase electricity complications," for instance, there is a higher demand, which leads to problems with overloads, voltage sags, and blackouts. It also makes the current electrical network more susceptible to cyberattacks [11]. The most crucial method insmart grid technology is online monitoring. The consumer and the smart grid communicate in both directions [12].

Many of electronic devices are connected via communication networks throughout major power plants, making cyber security a critical topic to be studied due to the growing complexityof the settings and the diffusion of the communication network [13]. This study identifies a thorough security assessment of the smart grid's architecture, potential attack scenarios, and strategies for detection and defense. To address the threat issues of the smart grid, a few difficulties and solution options are described [14].

Energy is injected into the structure and is essential to most human endeavors. The current conventional power system is overly reliant on fossil fuels. In recent years, governments and the technical community have begun to observe smart grids more and more. Going back to the beginning, the Electric Power Research Institute (EPRI), which is the form of "IntelliGrid," was the first to propose the idea of the smart grid in 2001. The US government formally beganbuilding the smart grid in 2003.

There may be some regional variations in the specific classifications of smart grids, such as "E-Energy" in Germany, "FREEDOM" in the USA, and "Digital Power Grid" in Japan. For online monitoring and control of the smart grid, there has been a significant improvement in the Advanced Metering Infrastructure (AMI), Information Communication Technologies (ICTs), Intelligent Demand-Side Management (IDSM) approaches flexibility, resilience, and

robustness [15]. With the aid of technological gadgets, the smart grid's complexity is rising. The many communication channel types utilized by the smart grid are depicted in Fig. 4.1. In termsof communication, the smart grid network is extremely intricate. The whole grid-like Local Area Network (LAN), Wide Area Network (WAN), and Home Area Network (HAN) wireless communications device connectivity must be made simpler. Because these gadgets are directly connected to the home, your system is intelligent [16]. The capacity to monitor and communicate online through these networks is related to online monitoring and communication. Things likevideo conferencing, security monitoring, and remote access may fall under this category.

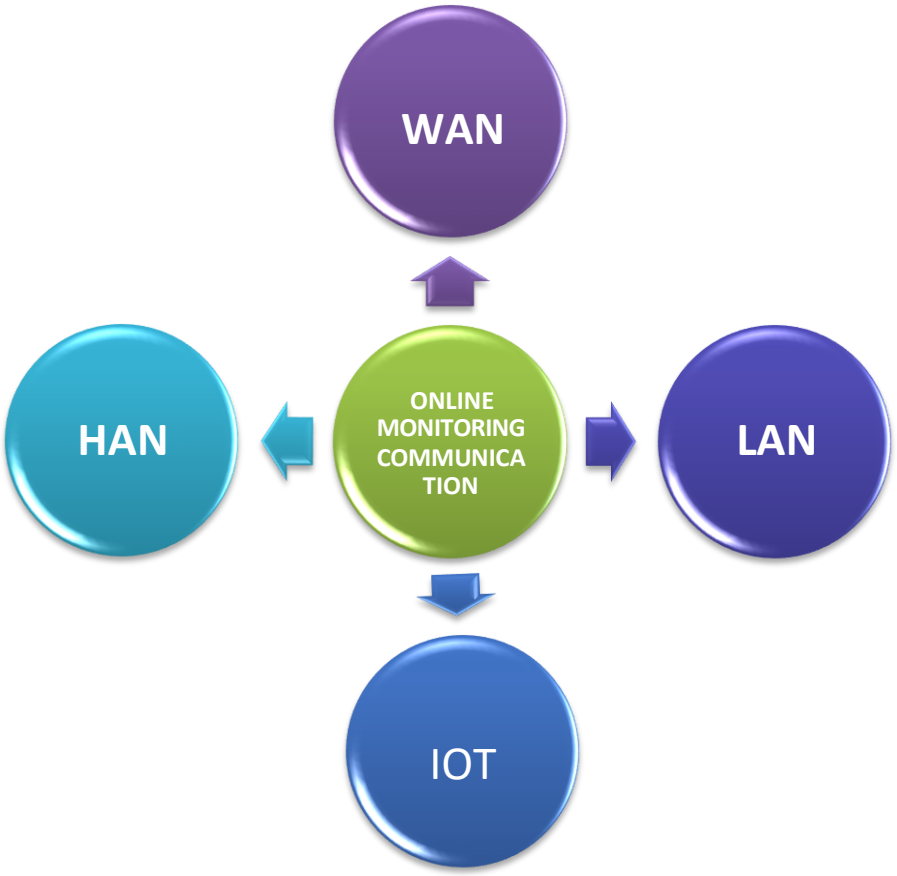

Fig. 4.1. Communication Infrastructure model.

4.2 Smart Meter & Its Characteristics

One extremely helpful piece of technology that can be added to the grid is the smart meter. It can offer comprehensive usage data to lower electricity costs and increase awareness of the state of the electrical system. Both the efficiency of smart meters and the level of customer care

they provide have increased. Electric vehicle charging stations, laptops, PCs, fans, and TVs areall directly connected to smart meters. An Internet of Things (IoT) gadget is a smart meter [17].With its ability to provide real-time data on electricity usage, support demand responseprograms, and enable efficient energy distribution, AMI is essential to the transformation of traditional power grids into smart grids. Improved grid reliability, higher customer engagement, and increased operational efficiency are just a few advantages it provides to utilities and consumers [18].

Features of smart meters: Energy usage is typically measured by smart meters. The abilityof smart meters to measure and store the total cumulative value was a very helpful feature. Among other things, smart meters are being substituted for regular meters thanks to smart grids.Customers are finding it simpler to enhance functionality and provide new services as a result.Additionally, the smart meter featured a telecommunications interface that allowed for remote reading and operation of the meter from the central systems. The ability to change the meter's setup and the parameters linked to contracts was a very helpful feature of smart meters [18].

Smart meters are essential for enabling the integration of renewable energy, and distributed energy resources (DER) are a valuable weapon in the fight against climate change. Numerous devices based on inverters and converters participate in distributed systems. Power electronics-enabled solar photovoltaic distribution systems and smart inverters. Implementing effective ways to track and manage those gadgets and DERs at the grid edge is crucial [19].

4.3 Cyber Security Importance In Smart Grid

Concerns regarding the software platforms and communication networks that govern and control the entire grid have been raised by the growing significance of cyber security in smart grid systems [20]. Because of the special characteristics of smart grid networks—such as theirvariety, scalability, time limits, bandwidth needs, and other factors—it is challenging to apply uniform security measures throughout the network. This study will examine the problems withcyber security that smart grid networks are now facing, go over some recent fixes, and offer a fresh idea for security that is based on the Internet of Things (IoT) [21].

Intelligent transportation, smart buildings, smart cities, connected healthcare, and—most importantly—the smart grid are just a few of the many uses for IoT [22]. The power line and

the communication line are the two main parts of the smart grid. One of the most important components in enabling connections within the system is the communication line [23]. Bidirectional smart devices, such as sensors, actuators, and smart meters, are part of a smart grid system that encompasses energy generation and consumer consumption. These gadgets make it possible to precisely balance energy in real time and to monitor it from any location atany time. The distribution and consumption of energy may be efficiently managed andoptimized thanks to the system [24].

As a result, the relationship between physical power systems and cyberspace implies that the main security issues are interconnected. It is clear that contemporary research has limitations. Information technology security tools and control implementations are distinguished from one another by the separation design. The main focus of this study will be an analysis of the security risks that smart grids confront from several angles. This research paper offers a succinct summary of the most recent studies done on smart grid security. This research paper's primarygoal is to identify the current state of the art, areas in need of more investigation, and future research directions for the development of intelligent, dependable, and efficient power systems.

The objective of this study is to present a succinct summary of pertinent studies on security concerns in smart grids, which comprises the following:

1. The concepts, strategies, and technologies of the security framework of smart grids are reviewed and analyzed in this study from the viewpoints of secure control theory and IT protection.
2. This survey offers difficult choices, especially for security precautions based on control-theoretic solutions.

CHAPTER 5
NETWORKING AND SMART GRID COMMUNICATION

5.1 Smart Grid Infrastructure

The smart grid presents an improved and novel perspective for the electrical infrastructure in this part. The bidirectional connectivity between the smart grid and its users is a key component. An essential factor in creating connectivity between the various parts of the smart grid is communication. However, the integration of network components from many vendors, each according to different standards, can make it difficult to construct a globally accepted network [26, 27]. Fig. 5.1 displays the LFC block diagram. It is necessary to have a full understanding of numerous communication factors to guarantee strong network connectivity. It is advised to validate the model using simulation tools prior to installing a network in real-time. This makes it possible to test several standards by varying important factors and determining the best course of action.

