Identifying Cybersecurity Best Practices for the Marine Renewable Energy

June 2023

What's next...

The RMIT University - Centre for Cyber Security Research and Innovation (CCSRI)

The RMIT University Centre for Cyber Security Research and Innovation (CCSRI) is a multi-disciplinary research centre that draws researchers from across RMIT's schools and colleges to bring a truly multidisciplinary approach to the organisational, human, and technical aspects of Cyber Security.

The mission of the RMIT University Centre for Cyber Security Research and Innovation is to be acknowledged as a world-class research centre in multi-disciplinary Cyber Security research and to be acknowledged by Australian and overseas industry and government as a leading source of knowledge and expertise in multi-disciplinary Cyber Security research.

Table of Content

Abbreviations and Acronyms

2FA	–	Two-Factor Authentication
AC	–	Alternating Current
AES	–	Advanced Encryption Standard
APAC	–	Asia-Pacific Region
ARENA	–	Australian Renewable Energy Agency
BDD	–	Built-in Data Diagnostics Mechanism
BDDA	–	Bad Data Detection Algorithms
BIPV	–	Building-Integrated Photovoltaics
CC	–	Control Centres
CCTV	–	Closed-Circuit Television
CSP	–	Concentrated Solar Power
DC	–	Ddirect Current
DLP	–	Data Loss Prevention
DMZ	–	Demilitarized Zone
DoS	–	Denial-Of-Service Attack
EMS	–	Energy Management System
GW	–	Giga Watt
GWEC	–	Global Wind Energy Council
HACT	–	Horizontal Axis Current Turbine
HAWT	–	Horizontal-Axis Wind Turbines
ICS	–	Industrial Control Systems
IDPS	–	Intrusion Detection And Prevention Systems
IT	–	Information Technology
MFA	–	Multifactor Authentication
MitM	–	Man-In-The-Middle Attack
MITM	–	Man-in-the-middle Attacks
MRE	–	Marine Renewable Energy
MRES	–	Marine Renewable Energy Systems
MW	–	Mega Watt
NAC	–	Network Access Control
OCEC	–	Ocean Current Energy Conversion System
OH	–	Oscillating Hydrofoil
OT	–	Operation Technology
OTEC	–	Ocean Thermal Energy Conversion
OWC	–	Oscillating Water Column
OWSC	–	Oscillating Wave Surge Converters
PPC	–	Power Plant Controller
PRO	–	Pressure-Retarded Osmosis
PV	–	Photovoltaic
RE	–	Renewable Energy
RED	–	Reverse Electrodialysis
SCADA	–	Supervisory Control and Data Acquisition
SDN	–	Software-Defined Networking
SIEM	–	Security Information And Event Management

SOAR	–	Security Orchestration, Automation, And Response
SQL	–	A Structured Query Language Injection
STE	–	Solar Thermal Power
TW	–	Tera Watt
UFDI	–	Undetected False Data Injection Attacks
VACT	–	Vertical Axis Current Turbine
VAWT	–	Vertical-Axis Wind Turbines
VPN	–	Virtual Private Networks
VSN	–	Virtual Secure Network
WEC	–	Wave Energy Converter
WTCP	–	Wind Turbine Control Panel

1. Introduction

Marine Renewable Energy Systems (MRES) are innovative and growing technology that captures the power of the ocean to produce electricity. The ocean is a powerful source of renewable energy, with the potential to provide a significant amount of clean and sustainable energy to the world. MRES are designed to be both resilient and efficient, to operate in harsh marine environments. There are several different types of marine technologies, such as tidal energy systems, wave energy systems and offshore wind farms. While still in their infancy, marine power technologies, hold great potential to contribute significantly to the global shift toward clean, renewable energy sources.

MRES are becoming increasingly important as a sustainable source of energy in the Asia Pacific (APAC) region. These systems rely heavily on digital technology, including control systems, sensors, and communication networks, to monitor and control their operations. As a result, MRES are vulnerable to cyberattacks, which can compromise the safe and efficient operation of these systems.

The identification and mitigation of cyber threats and vulnerabilities in MRES are crucial for ensuring the safe and efficient operation of these systems, as well as for protecting the information and digital assets of the maritime industry sector. However, the maritime industry sector may lack the knowledge and resources to effectively identify and mitigate cyber threats and vulnerabilities in MRES.

This project aims to address this gap by identifying and categorizing cyber threats and vulnerabilities associated with MRES currently being used in the APAC region and by identifying and categorizing best practices for mitigating these threats. The project will also develop a guidance and recommendation report to be used by the maritime industry sector to protect information and digital assets in MRES from cyberattacks.

The scope of the project will focus on MRES in the APAC region, specifically on offshore wind and wave energy converters. The research questions for this project are:

1. **What are the cyber threats and vulnerabilities associated with MRES currently being used in the Asia Pacific region?**
2. **What are the best practices for mitigating these cyber threats and vulnerabilities in MRES?**

The significance of this study lies in the increasing importance of MRES as a sustainable energy source and the need to ensure their safe and efficient operation by identifying and mitigating cyber threats and vulnerabilities. The findings of this project will provide valuable information for the maritime industry sector in the APAC region to protect information and digital assets in MRES from cyberattacks. Furthermore, this project can contribute to the development of a more resilient and secure maritime industry sector in the Asia Pacific region.

In this project, the term cyber threats refer to any malicious activity that targets information systems, networks, or devices. Vulnerabilities refer to weaknesses in systems, networks, or devices that can be exploited by cyber threats.

The methodology for this project involves a literature review of the current state of cyber threats and vulnerabilities in MRES and the maritime industry sector, as well as a review of previous research on this topic. This study will gather data from a variety of primary and secondary sources, including interviews with experts in the field, case studies, and analysis of existing data. The data will then be analysed using qualitative and quantitative techniques to identify and categorize cyber threats and vulnerabilities, as well as best practices for mitigating these threats.

Overall, this project aims to provide a comprehensive understanding of the cyber threats and vulnerabilities associated with MRES currently being used in the Asia Pacific region, as well as effective methods for mitigating these threats. The guidance and recommendations developed in this project will serve as a valuable resource for the maritime industry sector in the Asia Pacific region to protect information and digital assets in MRES from cyberattacks.

The maritime industry is experiencing a swift transformation with integrating innovative technology and digitizing existing services. While these advancements aim to boost profits, they may also present new risks and challenges. Recently, digital attack surface is increasing, and incidents can lead to severe consequences. Specifically, the growing interconnectivity and convergence of Information Technology (IT) and Operational Technology (OT) systems introduce new threats to maritime operations, which could lead to severe financial and reputational consequences. Moreover, the maritime sector faces an increasingly hostile threat landscape, with cyber-attacks occurring more frequently [1].

2. Renewable Energy Technologies

As environmental concerns gain prominence, economies are formulating strategies to reduce emissions, scientists are innovating new technologies, and investors are assessing the sustainability practices of companies to ensure a greener future. Fossil-fuel energy generators stands out as a major contributor to emissions on environment. Therefore, renewable energy technologies are becoming increasingly important as the world seeks to move away from fossil fuels and towards a more sustainable future. Renewable systems capture the power of naturally replenishing resources such as wave, water, sun, and wind to generate clean, renewable, and green energy. As opposed to fossil fuels, which are finite sources and release harmful emissions into the atmosphere, renewable energy sources are abundant and have a much lower impact on the environment. Renewable energy sources, unlike fossil fuels, can replenish themselves naturally without depleting the earth and have a minimal or zero carbon impact on the environment, making them a sustainable and eco-friendly solution for meeting our energy needs [2-3]. Renewable energy sources are depicted in Figure (1) [4-10]:

Figure 1. Renewable Energy Sources

Solar 	This source of energy harnesses the power of the sun to generate electricity. It is one of the most widely utilized renewable energy sources, and its popularity is proliferating due to its numerous benefits. Providing clean, safe, and reliable power is the most significant potential of solar energy.
Wind 	It is an abundant and clean source of renewable energy that harnesses the power of the wind to generate electricity.
Hydro 	Hydro is one of the most widely developed and utilized sources of clean energy. In contrast to solar and wind energy, which are affected by weather conditions, hydro energy can provide consistent energy generation, making it a more reliable energy source.
Geothermal 	This type of renewable energy is sourced directly from the Earth's core, providing a sustainable and eco-friendly power option.
Ocean 	The ocean can produce two kinds of renewable energy: thermal energy from the sun’s heat and mechanical energy from waves and tides. Wave and tide energy are generated from the ocean's movement. A tide is the rhythmic rise and fall of sea levels caused by the moon's and sun's gravitational pull on the Earth's oceans. In contrast, wave energy is derived from the movement of ocean waves caused by wind, earthquakes, or other factors.
Biomass 	It is a renewable energy source from organic matter, such as crops, trees, and agricultural waste. Photosynthesis produces this energy, and carbon dioxide is stored in plants as energy, then released when burning occurs. Biomass energy is sourced from two main categories: primary and secondary biomass. Plant materials grown for energy production are primary biomass sources, such as fruits, crops, sunflower seeds, and wood. Secondary biomass energy sources are waste materials that can be used as fuel, such as animal waste, plant residues, and sewage [11].

The rapid growth of the world's population is driving greater energy demand, leading to a greater reliance on finite fossil fuels such as coal, oil, and gas. This dependency creates numerous sustainability issues, including environmental degradation, greenhouse gas emissions, depletion of resources, global warming, and volatile fuel prices. With its low emissions and environmentally friendly characteristics, renewable energy presents a

sustainable solution to these challenges and offers multiple benefits, including economic, social, and environmental advantages [12].

It has been several decades since scientists began exploring the potential of renewable energy sources to generate electricity and heat. In light of the increasing concern about the negative environmental impacts of fossil fuels and the need for sustainable energy solutions, renewable energy sources are becoming increasingly crucial. Scientists are developing technologies to harness the mentioned source of renewable energies and transform them into an efficient and effective form of energy for humans, such as electricity [13]. There are several technologies used to create renewable energy, including solar photovoltaic panels, offshore/onshore turbines and power generators. The various renewable energy technologies used to generate electricity are summarized in Table (1) [14-17].

Table 1. Categories of renewable energy technologies

Energy Source	Technology Group	Designed Technologies
Solar	Solar Systems	Photovoltaic (PV) systems Concentrated solar power (CSP) Building-Integrated photovoltaics (BIPV) Solar Thermal Power (STE)
Hydro	Hydro Electric Power	Large and medium types Small, Micro, and Pico types Pumped storage hydro Run-of-River types
Wind	Wind Turbines	Offshore wind turbines Onshore wind turbines Horizontal-Axis wind turbines (HAWT) Vertical-Axis wind turbines (VAWT) Floating wind turbines
Geothermal	Geothermal technologies	Dry Steam Flash Steam Binary Cycle Heat Pump Direct Use
Ocean energy	Marine Technologies	Wave generators Tidal generators Current generators Ocean currents Ocean thermal energy conversion (OTEC) Salinity gradients/osmotic energy Marine biomass production
Biomass	Biomass technologies	Bioenergy plants Anaerobic digestion Biomass gasification Direct combustion

Solar Systems – Solar technologies are systems designed to harness and convert solar renewable energy into functional forms of energy such as heat and electricity. There are different forms of solar technologies. The leading technology in solar energy systems is photovoltaic (PV) cells, made from materials that can convert sunlight into electricity. PV cells come in two forms: monocrystalline and polycrystalline. Monocrystalline cells are made from a single crystal structure and are more efficient at converting sunlight into electricity and also more expensive. Polycrystalline cells are made from multiple crystal structures and are less

efficient but less expensive. Another solar energy technology is concentrated solar power (CSP), a method of concentrating sunlight onto a small area, which heats a fluid to produce steam and drives an electric turbine. BIPV systems are a type of solar technology that integrates PV cells into building materials, such as roofing tiles or windows. Solar technologies play a critical role in the transition to a sustainable energy future. They provide a clean and renewable source of electricity that does not emit harmful pollutants or greenhouse gases [14].

Hydro Electric Technologies - Hydro systems harness the power of moving water to generate electricity in hydropower plants. Hydro energy has been used for centuries, dating back to ancient civilizations where water wheels were used to grind grain and pump water. As of modern times, hydro energy is generated through dams, which store large amounts of water and release it through turbines to generate electricity. Hydro energy has several benefits, including being reliable, flexible, and capable of being stored for later use. Despite these advantages, some challenges are associated with hydro energy, such as the impact on local ecosystems, the cost of building and maintaining hydro dams, and the need for large amounts of water to generate a significant amount of energy.

Hydropower plants harness the kinetic energy of flowing water to generate electricity by rotating a turbine connected to a generator. The amount of electricity generated is affected by the volume and height of water above the turbine. In order to produce electricity, large hydroelectric power plants require dams to store the water required for generation. These dams not only provide a source of irrigation and drinking water but also generate electricity using turbines. These dams not only provide a source of irrigation and drinking water but also generate electricity through the use of turbines. The electricity output from hydropower plants can fluctuate significantly annually, depending on the demand for electricity and the amount of rainfall. However, they can provide both baseload and peak electricity, with the ability to quickly ramp up to maximum power in as little as 90 seconds [18-20].

Wind Turbines – The history of harnessing wind energy for generating electricity dates back to the late 19th century [21]; however, its widespread adoption was limited due to the dominance of steam turbines in the energy sector. The oil crises of the mid-1970s sparked renewed interest in wind energy and increased concerns over resource conservation. As a result, wind energy began to gain traction as a source of electricity, particularly in remote power systems, residential-scale power systems, isolated or island power systems, and utility networks where it was used to charge batteries [22].

The most common wind technology is the wind turbine, which consists of rotors, generators, towers, and various control and safety systems. Wind turbines generate electricity in the same manner as other generation technologies. There is only one difference: wind power, rather than diesel engines or steam turbines, supplies the mechanical power for the electric generator. Wind power turbines have blades that capture the energy from the wind, convert wind energy into mechanical power and turn the turbines. In response to changes in wind speed, control mechanisms direct the blades into the wind (yaw control) and, in the case of large wind turbines, modify blade pitch (blade angle). Electric generators are connected to blades (rotors) via gearboxes [23].