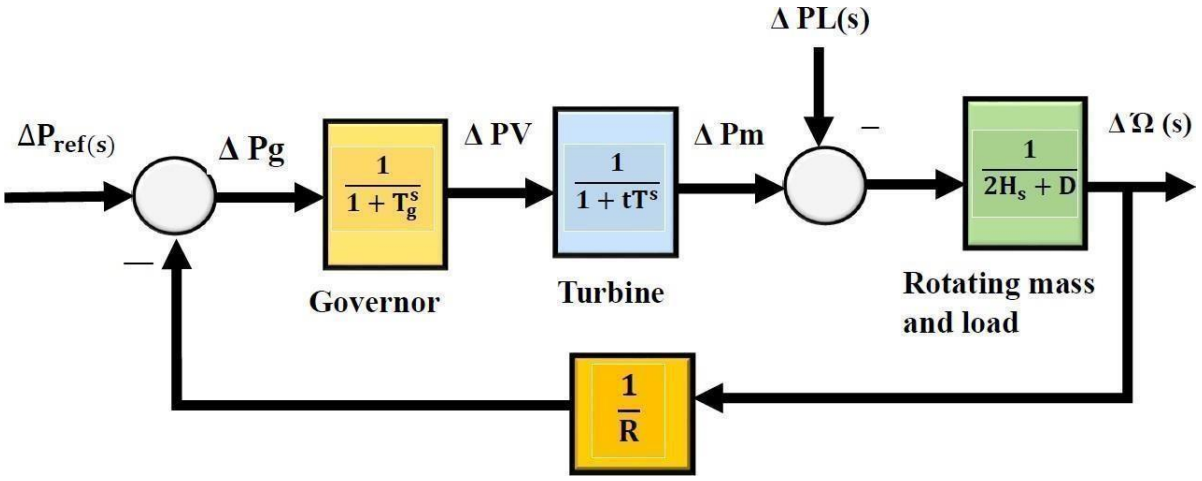

Fig. 5.1 Block Diagram of LFC.

Because of the many threats from both physical and cyber systems, Load Frequency Control (LFC), a typical depiction of the networked control framework in SGs, is selected, for the sake of simplicity and generality, to illustrate attack and defense techniques. In order to maintain tie-line power and the system nominal frequency, which is 60 Hz in North America and China,

LFC adjusts power generation references to generators in a power system in response to variations in load [28].

5.2 Components of LFC

The Load Frequency Control (LFC) model is a crucial element in smart grid cybersecurity as it guarantees that the equilibrium between power generation and consumption remains within reasonable bounds. Now let's examine the operation of the LFC model and its significance for cybersecurity:

Model for Load Frequency Control (LFC): Controlling the frequency and tie-line power flows in a multi-area power system is the main objective of the LFC model. To do this, it modifies the power output of generators in reaction to variations in generation capacity or load demand.

Parts: Typically, the LFC model consists of:

Control Area: Every control area is a geographical area that is connected by loads, tie-lines, and generators.

Controller: To preserve system stability, the LFC controller continuously tracks frequency variations and modifies the generators' power output.

Communication Infrastructure: Coordinated control actions and data sharing between control areas are made possible by real-time communication linkages.

Control Algorithm: Based on frequency deviations and tie-line power imbalances, the LFC controller uses control algorithms, such as proportional-integral-derivative (PID) controllers, to determine the necessary adjustments in generator setpoints.

The function of LFC in Cybersecurity: System Stability: By guaranteeing that power generationand load demand are met in real time, the LFC model is essential to preserving system stability.This equilibrium may be upset by cyberattacks directed at the LFC system, which could resultin voltage swings, frequency instability, and even blackouts.

Attack Resistant in LFC System: The LFC system must be resilient to cybersecurity measures to fend off risks including denial-of-service assaults, unauthorized access, and data manipulation. Preventing hostile interference necessitates the protection of communication lines, control algorithms, and control center infrastructure.

Detection and Reaction: You can detect unusual activity or attempted illegal access to the LFC system by putting intrusion detection systems and anomaly detection algorithms into place. Operators can quickly mitigate cyberattacks and restore system performance thanks to rapid reaction techniques.

Cooperation and Information Sharing: To exchange threat intelligence, best practices, and mitigation techniques pertaining to LFC cybersecurity, utilities, governmental organizations, and cybersecurity specialists must work together. Platforms for exchanging information make it easier to identify threats proactively and coordinate defenses against cyberattacks.

Note that a remote telemetry unit transmits measurement signals to the controller over the LFC system's networks. Consequently, one example of a networked control load frequency control in SGs is the LFC system. Hardware components can be used for deployment in systems (NCSs) where communication networks are used to close the control loop results [29–31]. Thepurpose of this study is to conduct a comprehensive review of the important IEEE and IEC standards related to networking and communication in smart grids. A thorough grasp of deliberate grid communication may be attained by looking at these standards, which will help in the creation of productive and successful networks [32].

5.3 Advanced Metering Infrastructure

The three tiers of the pyramid shown in Fig. 5.3. correspond to the various metering infrastructures: advanced, smart, and manual [33]. The pyramid shows how metering infrastructure is becoming more sophisticated, with each tier giving more sophisticated features and possible advantages. The manual meters at the bottom are examples of classic meters, which need meter readers to manually collect data. prone to delays in data access and human error. Their functionality and insights are restricted. The middle level is made up of smart

meters, which can collect data remotely since they have communication capabilities. Provide automated meter readings to increase accuracy and efficiency.

May be offers outage alerts and basic consumption information. The most advanced level, known as an Advanced Metering Infrastructure (AMI) with two-way communication and cutting-edge capabilities, is represented by top level. permits demand response programs, remote meter setting, and real-time data monitoring. offers thorough insights into grid performance and energy consumption trends. Depending on how it is implemented, each level may have different features and functionalities. AMI and smart meters are replacing manual meters due to cost and efficiency savings as well as the availability of smart grid technology. Individual demands and goals must be taken into account while selecting the appropriate metering infrastructure, which takes into account things like cost, data requirements, and desired functions.

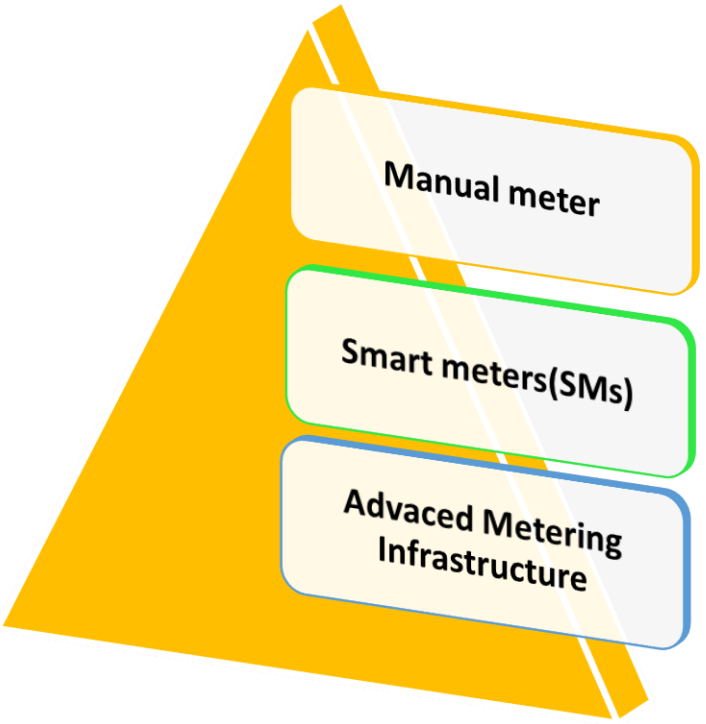

Fig. 5.3. Advancement technology evaluation in metering.

5.4 Basic Structure of Smart Grid

Fig. 5.4. (a) depicts the fundamental layout of the smart grid. It is a communication network for the smart grid that consists of various network segments, devices, and data flows. HAN establishes connections between smart appliances, thermostats, and meters inside a house or building. Usually, short-range wireless technologies like Z-Wave or Zigbee are used. A

Neighborhood region Network (NAN) links several HANs in a small geographic region, such as an apartment block or neighborhood. For greater coverage, mesh networking technologies are frequently used. To link NANs to central systems, a Wide Area Network (WAN) links a sizable geographic area, such as a city or region. Usually, fiber optic or cellular communication technologies are used. Depending on the particular implementation, many technologies and configurations may be employed in a smart grid communication network. To defend against cyberattacks, smart grid communication networks must prioritize security. To guarantee data privacy and interoperability in smart grids, standards and laws are being developed.