Geothermal technologies – Geothermal energy originates from stored heat in the earth. The heat is generated by the natural decay of radioactive isotopes in the earth's mantle and is transferred to the earth's surface through water circulation in the ground. Geothermal energy can be used for various purposes, including electricity generation, heating and cooling buildings, and various industrial processes. Geothermal energy is a reliable and constant renewable energy source as it is available throughout the year, unlike solar and wind energy, with higher variability and intermittence. Additionally, geothermal energy can be found globally, making it a widely accessible source of clean energy [19-20].

Geothermal power plants extract the heat from geothermal reservoirs to produce steam, which is then used to drive a turbine and generate electricity. Geothermal energy production is characterized by low emissions, as the steam and water used in the process are usually re-injected back into the underground reservoir. Geothermal power plants today can use water in the vapour phase, a combination of vapour and liquid phases, or the liquid phase only. The choice of the plant depends on the depth of the reservoir and the temperature, pressure and nature of the entire geothermal resource [24].

Marine Technologies – Marine technologies refer to the various methods used to harness energy from the ocean, including waves, tides, and ocean thermal energy. Ocean technologies hold immense potential as a clean and renewable source of energy. They have the ability to contribute significantly towards addressing the impacts of climate change and minimizing greenhouse gas emissions. Tidal energy technology uses underwater turbines to convert the kinetic energy from tidal currents into electricity. Wave energy technology uses devices such as buoys or floats that move with the waves, generating electricity through mechanical or hydraulic means. Ocean thermal energy conversion technologies use the temperature difference between the surface and deep ocean waters to drive a power cycle and produce electricity.

Biomass technologies – Biomass technologies refer to the various methods and systems designed to convert biomass, or organic matter, into energy, such as heat, electricity, or biofuels. Some common biomass technologies include direct combustion, anaerobic digestion, pyrolysis, and gasification. These technologies can be used to generate energy from various biomass sources, such as wood chips, agricultural waste, and municipal solid waste. Biomass technologies are becoming increasingly popular as renewable energy sources because they are relatively low-cost and can reduce dependence on non-renewable energy sources, such as fossil fuels [25].

2.1. Overview of Marine Renewable Energy Systems

Marine Renewable Energy (MRE) systems refer to technologies developed to capture the power of the ocean to generate clean and sustainable energy. Marine energy is defined as “mechanical energy derived from tidal movement, wave motion or ocean current and exploited for electricity generation” [26]. MRE sources include waves, tides, offshore wind, ocean currents, salinity gradients, thermal differences, and biomass. This renewable energy source can provide a sustainable solution to meet the energy demands of homes, businesses, and

industries, reducing reliance on non-renewable energy sources and mitigating their negative environmental impacts. By utilizing the natural movements of ocean waves, tides, currents, and thermal differences, these systems aim to provide a sustainable and environmentally friendly energy source that can contribute to the fight against climate change [104].

Marine technologies are at different stages of maturity and are accompanied by a variety of technical and economic challenges. A common form of MRES is offshore wind turbines.

Offshore Wind Technologies

The process of generating electricity through wind farms located in bodies of water, typically at sea or ocean, is known as offshore wind power technology. These power plants benefit from higher wind speeds offshore compared to on land, resulting in a higher rate of electricity generation per unit of installed capacity [100].

The concept of utilizing wind energy has been around for centuries, with the use of windmills and wind-powered sailboats dating back to ancient civilizations. However, the development of offshore wind technologies as a source of electricity is a relatively new phenomenon. The inaugural offshore wind farm was installed in 1991 in Vindeby, Denmark. Since its inception, the technology has experienced remarkable advancements, both in terms of efficiency and capacity. With larger and more powerful turbines being developed, offshore wind farms have expanded to deeper waters and further from coastlines, unlocking the potential for greater energy production. Furthermore, advances in installation, operations, and maintenance have helped to lower costs and improve the reliability of offshore wind farms. These advancements have spurred the growth of the industry, making offshore wind energy a vital component of the global renewable energy mix. Governments and private sector entities around the world are investing in the deployment of offshore wind farms to meet increasing energy demands while fostering a sustainable future and reducing carbon emissions.

Offshore wind farms have several advantages over their onshore counterparts, including higher wind speeds and more consistent wind patterns. This results in greater electricity generation per unit of capacity installed, making offshore wind farms an increasingly attractive option for meeting energy demands.

In the early years of offshore wind development, projects were small, and investment was limited. In recent years, however, there has been a significant increase in investment and progress in constructing larger offshore wind farm projects. This has been driven by a growing awareness for lessening carbon emissions and addressing climate change, as well as development in technologies that have reduced the cost of offshore wind energy.

Today, offshore wind technology is a rapidly growing industry with the potential to play a crucial role in meeting the world's energy demands in a sustainable and environmentally responsible manner. The development of offshore wind technologies continues to advance, with innovations in design, materials, and construction methods aimed at increasing efficiency, reducing costs, and improving reliability.

The key benefits of utilizing offshore wind energy are listed below [27]:

- Renewable source – Offshore wind energy is a renewable energy source that is not constrained by finite resources like fossil fuels. Being inexhaustible, it serves as a sustainable and limitless energy solution.
- Clean energy – Offshore wind energy is a clean energy that does not emit CO2 or other harmful pollutants, making it an environmentally friendly option.
- Abundant Resource – Offshore wind energy has a vast and abundant resource, especially in areas with strong and consistent winds.
- High-Capacity Factor – Offshore wind turbines can generate more energy than onshore turbines due to stronger and more consistent wind speeds. The wind speeds offshore are often higher compared to those found in medium-sized onshore wind farms, sometimes even twice as much.
- Increased Energy Production – Offshore wind farms offer significant advantages over their onshore counterparts due to the availability of larger, uninterrupted areas at sea. This ample space enables the installation of more turbines, and often, larger ones, which can capture and convert greater amounts of wind energy into electricity.
- Reduced Land Use – Offshore wind farms take up less land than onshore wind farms, making it a more environmentally friendly option.
- Better Visibility – Offshore wind turbines are located in the ocean and are, therefore, less visible from land. This makes them a more aesthetically pleasing option.
- Reduced Interference with Wildlife – Offshore wind turbines impact wildlife habitats and migration patterns less than onshore wind farms.
- Transportation – Offshore wind turbines have the advantage of being able to reach much larger unit capacities and sizes than onshore wind turbines due to the ease of maritime transport, which has fewer limitations compared to land transportation. This makes it possible to efficiently transport large components such as blades, nacelles, and towers.
- Space utilization – The ocean provides ample space for large offshore wind turbines, allowing for the construction of bigger turbines and, thus, the generation of more energy. This leads to increased efficiency and reduced reliance on fossil fuels for coastal cities.
- Cost-effective – The cost of offshore wind farm has been decreasing in recent years and is becoming increasingly competitive with traditional energy sources.
- Increased energy security – By diversifying energy sources, countries can reduce their dependence on imported energy and increase their energy security.

There are several challenges associated with the deployment and operation of offshore wind energy generators, including [28-30]:

- Limited shallow water areas – Most shallow water areas, where wind farms are easier to build, are already developed, so new wind farm projects must be built in deeper waters. But building wind farms in water deeper than 200 feet (~60 m) is very challenging.