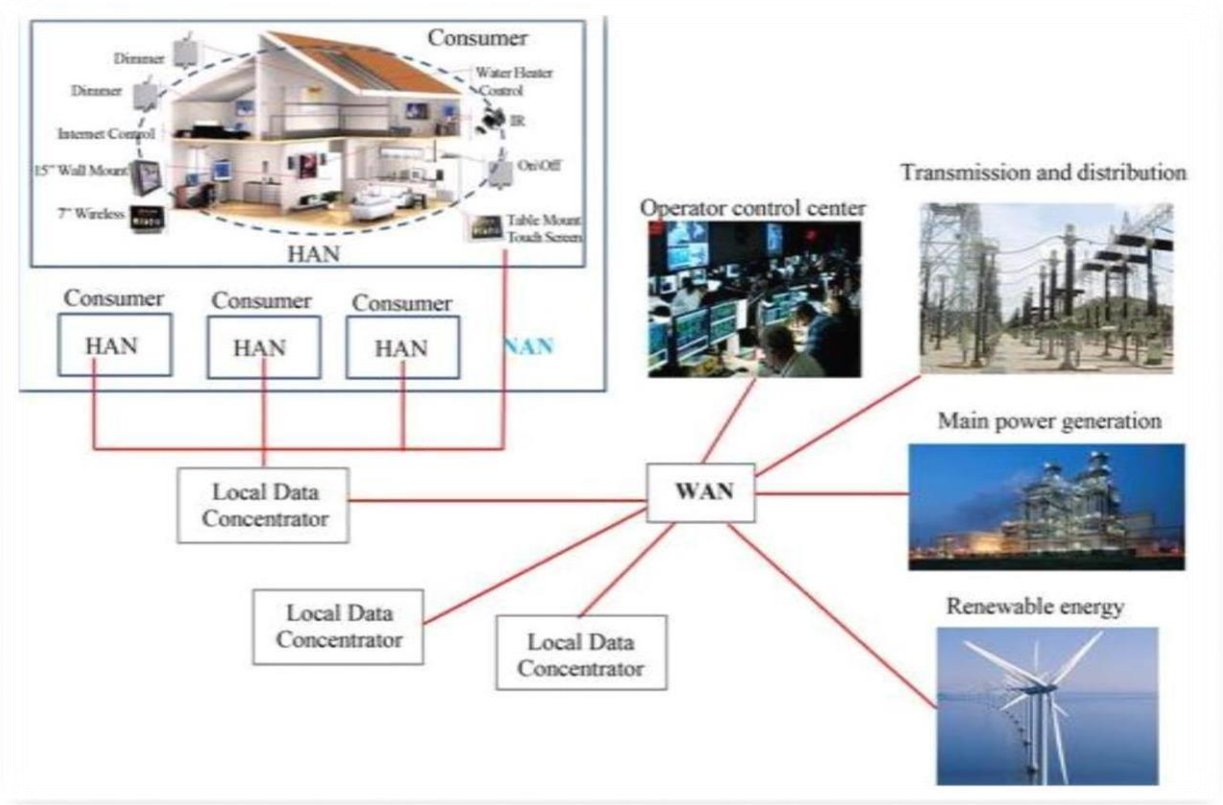

Fig. 5.4. (a). Basic structural model of the Smart Grid communication networking.

Fig. 5.4 (b). displays the block diagram of a smart grid's communication network architecture. Depending on the particular implementation, many technologies and configurations may be employed in a smart grid communication network. This picture shows one conceivable

arrangement, but there are others. To defend against cyberattacks, smart grid communication networks must prioritize security. Although security precautions are necessary for safe operation, they are not specifically depicted in the diagram. To guarantee data privacy and interoperability in smart grids, standards and laws are being developed. Although they are not depicted in the figure directly, these are crucial components of the design and operation of smart grid communication networks [34].

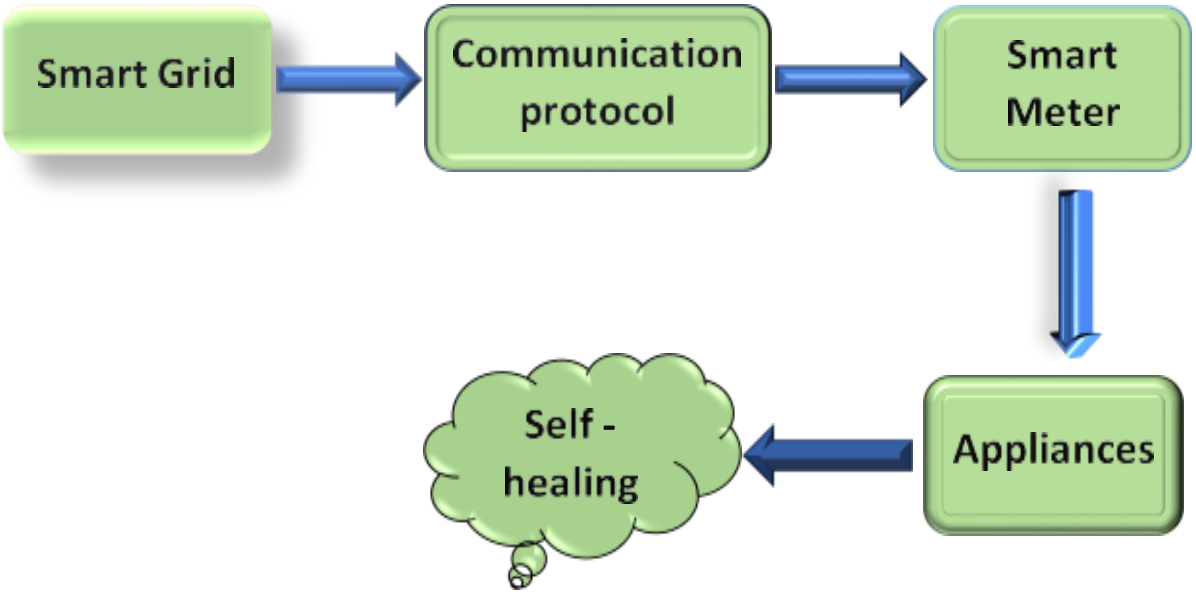

Fig. 5.4. (b). Block diagram of communication network system of smart grid.

CHAPTER 6

CYBER SECURITY ATTACK IN THE SMART GRID

6.1 Cyber Attacks

Smart grid cybersecurity attacks present serious hazards to vital infrastructure and can have far-reaching effects, such as power disruptions, monetary losses, and possible dangers to public safety. The following is a thorough summary of frequent cyber threats directed at smart grids and their possible effects:

Advanced Persistent Threats (APTs): Nation-states or highly skilled cybercriminal organizations are examples of well-funded, well-organized adversaries that launch long-term, complex cyberattacks. These attacks can go unnoticed for a long time inside a network and frequently include several phases. Attacks on intelligent power systems (APTs) have the potential to cause sensitive data theft, tampering with energy distribution procedures, and illegal access to control systems. They might also aid in sabotage or espionage operations, which could result in power outages and possible harm to physical infrastructure.

Zero-Day Exploits: These are software or hardware vulnerabilities that are not known to the vendor or the security community. By taking advantage of these flaws, attackers can access systems without authorization or run malicious programs. Because they can get past security protections and allow attackers to access networks that are vital to critical infrastructure, zero-day attacks can be especially harmful to smart grids. Taking use of zero-day vulnerabilities in control systems may cause extensive disruptions or allow for the manipulation of energy distribution procedures.

Phishing and social engineering: Phishing attacks use phone calls, emails, or other misleading communications to fool people into disclosing personal information or taking activities that put their security at risk. Social engineering techniques use psychological tricks on their victims to coerce them into doing things that will help the attacker. Phishing and social engineering attacks that are successful against employees of smart grid companies have the potential to introduce malware into the system, grant unauthorized users access to network credentials, and

leak confidential data. Additionally, hackers may utilize credentials they've obtained to elevate privileges and take over vital infrastructure components.

Ransomware: Malicious software known as "ransomware" encrypts data or systems and prevents access until a ransom is paid. Threats of data theft or irreversible data loss are frequently associated with ransomware attacks. Attacks using ransomware that target smart grids have the potential to interfere with energy distribution systems, resulting in service interruptions and power outages. Paying a ransom, restoring a system, and paying fines to the government can all be quite expensive. Furthermore, extended blackouts brought on by ransomware attacks may have a domino impact on other industries and towns that depend on a steady supply of electricity.

Supply Chain Attacks: To obtain unauthorized access to a target organization's network or systems, supply chain attacks target independent contractors, suppliers, or service providers. Attackers gain access to the target's infrastructure by taking advantage of weaknesses in the supply chain. Attackers may use compromised vendors or suppliers in the smart grid ecosystem as a springboard to target utilities or energy corporations. Attackers can inject malware, steal confidential information, or interfere with energy distribution processes by taking advantage of trusted connections and access privileges.

Denial-of-Service (DoS): DoS assaults overload target systems or networks with excessive requests or traffic, making them unusable or unresponsive to authorized users. Energy distribution services can be interfered with by denial-of-service (DoS) attacks on smart grid infrastructure, resulting in power outages and poor service. Attackers can impede operators from efficiently monitoring and controlling grid operations by flooding control systems or communication networks.