- High cost – Offshore wind projects are generally more expensive than onshore wind energy projects due to the additional costs associated with building and maintaining turbines in an offshore environment.
- Technical difficulties – Offshore wind turbines must be able to withstand harsh weather conditions and saltwater corrosion, which can lead to technical difficulties and maintenance issues.
- Environmental concerns – Offshore wind turbines can impact the marine environment, including the migration patterns of marine animals and birds.
- Grid connection – Connecting offshore wind farms to the existing power grid can be a challenge, as the electricity generated by the wind turbines must be transported to the shore.
- Public opposition – Offshore wind turbines can be visually intrusive, leading to public opposition to new wind farm projects.

How Does Offshore Wind Power Work?

Offshore wind power is generated by harnessing the energy from wind turbines situated in the ocean. These turbines comprise several key components, including a rotor, gearbox, generator, control system, and tower. As the wind blows, it causes the rotor blades to rotate, driving the gearbox, which in turn powers the generator to produce electricity. The control system is responsible for regulating the rotor blades' speed, ensuring optimal energy production. The tower supports the rotor, gearbox, and generator, positioning the rotor blades at the ideal angle to capture the wind most efficiently.

Once electricity is generated by offshore wind turbines, it is transmitted to the shore through a series of steps. Initially, cables run down the tower and beneath the seabed, connecting the turbines to an offshore substation. At the offshore substation, the electrical voltage is increased to minimize transmission losses as the energy is sent to the shore through high-voltage underwater cables. Upon reaching land, the electricity is directed to an onshore substation, where it undergoes further adjustments in voltage to match the requirements of the electrical grid. These voltage adjustments ensure the efficient and stable integration of the generated electricity into the grid for distribution to consumers. This process highlights the critical role of substations and transmission infrastructure in delivering electricity from offshore wind farms to the grid. After the electricity generated by offshore wind farms has been adjusted to the appropriate voltage at the onshore substation and integrated into the electrical grid, it is distributed to customers through the existing power distribution network. This network carries electricity to residential, commercial, and industrial consumers, supplying them with the clean and renewable energy produced by the offshore wind turbines [31].

Figure (2) illustrates the overall process of generating electricity in offshore wind farms and transforming it for distribution.

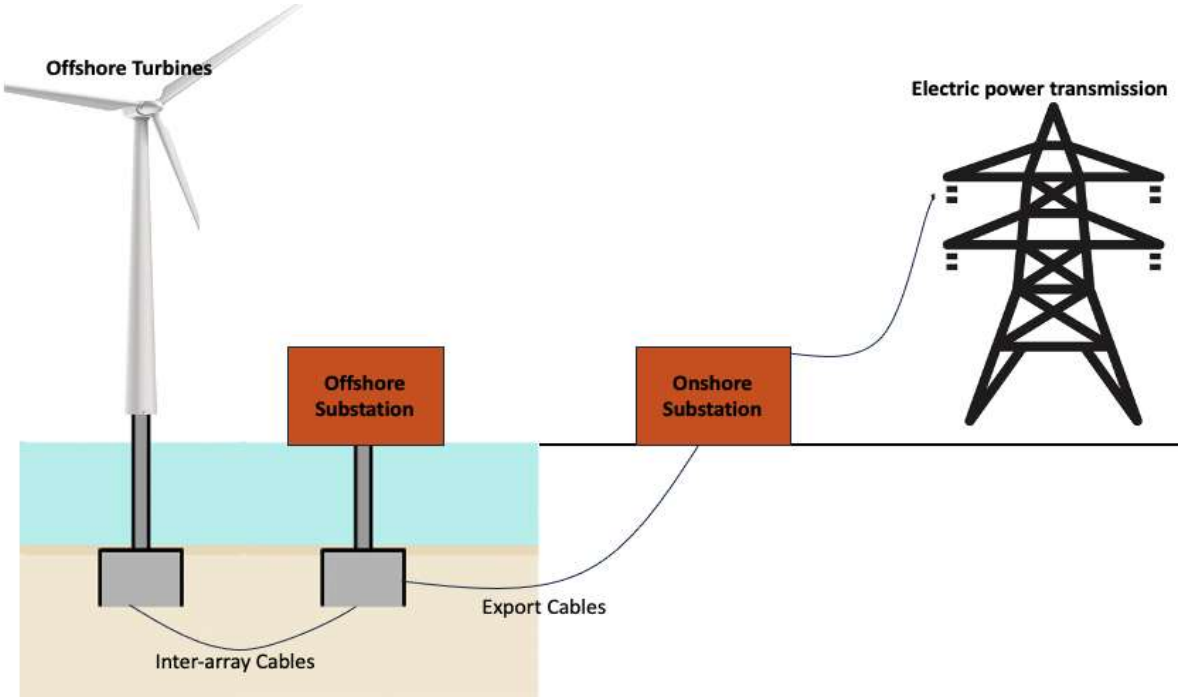

Figure 2. Process of Offshore Wind Farms

An ideal location for an offshore wind project should have strong and consistent wind speeds, appropriate water depths, and easy access to an electricity grid or potential for energy export production, such as hydrogen and ammonia.

The desired generating capacity and site-specific factors, such as wind speeds, determine the number of wind turbines required for an offshore wind farm. For instance, an offshore wind farm of 1 GW that uses current technologies may need between 60 and 100 turbines. These turbines are connected via subsea cables to offshore electrical substations that regulate current and boost voltage, enabling the generated electricity to be exported to onshore grid connection infrastructure through a high-voltage export cable [32].

Types of Offshore Wind Technologies

The wind energy sector has experienced remarkable technological progress in recent years, particularly in terms of the size and generation capacity of wind turbines. These advancements have significantly increased the efficiency and reliability of wind energy production, making it a more competitive and cost-effective alternative to traditional fossil fuels. The development of larger wind turbines with higher capacity has also allowed wind farms to generate more energy per unit of land and offshore space, leading to an increased demand for wind energy worldwide. This has spurred further innovation and investment in the industry, and many experts believe that wind energy will be crucial to the transition to a low-carbon economy.

The capacity of wind turbines has seen an upward trend over the years. In 1985, the average wind turbine had a rated capacity of 0.05 MW and a rotor diameter of 15 meters. Today, newly established wind power projects utilize wind turbines with much higher capacities, ranging from 3-4 MW onshore to 8-12 MW offshore [33].

The evolution of wind turbines, as seen in terms of their size and capacity, is shown in Figure (3). The figure demonstrates that, in the early stages of wind energy technology, wind turbines were of modest size and had low power output, usually measured in kilowatts. With advancements in technology, wind turbines' size and power generation capabilities have grown significantly. In the 1980s, wind turbines were typically 17 meters tall and had a capacity of around 75 kilowatts, or 0.75 megawatts (MW). In recent years, wind turbine technology has advanced rapidly, leading to even larger and more powerful machines. Today, wind turbines with capacities of several megawatts are common, and there are even wind turbines with capacities exceeding 10 MW. The world record for the largest wind turbine currently belongs to MingYang Smart Energy, a Chinese wind turbine manufacturer [101]. MySE is an offshore hybrid drive wind turbine with a diameter of 242 meters, blades that are 118 meters long, and a swept area of 46,000 square meters. With a nameplate capacity of 16MW, this wind turbine is a testament to the advances in wind energy technology. The technology continues to evolve rapidly, with floating offshore turbine technologies now allowing access to a much wider range of suitable offshore locations for energy generation. The figure and data illustrate that technological advancements have resulted in a growth in both the size and generation capacity of wind turbines [32,34].