Insider Threats: These are malevolent or careless acts by those who have been granted permission to access smart grid systems, such as partners, contractors, or employees. Insider risks may lead to malware introduction, sabotage, data theft, or unauthorized access to vital infrastructure. Insiders with malicious intent may use their access privileges to disrupt energy distribution systems or steal confidential data for their benefit or espionage.

6.2 Malicious Attacks On the Smart Grid

Malicious attacks on the Smart Grid can have serious repercussions that affect both the general operation of our energy infrastructure and our daily lives. The impacts are broken down as follows:

1. **Power Outages:** Malicious assaults on the Smart Grid may result in widespread power outages that impact residences, places of business, and critical infrastructure. As a

result, there won't be any electricity to run appliances, heat, cool, or illuminate the room. It may also interfere with transit networks, making it more difficult for people to move about.

2. **Disrupted Communication:** Malevolent assaults have the potential to seriously impair the Smart Grid's communication networks. Thus, utility companies find it difficult to keep an eye on and maintain the system.
3. **Financial Losses:** Both the companies that supply the power and the customers who use it could suffer large financial losses as a result of malicious assaults on the smart grid. Companies may have times when they are unable to run on a regular basis, which will cause them to lose money.
4. **Health and Safety Risks:** Hospitals, emergency services, and public buildings are among the locations where safety is at stake when electrical systems malfunction as a result of these malevolent attacks. Emergency personnel may find it difficult to deliver prompt aid if medical equipment that depends on electricity malfunctions.
5. **Data Breach and Privacy Issues:** The Smart Grid is the target of cyberattacks. There's a chance that private data will be taken. Due to the potential for fraud or identity theft against both persons and organizations, this poses grave privacy problems. Imagine that personal information is obtained without authorization, maybe resulting in losses of money and other negative effects.
6. **Social Disruptions:** These attacks can cause power outages that last for a long time, which can seriously interfere with our daily lives. Businesses and schools might have to close, which would make it challenging for people to work, learn, or even communicate with one another. In the neighborhood, this situation may lead to stress and anxiety as people get agitated and worried about the prolonged power outage. Everyone concerned is going through a trying and stressful time, and it may lead to social unrest and unrest in the community.
7. **National Security Risk:** The Smart Grid may pose a serious risk to national security if it is the subject of widespread cyberattacks. This implies that it may have a major impact on the proper functioning of our nation. The effects might affect not just the energy industry but other vital sectors including defense, healthcare, and transportation.

Disregarding other important projects. Because funds and efforts that could have been utilized to create new technologies or upgrade infrastructure are now being directed toward repairing the damage caused by the assaults, this resource diversion may impede economic progress. Cybersecurity must become a primary priority for governments, energy companies, and individuals in order to prevent the dire repercussions of these attacks. This entails being

proactive in defending the Smart Grid against malevolent attacks. It is essential to invest in infrastructure that is resilient and able to repel attacks. By doing this, we can guarantee the security and stability of our energy infrastructure and shield our communities and ourselves from the possible destruction brought about by cyberattacks. To build a safer and more dependable energy future, everyone must be committed to a collaborative effort [35].

Figure 6.2. illustrates the cyber threat to a smart grid, including various attack paths, weaknesses, and possible effects. Phishing is the practice of sending emails or SMS messages that look to be from reliable sources, such as the energy company, in an attempt to deceive recipients into opening attachments or links that could be harmful. It targets a computer with a brain symbol and appears as an email icon with a fishhook. Viruses, worms, and ransomware are examples of harmful software that can be placed on devices with the intention of stealing data, interfering with normal operations, or taking control of systems. It is portrayed as a malware icon that targets several gadgets, including substation equipment, laptops, and smart meters. Zero-Day Attacks: These are attacks that take use of flaws in systems or software that the vendor is not yet aware of. They are symbolized by an emblem of a bomb aimed at a question-mark-equipped computer. Attacks known as denial-of-service (DoS): These flood systems with traffic, rendering them unusable for authorized users. A barrage of arrows aimed at the utilities data center is seen.

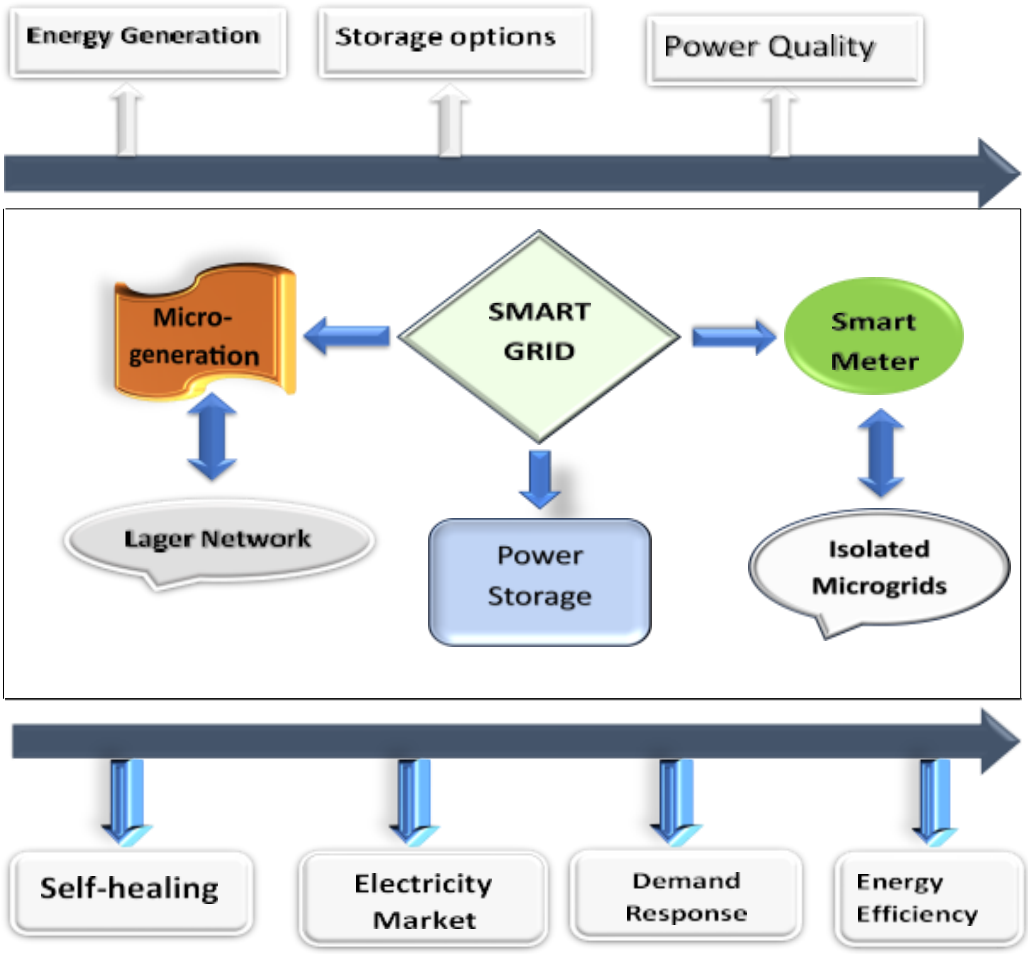

Fig. 6.2. Block Diagram of Smart Grid Utilities.

6.3 Smart Distribution Grid Objective

Enabling dependable and instantaneous information exchange across various entities inside the distribution grid is one of the main goals of the overlay communication network in the intelligent distribution grid architecture depicted in Figure 8.5 (b). In order for each microgrid to run smoothly and for the smart distribution grid to make choices on time, this objective is essential. However, the overlay communication infrastructure introduces instability in the communication links because of the spatial distribution and position dependency of the grid components.

The challenge is that handling the multiple requirements of data packets with changing Quality of Service (QoS) from different power grid entities would be too much for a single communication system to handle. To guarantee the overall stability of the communication architecture in the smart distribution grid, it is therefore best to use a combination of communication technologies [36].

ZigBee, Wi-Fi, Cellular, Wi-Max, Power Line Communication (PLC), and other technologies are among those being evaluated for integration [37, 38]. This heterogeneous communication architecture's adaptability to different communication technologies throughout the smart distribution grid is one of its advantages. The overall effectiveness and adaptability of the communication network are improved by allowing devices to communicate with one another despite their disparate technological backgrounds.

It is crucial to keep in mind that giving every device this variety of communication capability could make the communication network as a whole more expensive. A smart distribution grid's hybrid communication design offers a less costly solution to this issue. The heterogeneous communication feature in a hybrid architecture is only used in some places within the network of intelligent devices when a technology shift takes place. When needed, the hybrid architecture's strategic application of heterogeneous communication features lowers needless costs while preserving the advantages of various communication technologies in key smart distribution grid regions. This strategy balances communication effectiveness and cost efficiency, making it a workable and feasible option for smart grid infrastructure.