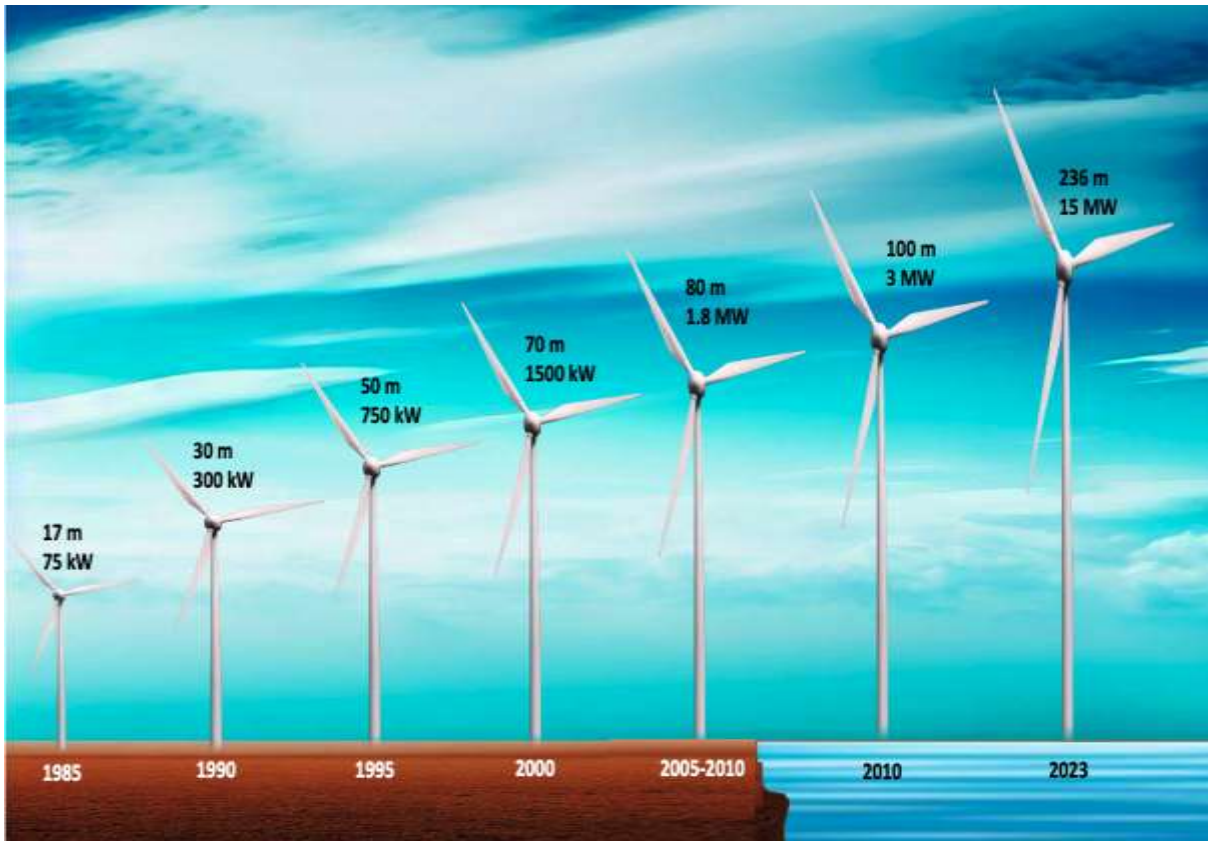

Figure 3. Evolution of Wind Turbine Size

International Breakdown of Offshore Wind Installations

In contrast to the onshore wind industry, the offshore wind industry is in the early stages of expansion. China has an offshore record capacity, which contributes to an increase in offshore

wind capacity. Despite a steady increase in onshore wind capacity, offshore systems are expected to continue to grow in their existing markets, such as Eurozone and China, and in new markets, such as the US, Vietnam, Taiwan, and Japan [35].

Europe has a long history of leadership in offshore wind energy technology and capacity; however, the Asia-Pacific region has recently gained momentum, with China taking the top spot for new installed capacity from 2019.

According to 2021 data, the total worldwide capacity of offshore wind energy installations was 57.2 GW, with China accounting for 48% of the installations, followed by the UK with 22%, Germany with 13%, Netherlands with 5%, Denmark with 4%, and the remaining 7% spread across the rest of the world [10]. Figure (4) provides an overview of the global distribution of offshore wind installations by country, showing the leading countries and their respective capacities [36].

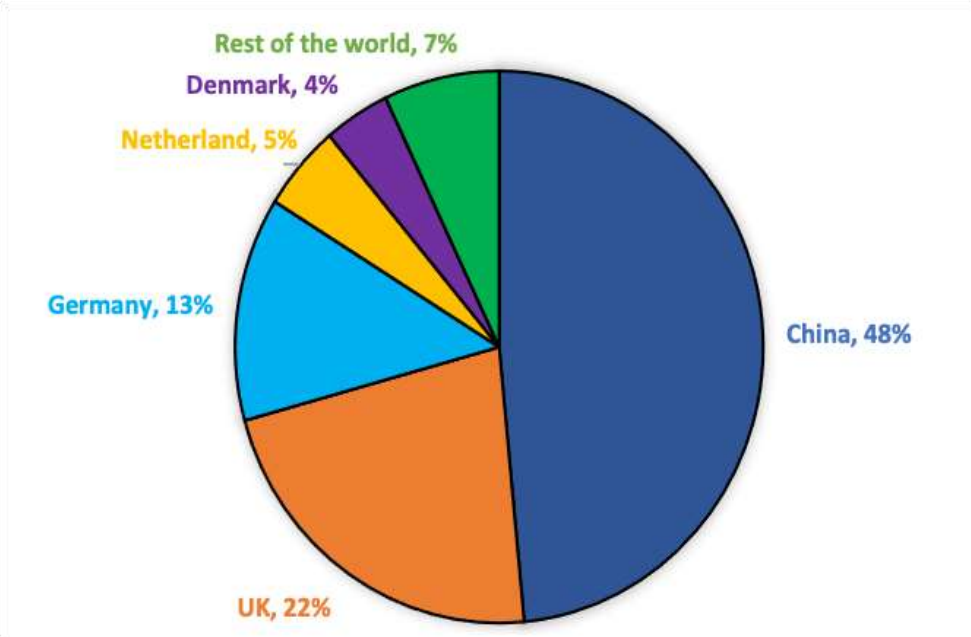

Figure 4. Distribution of Offshore Wind Installations

As depicted in Figure (4), China is at the forefront of offshore wind energy utilization globally. Europe, on the other hand, follows China with a considerable number of countries utilizing this technology. This highlights the fact that the APAC region lags behind in the adoption of offshore wind energy.

Wave Technologies

Ocean waves are generated by the wind's effect on the ocean's surface, which is caused by atmospheric disturbance from the sun's radiation [37]. Ocean waves are a vast source of energy, with an estimated potential of 8000 to 80,000 TW/year. Each wave crest holds an energy density of 10 to 50 kW/m [38].