6.4 Smart Grid Diversity

The astute allocation grid must continue to function in all-weather circumstances. Dependence on a single communication method might not provide ongoing functionality in difficult situations. However, the chance of successful data delivery rises when a variety of methods are used. Multiple communication systems provide increased resilience and adaptation under challenging circumstances, improving the overall stability of the grid.

One way to drastically cut the overall cost of the communication network for a smart distribution grid is to integrate a heterogeneous communication feature only in those intelligent devices that need to make technological changes. Focusing on important areas where technology changes occur minimizes unnecessary expenses while keeping the benefits of seamless integration and efficient data transfer, as opposed to implementing different communication capabilities across all devices. This method maximizes the communication infrastructure's cost-effectiveness without sacrificing its functionality [36].

Fig. 6.4 [30] displays the smart grid's classification and general block diagram. The eight main components of the smart grid are: (1) energy management systems (EMS), (2) transmission systems, (3) substations, (4) distribution systems, (5) smart meters, (6) communications systems, and (7) customer involvement [39–40]. Smart meters are installed at customer locations to enable two-way communication between customers and the utility provider. In

addition to enabling demand response programs, smart meters offer real-time data on electricity usage. The infrastructure for communication between the various smart grid components is represented by a communication network. Throughout the system, it guarantees dependable data transport and control commands.

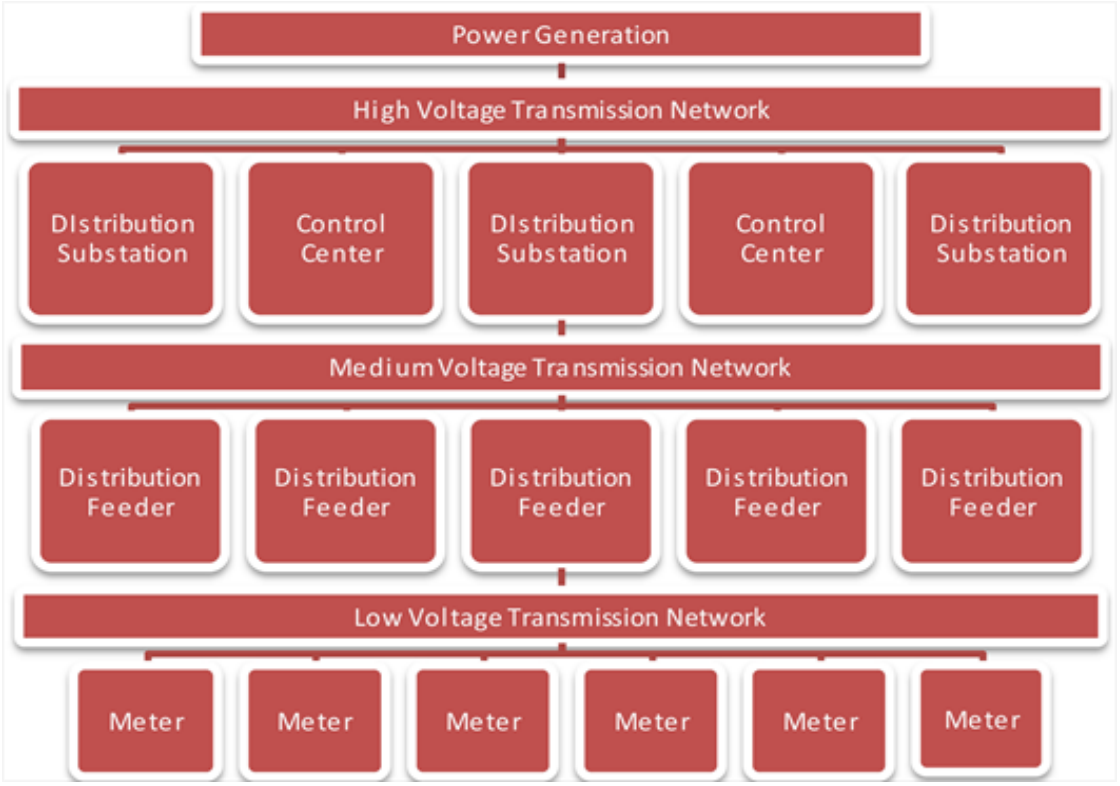

Fig. 6.4. Classifications and general block diagram of the smart grid.

CHAPTER 7

CHALLENGES AND SOLUTIONS IN SECURING SMART GRID

7.1 Challenges in Securing Smart Grid

Given the complexity and interconnectedness of energy distribution networks, cybersecurity in the context of the smart grid poses several difficulties. The following are some major issues and possible fixes:

Challenges:

1. **Interrelated Systems:** Sensors, communication networks, control systems, and consumer electronics are some of the interrelated parts that make up smart grids. The complexity of cybersecurity defenses and the attack surface are both increased by these systems' interdependence.
2. **Legacy Infrastructure:** SCADA systems and older equipment are only two examples of smart grid components that were not created with cybersecurity in mind at the outset. Cost and compatibility concerns make retrofitting legacy infrastructure to new security standards difficult.
3. **Diverse Threat Landscape:** Supply chain attacks, ransomware, malware, and insider threats are just a few of the many cyber threats that smart grids must contend with. Vulnerabilities in hardware, software, or human factors can be used by adversaries to compromise systems or pilfer confidential data.
4. **Resource Restrictions:** Energy utilities and operators frequently deal with resource restrictions, such as a lack of funds, staff, and cybersecurity-specific knowledge. Maintaining operational efficiency while allocating adequate resources to cybersecurity activities is a major challenge.
5. **Regulatory Compliance:** Complying with cybersecurity laws and guidelines, such as those set forth by the North American Electric Reliability Corporation's Critical

Infrastructure Protection program, makes attempts to protect smart grids more difficult. It takes constant observation and updates to ensure compliance while responding to changing threats.

6. **Human Factors:** There are substantial cybersecurity concerns associated with smart grid operations due to human mistakes, carelessness, and hostile insider activity. Mitigating threats associated with humans requires staff training, educating the public about cybersecurity best practices, and putting access controls in place.
7. **Supply Chain Risks:** Because smart grid components frequently depend on outside suppliers and vendors, there is a higher chance of supply chain intrusions. To reduce supply chain risks, vendors' security policies must be confirmed, extensive risk analyses must be carried out, and supply chain resilience measures must be put in place.

Solutions:

1. **Risk Assessment and Management:** Identify vulnerabilities, evaluate possible threats, and rank cybersecurity investments according to risk exposure by conducting thorough risk assessments. Use risk management techniques to successfully reduce hazards that have been identified.
2. **Defense-in-Depth:** Implement a multi-layered defense plan that includes endpoint protection, network segmentation, encryption, access controls, and intrusion detection systems. Defense-in-depth strategies are put into place to lessen the effects of cyberattacks and stop illegal access to vital systems.
3. **Constant Monitoring and Incident Handling:** Put in place real-time monitoring tools to identify unusual activity, hacking attempts, or security lapses. To guarantee a timely and well-coordinated reaction to cyber-attacks, create incident response plans and hold frequent cybersecurity drills.
4. **Cybersecurity Awareness and Training:** Provide cybersecurity best practices, threat awareness, and incident response protocols to staff members at all organizational levels. Encourage a culture of cybersecurity awareness to enable staff members to identify andreport possible security risks.
5. **Regulatory Compliance:** Make sure that frequent audits, assessments, and security control upgrades are conducted to guarantee compliance with cybersecurity legislation and standards that are relevant to smart grid operations. To handle new cybersecurity issues, interact with industry associations and regulatory bodies.
6. **Investing in Cybersecurity Knowledge and Tools:** Invest in cybersecurity technology, including threat intelligence platforms, intrusion detection/prevention

systems, security information and event management (SIEM) systems, and next-generation firewalls. To develop internal competence, and fund cybersecurity training and certification programs for staff members.

7. **Cooperation and Information Sharing:** To share threat intelligence, best practices, and lessons gained, and encourage cooperation with government agencies, business associates, cybersecurity researchers, and information-sharing organizations. Engage in working groups, workshops, and forums on cybersecurity to solve problems as a group.

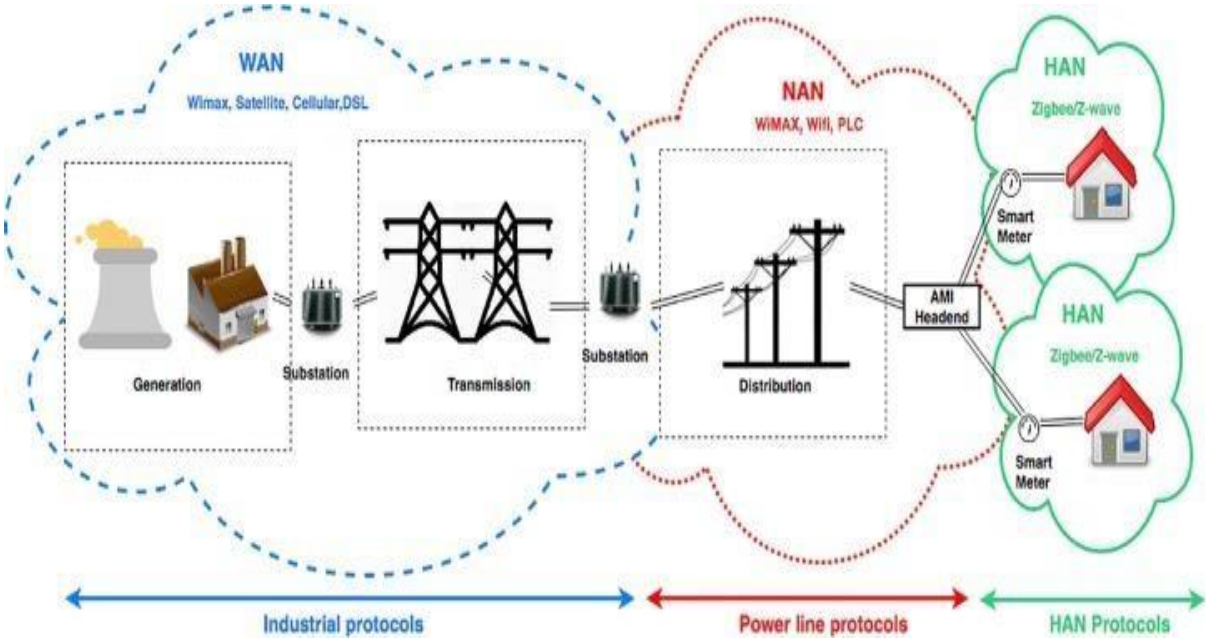

Fig. 7.1. Cyber-Security in Smart Grid: Survey and challenges.

7.2 Simulation & Results

To examine the frequency response of the grid, the load frequency control (LFC) model has been put into practice in the MATLAB/Simulink environment. Fig. 7.2 (a) displays the inertia vs. time waveform. Here, the supply frequency for the LFC model is 60 Hz. The load and inertia waveforms return to their initial frequency. In a time-delay attack, the attacker makes sure that the incoming Area Control Error (ACE) values are not received by the controller promptly, hence causing a delay in the system. Consequently, the response eventually exhibits some instability.

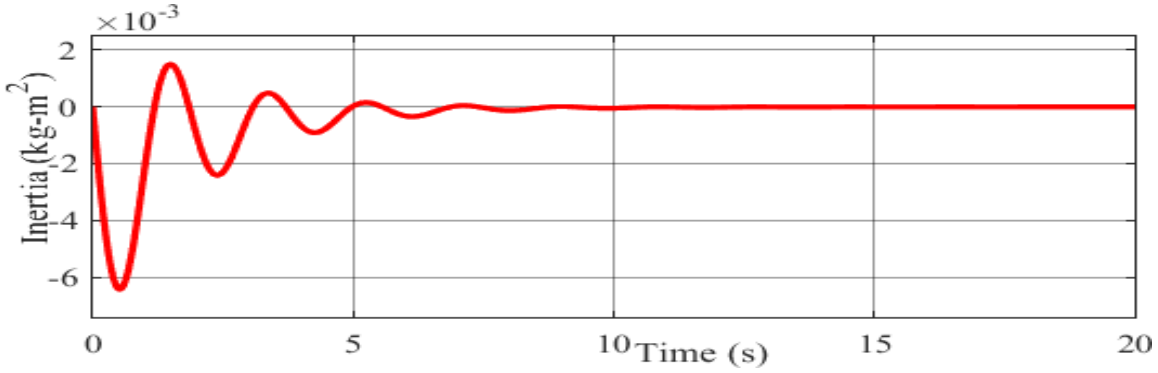

Fig. 7.2 (a). Inertia and Load Waveform of LFC.

This indicates that, as seen in Fig. 7.2 (b), the change in frequency per unit and hertz is currently zero. This waveform illustrates what happened in the LFC model when the PID Controller block was attached. The waveform returns to its starting point. PID Controller smooths the waveform and eliminates ripple and transients. Fig. 9 displays the frequency vs. time curve.

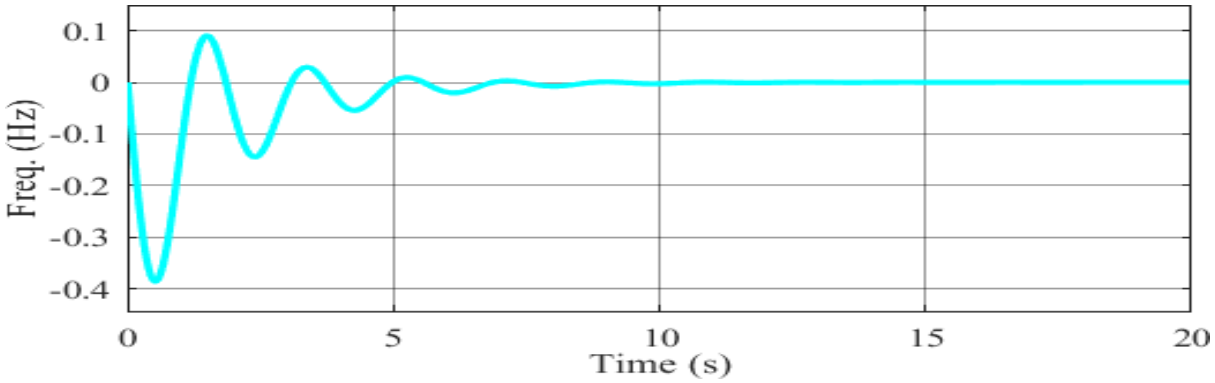

Fig. 7.2 (b). Variation of the frequency of the LFC model.

The LFC model's frequency range at 60 Hz. This indicates that, as of right now, Fig. 7.2 (c) displays the frequency change per unit and hertz. This waveform illustrates what happened when the PID Controller block in the LFC model was linked. The waveform returns to its starting point. PID Controller smooths the waveform and eliminates ripple and transients.

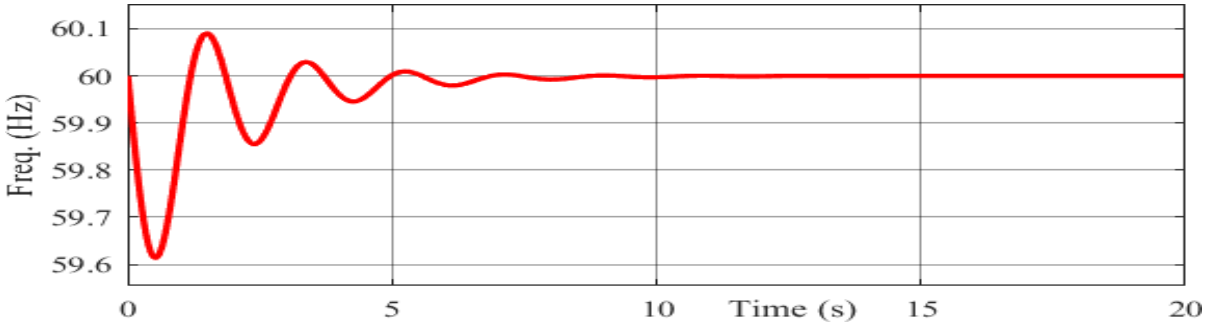

Fig. 7.2 (c). Frequency in waveform of LFC model.

The waveform now displays the variation in load power per unit. In Fig. 7.2 (d), this waveform is displayed. That works out to be 0.2 per unit. This waveform illustrates what happened in the LFC model when the PID Controller block was attached. The waveform returns to its starting point. In addition, the PID Controller produces a smooth waveform.

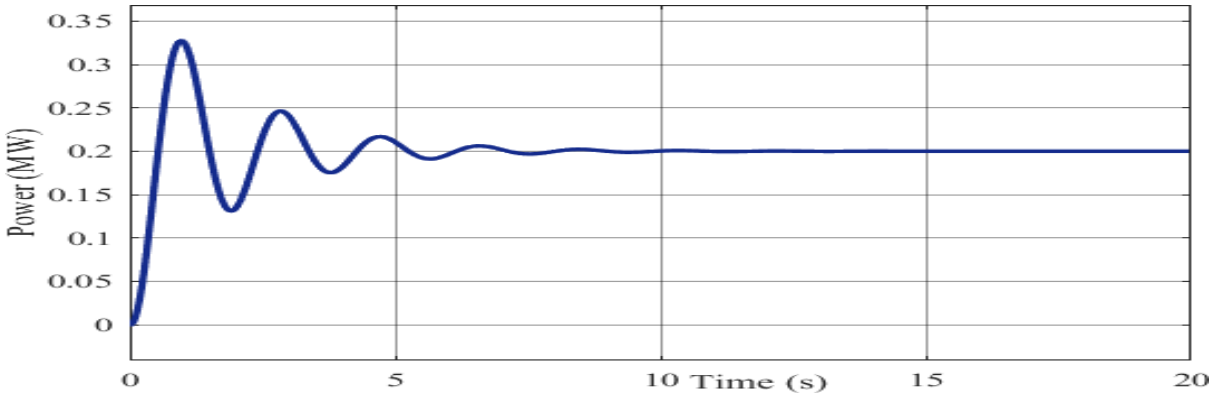

Fig. 7.2 (d). Turbine waveform of LFC model.