Ocean wave energy can be used to generate electricity through Wave Energy Converters (WECs) that capture the motion of ocean waves and convert it into mechanical or electrical

energy, which can then be used to power homes and businesses. WECs can be deployed in various locations, including offshore, nearshore, and shore-based, and are designed to be modular and deployed in arrays for optimal energy capture and scalability. The diversity of wave conditions in different regions of the world has led to the development of a wide range of WECs, with various designs and stages of research and development.

Types of wave energy converters

There are different types of marine wave energy technologies. Each type of technology has its own unique features, advantages, and limitations, and the best technology for a particular location and application will depend on factors such as the size and strength of the waves, the location and depth of the ocean, and the technical and economic requirements of the project. Some of the most common types of wave energy technologies include [39-42]:

1. Point Absorbers – A Point Absorber is a floating device designed to harness energy from ocean waves. It absorbs energy from all directions through its movements at or near the water's surface. The device consists of a buoyant top that moves relative to the base in response to the motion of the waves. This movement is then converted into electrical power through a power take-off system, which can take several forms depending on the specific configuration of the displacers and reactors. Point absorbers are designed to be modular and can be deployed in arrays, making them a scalable and efficient means of capturing energy from ocean waves.
2. Overtopping Devices – This type of wave energy conversion technology works by capturing the energy of ocean waves and converting it into potential energy in a water reservoir. Essentially, they act as a pump, using the energy of the waves to pump seawater into a reservoir, where it is stored until it can be used to generate electricity.
3. Oscillating Water Column (OWC) Technology – This type of wave energy conversion technology is a partially submerged enclosed structure that captures energy from incoming ocean waves. This device is typically positioned on or near rocks or cliffs close to deep sea bottoms. The top of the structure above the water is filled with air, which funnels the waves into the bottom of the structure. The movement of the waves causes the water column to rise and fall, changing the air pressure at the top of the structure. This movement drives air through a connected air turbine, converting the energy from the wave motion into electricity.
4. Oscillating wave surge converters (OWSC) – OWSCs capture the energy from the rise and fall of ocean waves to generate electricity. This is achieved by capturing the surge of water created by the waves, which drives a piston or turbine. OWSCs are usually located in shallow waters near the shoreline and can be placed on the seabed or float on the surface of the water.
5. Attenuator – An attenuator is a type of wave energy conversion technology that captures energy from the movement of ocean waves. It consists of a floating device that runs parallel to the direction of the waves and captures energy as it moves with the waves. As

the waves pass them, the relative motion of the two arms generates energy that can be converted into electricity.

6. Bulge wave technology – Bulge wave technology utilizes a rubber tube filled with water, anchored to the ocean floor and facing incoming waves. Water enters the tube from the rear, and as waves pass by, they cause pressure fluctuations along the length of the tube, forming a 'bulge.' This bulge moves through the tube, accumulating energy that can power a standard low-head turbine situated at the front of the tube. Finally, the water exits the tube and returns to the ocean.

Barriers

Challenges impeding the widespread adoption of marine wave energy technologies include [43]:

- Seasonal variations – Sea conditions are inherently variable, with waves and currents changing throughout the year due to seasonal patterns and other factors. This inconsistency in the marine environment creates challenges when designing Wave Energy Converters (WECs). Engineers and developers must account for a wide range of operating conditions to ensure that WECs can adapt and maintain efficiency in the face of these fluctuations. Balancing cost, durability, and performance in ever-changing conditions is a significant obstacle to successfully implementing wave energy technologies.
- Challenges of Long Wave Periods – Large wave periods can present significant challenges for WEC systems. Many types of WECs rely on resonance to capture energy efficiently, which requires the device's natural frequency to align with the frequency of the incoming ocean waves. In locations with high-energy waves, such as the southern shores of Australia, the wave period is typically longer, which means that larger devices with greater masses are required to achieve resonance.
- Maintenance and Reliability – Marine wave systems must be able to operate reliably for many years in a harsh and corrosive marine environment. This requires robust and reliable components, as well as effective maintenance and repair strategies, to ensure the long-term performance of the systems.

International Breakdown of Wave Energy Technologies

The deployment of wave energy technologies is still in its early stages, and currently, there are only a limited number of countries that have established wave farms or are in the process of installing them. The reasons behind this limited adoption could be a combination of determinants such as lack of investment, technological challenges, and regulatory hurdles. These countries include Portugal, the UK, Australia, and the United States, while Russia and Italy have also shown potential interest in exploring wave energy as a renewable energy source [44].

The UK has a long history of wave energy development, dating back to the 1970s. Currently, there are active wave energy projects in Scotland, England, and Wales, showcasing the

country's commitment to harnessing the power of the ocean for sustainable energy generation. The UK has a significant wave resource and a supportive policy framework, making it a favourable location for wave energy development [45].

Tidal Technologies

Tidal energy is a form of renewable energy that captures the power of ocean tides to produce electricity. It is regarded as a dependable and predictable form of renewable energy, as tides are influenced by the stable and foreseeable gravitational pull of the moon and the sun. Tidal energy primarily consists of two types: tidal stream energy and tidal barrage energy.

Technology

Tidal energy operates in various ways, depending on the type of system employed. The three primary categories of tidal energy systems are described below [46-47]:

1- Tidal Stream Turbines – Tidal stream turbines are underwater turbines that are placed in areas with strong tidal currents to generate electricity. They generate electricity as the water flows past them, much like wind turbines generate electricity from the wind. They work by harnessing the energy from the flow of water, much like wind turbines harness the energy from the flow of air.

2- Tidal stream turbines are typically composed of a rotor, a generator, and a nacelle. The rotor consists of one or more blades that rotate as the water flows past them, which drives the generator to produce electricity. The nacelle is the housing that contains the generator, gearbox, and other components.

   Tidal stream turbines are typically placed in shallow waters, where the tidal currents are strongest, to maximize energy production. They are usually positioned on the seabed but can also be suspended from floating platforms. The turbines are designed to rotate slowly, which helps to minimize the risk of harm to marine life.

   Tidal stream turbines are considered to be a more environmentally friendly form of tidal energy compared to tidal barrages, as they do not require the construction of large structures that can impact local ecosystems. Additionally, the underwater environment can be challenging, and the turbines must be designed to withstand harsh conditions, such as strong currents, corrosive saltwater, and changes in water pressure.

   In spite of these challenges, tidal stream turbines hold the potential to contribute substantially to renewable energy production, and their advancement is integral to many nations' efforts toward a sustainable energy transition. As technology progresses, tidal stream turbines are expected to play an increasingly vital role in the worldwide energy landscape, addressing the rising demand for clean, dependable, and renewable energy sources.