The MW graph's power change can also be found in this waveform. The power reached 50 MW, which was the ultimate value. This waveform illustrates what happened in the LFC modelwhen the PID Controller block was attached. The PID Controller eliminates ripple andtransients from the waveform and smooths it down. In Fig. 7.2 (e), the power is plotted againsttime.

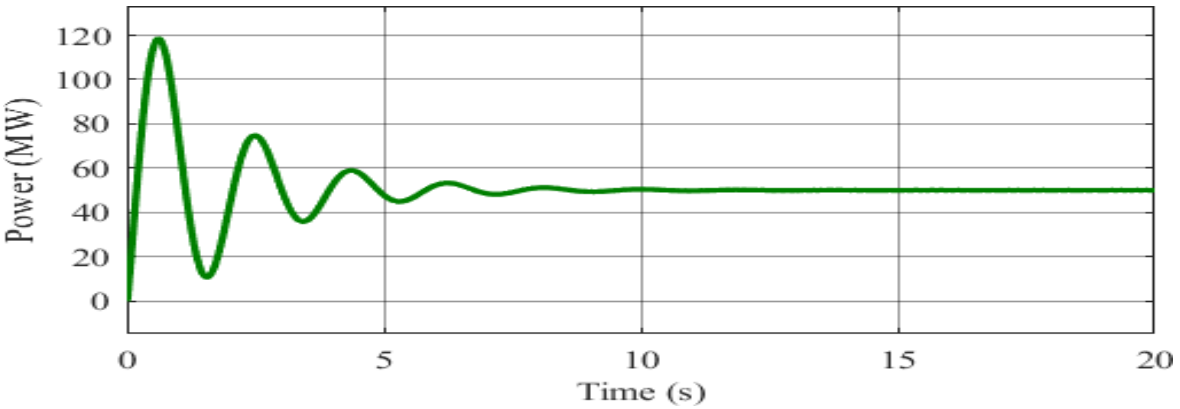

Fig. 7.2 (e). Power waveform in LFC model.

Ultimately, the graph displays the 300 W total load demand. Thus, it has been demonstrated that the load power measurements are accurate at this point as well, provided that the frequency is returned to its initial value. The waveform returns to its starting point. The PID controller eliminates ripple and transients from the waveform and smooths it down. In Fig. 7.2 (f), the power is displayed against time.

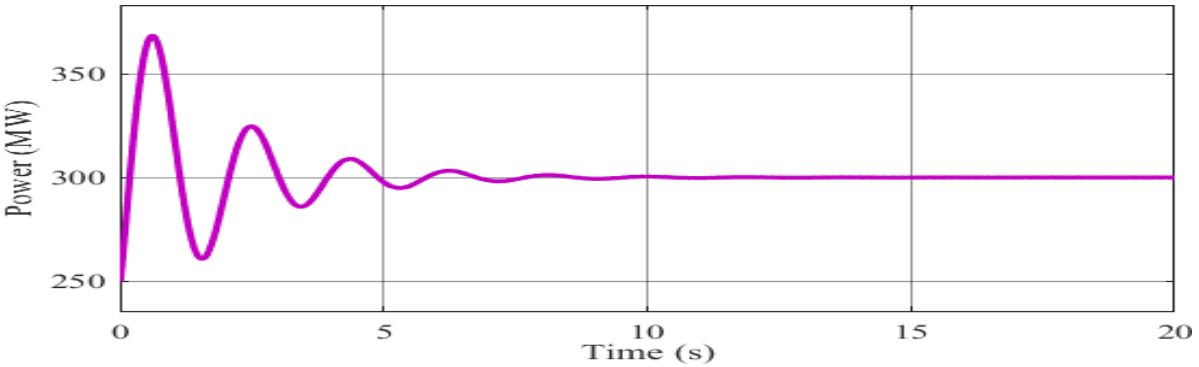

Fig. 7.2 (f). Total power in MW waveforms in the LFC model.

Table 7. Simulation Components of Smart Grid

Parameters	**Values**
PL in MW	300MW
ΔPL in MW	50MW
Base MVA	250MVA
Δf in per unit1	0.2Hz
Base frequency	60Hz
Conductance	0.05℧
Proportional (P) of PID controller	50
Integral (I) of PID controller	30
Derivative (D) of PID controller	10
Filter coefficient (N) of PID controller	100

CHAPTER 8
CONCLUSION & FUTURE SCOPE OF WORK

8.1 Conclusion

This study examines creative ways to reduce these risks and provides a full analysis of the many difficulties that cyber security in the smart grid faces. The smart grid is becoming an essential piece of infrastructure meeting the energy demands of the modern world as communication networks and digital technology continue to transform the power grid. The study emphasized how diverse cyber threats might be when considering the smart grid. These risks include possible flaws in communication protocols as well as sophisticated attacks aimed at vital infrastructure. Given that the smart grid depends on digital technology to improve its sustainability, dependability, and efficiency, these cybersecurity issues must be successfully resolved. The MATLAB/Simulink environment has been used to implement the load frequency control model.

8.2 Future Scope of Work

Future research on cybersecurity in smart grid technology has a wide range of possible applications. The following are some important topics of study that academics, business experts, and legislators may consider:

Advanced Threat Detection and Response: To proactively identify and mitigate cyber threats in real-time, develop and use advanced threat detection approaches, such as machine learning, artificial intelligence, and behavior analytics. Boost incident response capacities with swift threat containment, automation, and coordination.

Resilient Communication Networks: To improve the resilience and robustness of smart grid communication networks against cyberattacks, network failures, and natural disasters, research resilient communication architectures, such as mesh networks, Software-Defined Networking (SDN), and edge computing.

Safe Internet of Things Devices and Edge Computing: Handle security issues about distributed energy resources (DERs) connected to smart grids, edge computing platforms, and Internet of Things (IoT) devices. To reduce IoT-related cyber risks, create safe firmware update procedures, IoT device authentication methods, and security-by-design principles.

Blockchain For Grid Security: Examine how blockchain technology can be applied to improve the security, integrity, and transparency of smart grid operations. This includes safe peer-to-peer energy transactions, tamper-evident logging, and decentralized authentication. Examine blockchain-based methods for safely storing identities, transactions, and data related to smart grids.

Privacy-Preserving Data Analytics: Develop privacy-preserving data analytics methods, such as homomorphic encryption, federated learning, and differential privacy, to enable safe and privacy-aware analysis of sensitive smart grid data while preserving consumer rights to privacy and regulatory compliance.

Cyber-Physical System Security: Examine the safety of industrial Internet of Things (IoT) devices, SCADA systems, and integrated control systems (ICS) in smart grids. To reduce cyber-physical risks and vulnerabilities at the system level, investigate CPS security modeling, vulnerability assessment, and resilience analysis.

Supply Chain Security: To reduce supply chain attacks, fake parts, and malicious firmware implants in smart grid hardware and software, reinforce supply chain security procedures and vendor risk management techniques. To improve resilience against supply chain risks, conduct supplier cybersecurity evaluations, supply chain audits, and supply chain risk assessments.

REFERENCES

[1]. S. I. Vagropoulos and A. G. Bakirtzis, ``Optimal bidding strategy for electric vehicle aggregators in electricity markets," IEEE Trans. PowerSyst., vol. 28, no. 4, pp. 4031-4041, Nov. 2013.

[2]. IEA.WorldEnergyOutlook2017.2017,https://www.iea.org/reports/world-energy-outlook-2017.

[3]. Tseng C, Chau SC, Liu X. Improving viability of electric taxis by taxi service strategy optimization: A big data study of New York City. IEEE Trans Intell Transp Syst 2019;20(3):817–29.

[4]. Aghajan-Eshkevari, S.; Azad, S.; Nazari-Heris, M.; Ameli, M.T.; Asadi, S. Charging and Discharging of Electric Vehicles in Power Systems: An Updated and Detailed Review of Methods, Control Structures, Objectives, and Optimization Methodologies. Sustainability 2022, 14, 2137.

[5]. Mojumder, M.R.H.; Ahmed Antara, F.; Hasanuzzaman, M.; Alamri, B.; Alsharef, M. Electric Vehicle-to-Grid (V2G) Technologies: Impact on the Power Grid and Battery *Sustainability* **2022**, *14*, 13856.

[6]. Zhang, Z.; Lv, L. Status and Development of Research on Orderly Charging andDischarging of Electric Vehicles. *Electronics* **2023**, *12*, 2041.

[7]. R. Mkahl, "Contribution to the modeling, dimensioning, and management of the energy flows of an electric vehicle charging system: Study of the interconnection with the electric network," Ph.D. dissertation, Dept.Eng. Sci. Microengineering, Univ. Technol. Belfort-Montbéliard, Belfort, France, 2015.

[8]. C. Ma, J. Rautiainen, D. Dahlhaus, A. Lakshman, J.-C. Toebermann, andM. Braun, "Online optimal charging strategy for electric vehicles," EnergyProcedia, vol. 73, pp. 173–181, Jun. 2015.

[9]. Di Somma, M.; Graditi, G.; Siano, P. Optimal bidding strategy for a DER aggregator inthe day-ahead market in the presence of demand flexibility. IEEE Trans. Ind. Electron. 2018, 66, 1509–1519.

[10]. J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012.

[11]. D. Faquir, N. Chouliaras, V. Sofia, K. Olga, L. Maglaras, "Cybersecurity in smart grids, challenges and solutions," in *Journal of AIMS Electronics and Electrical Engineering*, vol. 5, no. 1, pp. 24-37, 2021.

[12]. F. E. Abrahamsen, Y. Ai, M. Cheffena, “Communication Technologies for Smart Grid: A Comprehensive Survey,” in *Sensors 2021*, vol. *21*, pp. 1-24, 2021.

[13]. U. Tariq, I. Ahmed, A. K. Bashir, A. K. Shaukat, “Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review,” in *Sensors 2023*, vol. *23*, pp. 1- 24.

[14]. T. Alsuwian, A. Shahid Butt, A. A. Amin, “Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review,” in *Sustainability* 2022, vol. *14*, pp. 1-21, 2022.

[15]. M. Orlando et al., “A Smart Meter Infrastructure for Smart Grid IoT Applications,” in *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12529-12541, 15 July 15, 2022.

[16]. G. R. Barai, S. Krishnan and B. Venkatesh, “Smart metering and functionalities of smart meters in smart grid - a review,” *2015 IEEE Electrical Power and Energy Conference (EPEC)*, London, ON, Canada, 2015, pp. 138-145, 2015.

[17]. S. Shapsough, Y. Salsabeel Y. et al. “Smart grid cyber security: Challenges and solutions,” *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pp. 170-175, 2015.

[18]. A. A. Bouramdane, “Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process,” in *Journal of Cybersecurity and Privacy*, vol. *3*, pp. 662-705, 2023.

[19]. V. Gomez, C. Hernandez, and F. Martinez, “Energy policies in smart grids,” in *Journal of Contemporary Engineering Sciences*, vol. 10, no. 20, pp. 987–999, 2017.

[20]. A. A. Abdullah, B. M. El-den, K. M. Abo-Al-Ez, T. M. Hassan, “Security Management for an Advanced Metering Infrastructure (AMI) System of Smart Electrical Grids,” in *MDPI Journal of Applied Science*, vol. *13*, pp. 1-21, 2023

[21]. Farhangi, "The path of the smart grid," in IEEE Power and Energy Magazine, vol. 8, no. 1, pp. 18-28, January-February 2010.

[22]. M. Ghalib, A. Ahmed, I. Al-Shiab, Z. Bouida and M. Ibnkahla, "Implementation of a Smart Grid Communication System Compliant with IEEE 2030.5," *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, USA, 2018, pp. 1-6.

[23]. C. Peng, H. Sun, M. Yang and Y. -L. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554-1569, Aug. 2019.

[24]. M. Guerin, A. Orda, and D. Towsley, “A Framework for Network Modeling and Simulation: Tools and Techniques,” in *EEE Transactions on Automatic Control*, vol. 40, no.

2, pp. 115-131, Feb. 1995.

[25]. Y. -L. Wang, Q. -L. Han, M. -R. Fei and C. Peng, "Network-Based T– S Fuzzy Dynamic Positioning Controller Design for Unmanned Marine Vehicles," in IEEE Transactions on Cybernetics, vol. 48, no. 9, pp. 2750-2763, Sept. 2018.

[26]. H.-B. Zeng, K. L. Teo, and Y. He, "A new looped-functional for stability analysis of sampled-data systems," in Elsevier, Journal of *Automatica*, vol. 82, pp. 328–331, Aug. 2017.

[27]. W. Wang, Y. Xu, M. Khanna, "A survey on the communication architectures in smart grid," In *Journal of Computer Networks*, vol. 55, no. 15, pp. 3604-3629, 2011.

[28]. S. Bimenyimana, and A. Godwin, "Traditional vs Smart Electricity Metering Systems: A Brief Overview," in *Journal of Marketing and Consumer Research*, vol. 46, pp. 1-7, 2018.

[29]. C. Peng, H. Sun, M. Yang and Y. -L. Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554-1569, Aug. 2019.

[30]. O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious Data Attacks on the Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[31]. A. R. Devidas and M. V. Ramesh, "Cost Optimal Hybrid Communication Model for Smart Distribution Grid," in *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4931-4942, Nov. 2022.

[32]. V. Tiwari, S. M. Dubey, H. M. Dubey, and M. Pandit, "Smart grid communication: A survey of state-of-the-art," in *Proc. Int. Conf. Sustain. Innov. Solutions Current Challenges Eng. Technol.*, pp. 524– 534, Nov. 2019.

[33]. F. A. Asuhaimi, S. Bu, P. V. Klaine, and M. A. Imran, "Channel access and power control for energy-efficient delay-aware heterogeneous cellular networks for smart grid communications using deep reinforcement learning," *IEEE Access*, vol. 7, pp. 133474–133484, 2019.

[34]. W. Strielkowski, L. Civín, E. Tarkhanova, and et al. "Renewable Energy in the Sustainable Development of Electrical Power Sector: A Review," in *Energies*, vol. *14*, pp. 1-22, 2021.

[35]. H. Jokar, B. Bahmani-Firouzi, H. H. Alhelou and P. Siano, "Transmission and Distribution Substation Energy Management Considering Large-Scale Energy Storage, Demand Side Management and Security-Constrained Unit Commitment," in *IEEE Access*, vol. 10, pp. 123723-123735, 2022.

[36]. M. Orlando *et al*., "A Smart Meter Infrastructure for Smart Grid IoT Applications," in *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12529-12541, 15 July 15, 2022.

[37]. F. E. Abrahamsen, Y. Ai, M. Cheffena, "Communication Technologies for Smart Grid:A

Comprehensive Survey," *Sensors* 2021, *21*, pp. 1- 22.

[38]. Y. E. G. Vera, R. Dufo-Lopez, J. L. B. Agustín, "Energy Management in Microgrids with Renewable Energy Sources: A Literature Review," *Applied Science* 2019, vol. *9*, pp. 1-24, 2019.

[39]. O. Bogdanova, K. Viskuba, L. Zemite, "A Review of Barriers and Enables in Demand Response Performance Chain," MDPT Journal of *Energies*, vol. 16, pp. 1-33, 2023.

[40]. T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, "Cybersecurity in Power Grids: Challenges and Opportunities," in PMDI Journal of Sensors (Basel), vol. 18, pp. 1-14, 2021.

RESEARCH PUBLICATIONS

1. Naman, **R. M. Pindoriya**, Pratim Kundu, and B. S. Rajpurohit, "Impact of V2G/G2V on Voltage Stability in Distribution Networks", *2024 IEEE Region 10 Symposium (TENSYMP)*, September 27-29, 2024, in NSUT, Delhi, India *(Accepted)*

2. Naman, **R. M. Pindoriya**, and B. S. Rajpurohit, "Cyber Security in the Smart Grid: Challenges and Solutions-A Review", *2024 IEEE 4th International Conference on Sustainable Energy and Future Electric Transportation (SeFeT2024)*, 31 July – 3 August 2024, in Hyderabad, India

Naman Thesis

ORIGINALITY REPORT

11%	6%	7%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Chen Peng, Hongtao Sun, Mingjin Yang, Yu-Long Wang. "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019 Publication	1%
2	www.mdpi.com Internet Source	1%
3	"Data Analytics for Smart Grids Applications—A Key to Smart City Development", Springer Science and Business Media LLC, 2023 Publication	1%
4	Aryadevi Remanidevi Devidas, Maneesha Vinodini Ramesh. "Cost Optimal Hybrid Communication Model for Smart Distribution Grid", IEEE Transactions on Smart Grid, 2022 Publication	1%
5	"Smart Grids and Their Communication Systems", Springer Science and Business Media LLC, 2019	<1%