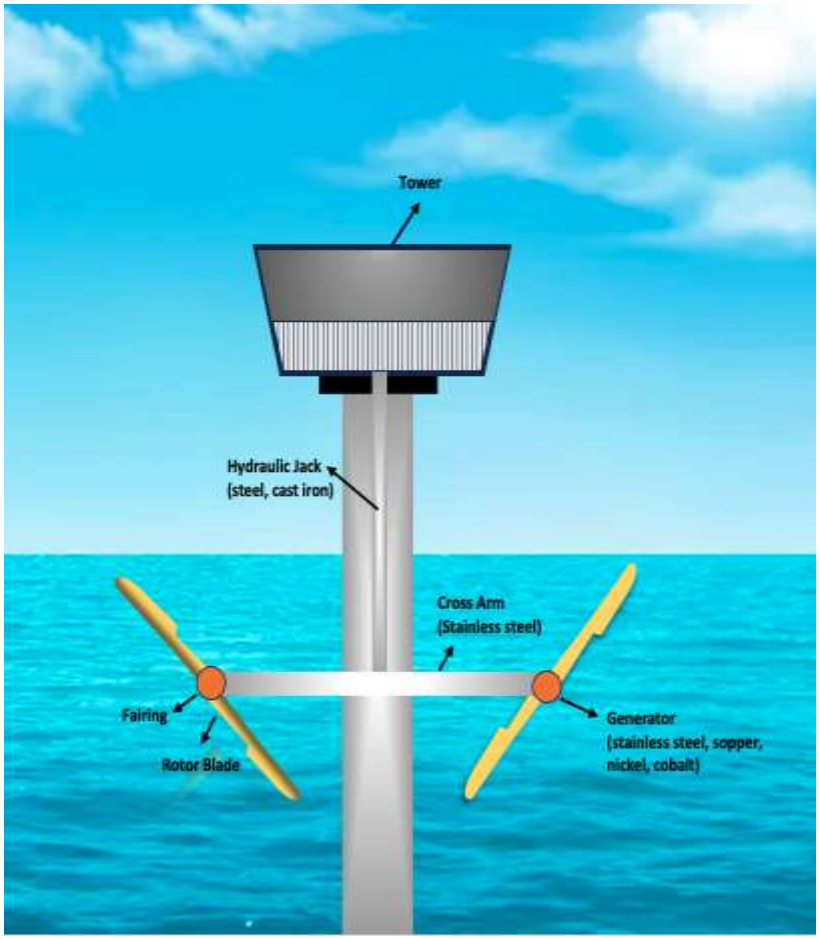

Figure 5. Tidal Power Turbine

3- Tidal Barrage Technology – It is another type of tidal energy generator that involves the construction of a dam-like structure across a tidal estuary, called a barrage, to generate electricity from the rise and fall of tides. Tidal barrages are structures built across tidal rivers, bays, or estuaries. Tidal barrages are essentially large-scale hydropower systems that use the tidal difference in water levels to drive turbines and generate electricity.

A tidal barrage typically consists of a dam-like structure that spans the tidal estuary, with turbines placed in openings in the structure. As the tide comes in and goes out, the water level on either side of the barrage changes, creating a difference in water pressure. This pressure difference drives the turbines, which generate electricity.

There are also some challenges associated with tidal barrage technology. One of the biggest challenges is the high upfront cost of building tidal barrage projects. Compared to a single turbine, the construction of a tidal barrage requires a significantly higher investment. Additionally, tidal barrages can have significant impacts on local ecosystems, as they can alter tidal patterns and disrupt local ecosystems.

A barrage system can have a significant environmental impact. The tidal range area is significantly disrupted, and alterations in water levels within the tidal lagoon could adversely affect plant and animal life. A decrease in salinity inside the tidal lagoon may lead to changes in the organisms inhabiting the area. Similar to river dams, fish may be obstructed from entering or leaving the tidal lagoon. Barrage turbines operate at high

speeds, posing a risk to marine animals that could be caught in the blades. Additionally, with limited food sources, birds may be forced to seek alternative migration destinations.

4- Tidal Lagoon Technology – The last category of tidal energy systems involves the creation of tidal lagoons. Tidal lagoons are artificial structures that are built in shallow coastal waters to generate electricity from the rise and fall of tides. Tidal lagoons use the difference in water levels created by the tides to drive turbines and generate electricity.

   A tidal lagoon typically consists of a partially enclosed body of water that is surrounded by a man-made barrier, such as a breakwater or seawall. The barrier creates a lagoon that is partially isolated from the open ocean, allowing the tide to flow in and out. The turbines are placed in openings in the barrier, and as the tide changes, the difference in water level drives the turbines and generates electricity.

   Tidal lagoons offer several advantages as a source of renewable energy. The biggest advantage is that they can be built along the natural coastline, which can reduce the environmental impact compared to other forms of tidal energy. Additionally, tidal lagoons can provide other benefits, such as flood control and water management.

   However, there are also some challenges associated with tidal lagoon technology. One of the biggest challenges is the high upfront cost of building tidal lagoons, as they often require significant infrastructure investments. Additionally, tidal lagoons can also have significant impacts on local ecosystems, as they can alter tidal patterns and disrupt local ecosystems.

Barriers and Drivers

Tidal energy is a source of renewable energy that captures the kinetic energy of ocean tides and converts it into electrical power. Here are some potential advantages of tidal energy [48-50]:

- Abundance – Given that around two-thirds of the Earth's surface is covered by water, there is significant potential to generate tidal energy on a large scale.
- Clean and Renewable – Tidal energy is a clean and renewable energy source that does not produce any greenhouse gas emissions or air pollution. It is therefore considered a more sustainable alternative to fossil fuels.
- Predictable and Reliable Source – Tidal energy is a highly predictable and reliable source of renewable energy. In contrast to solar and wind power, which depend on uncertain weather conditions, tidal power is derived from the predictable ebb and flow of ocean tides that are generated by the gravitational attraction between the Earth, moon, and sun. This means that the ocean will continue to generate motion and energy as long as the Earth rotates and the moon orbits. Tides will always be present in the same way that the sun shines in the sky. As a result, tidal power is easier to plan for and integrate into the electrical grid, making it a more stable and consistent source of energy. By strategically placing tidal energy systems in locations where the ocean's currents are strongest, we can harness the full potential of this predictable and reliable energy source, providing a sustainable and clean energy solution for our future energy needs.

- Long Lifespan – Tidal energy systems have a long lifespan, making them a more sustainable option than other sources requiring frequent replacement. Tidal turbines, for example, can operate for up to 25 years or more with proper maintenance. In contrast, solar or wind farms may require replacement after a shorter period of time. For instance, tidal barrages are concrete structures that can last as long as 100 years. A prime example is La Rance in France, which has been in operation since 1966 and continues to produce clean energy to this day. This longevity makes tidal energy a reliable and cost-effective solution for meeting our energy needs.
- High Energy Density – Tidal energy has a high energy density, meaning that a relatively small tidal turbine can generate a significant amount of power compared to other renewable sources. Water's high density compared to air also means that tidal energy systems waste little energy. Additionally, the high density of water makes it easier to generate electricity, enabling the production of significant amounts of energy even with minimal movement and speed.
- Low operational and maintenance costs are a key advantage of tidal energy. Because tidal turbines have fewer moving parts and can operate for long periods without major maintenance, the costs associated with their operation and upkeep are relatively low. This makes tidal energy an attractive and cost-effective option for meeting our energy needs while also reducing our carbon footprint.

However, there are also some challenges associated with tidal energy which are mentioned below:

- High Capital Costs – Building and installing tidal energy systems can be expensive due to the need for specialized equipment and installation in harsh marine environments.
- Environmental Impact – Tidal energy projects can have an impact on the local marine environment, including changes to the water flow and the behavior of marine animals.
- Limited Availability – Tidal energy is only viable in areas with strong tidal currents, which limits the number of suitable locations for tidal energy projects.
- Interference with Navigation – Tidal energy systems can interfere with shipping and navigation channels, which can lead to conflicts with other marine users.
- Maintenance Challenges – Tidal turbines are subject to wear and tear from the harsh marine environment, making maintenance and repair more challenging and costly than other energy systems.
- Despite its potential, tidal energy technology currently faces challenges with cost-effectiveness. Further technological advancements are needed to make tidal energy commercially viable and competitive with other energy sources.
- A requirement for technology development – Despite its potential, tidal energy technology currently faces challenges with cost-effectiveness. Further technological advancements are needed to make tidal energy commercially viable and competitive with other sources of energy.

- Distance Transmission Challenges – A potential disadvantage of tidal energy is that the locations where it can be produced are often far from the places where it is consumed. As a result, transmitting the energy over long distances can be expensive and challenging, which may increase the overall cost of tidal energy projects.

Recently, tidal energy has garnered increased attention, with numerous large-scale tidal energy projects being constructed or in development globally. As technology progresses, tidal energy is expected to become a more prominent player in the worldwide energy landscape, contributing to the rising demand for clean, dependable, and renewable energy sources.

International Breakdown of Tidal Installations

Tidal energy production is still in the early stages of development, with a relatively small amount of power generated thus far. Currently, only a few commercial-scale tidal power plants are operating worldwide.

Tidal barrage (or tidal range) technology still dominates deployed capacity. More than 98% of the total combined capacity that is currently operational, or 521.5 MW, is tidal barrage technology. This comprises mainly three large projects – a 254 MW plant in the Republic of Korea (which came online in 2011), a 240 MW plant in France (1966) and a 20 MW station in Canada (1984) – and the remaining 7.5 MW is split between two plants in China (4.1 MW) and the Russian Federation (3.4 MW). Despite the dominance of this technology, no tidal barrage power plants of relevant scale have been developed in almost 10 years, and there is relatively low resource potential to be explored. However, a pipeline of more than 2.5 gigawatts (GW) in planned projects worldwide indicates that the market still sees opportunities [51].

The Sihwa Lake Tidal Power Station in South Korea is currently the largest tidal power plant in the world, with a capacity to generate up to 254 megawatts of electricity. La Rance is the second-largest operating tidal generator capable of 240 MW. The La Rance Tidal Power Station, located in Brittany, France, was the first tidal energy generator in the world. It was built in the 1960s and began generating electricity on the 26th of November 1966. The power station operates as a tidal barrage, using the tidal flow of the Rance River to generate electricity. With a capacity of 240 megawatts, it can power around 300,000 homes. Today, Électricité de France (EDF) owns and operates La Rance Tidal Power Station. It remains one of the largest tidal power stations in the world, ranking second in installed capacity. The plant's 24 turbines have the capacity to generate up to 240 MW of power, equivalent to the power consumption of Rennes city in France. The plant can produce up to 600 million kilowatt-hours of electricity in a year [52-54].

Despite the United States having significant potential for tidal energy, there are currently no commercially operating tidal energy power plants in the country. However, several demonstration projects are in various stages of development. Two locations with strong potential for tidal power in the US are the Cook Inlet in Alaska, which has the second-highest tidal range in North America, and several locations in Maine. Smaller tidal power plants are also in operation in countries, including the United Kingdom, the Netherlands, China, and Russia [55].

Ocean Thermal Energy Conversion

Ocean Thermal Energy Conversion (OTEC) is a power generation method utilizing ocean thermal differences to generate sustainable, green, and reliable electricity 24 hours a day, 365 days a year. This technology harnesses the temperature difference between deep cold seawater and warm tropical surface waters to produce electricity. The process involves pumping large quantities of deep cold and surface seawater to run a power cycle, providing a clean and sustainable source of firm power (24/7) with the potential to generate massive amounts of energy [102-103].

Technologies:

Currently, there are four types of OTEC systems, including [56-57]:

- Open-cycle OTEC – An open-cycle OTEC system generates electricity by utilizing warm seawater as the driving fluid in a heat exchanger. The warm seawater is pumped into a low-pressure chamber, lowering its boiling point and converting it into steam. This steam drives a low-pressure turbine and generator to produce electricity. Cold deep seawater is then used to condense the steam back into liquid form, which is then safely discharged into the ocean. One major advantage of this system is its ability to produce fresh drinking water for local communities, as the warm seawater is evaporated into steam and desalinated. However, it also presents some challenges, such as the need for careful sealing to prevent atmospheric air from destroying the vacuum.

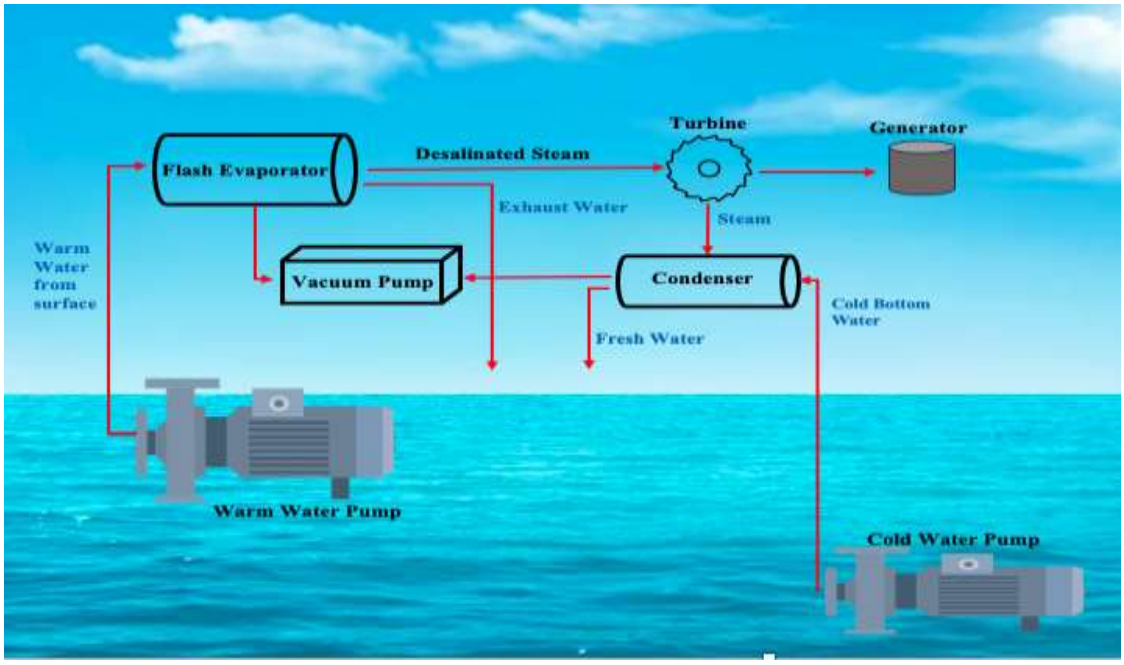

Figure 6. Open-cycle OTEC

- Closed-cycle OTEC – This system employs a gas or liquid working liquid, like ammonia or propane, with a low boiling point, in a closed and sealed circuit to rotate a turbine. The warm surface ocean water is pumped into an evaporator, where the liquid ammonia is pressurized and boils, creating vapor that drives a generator. The cold deep ocean water

is pumped through the other side of the heat exchanger, causing the ammonia vapor to condense back into a liquid form. A pump pressures this liquid again, and the cycle repeats.

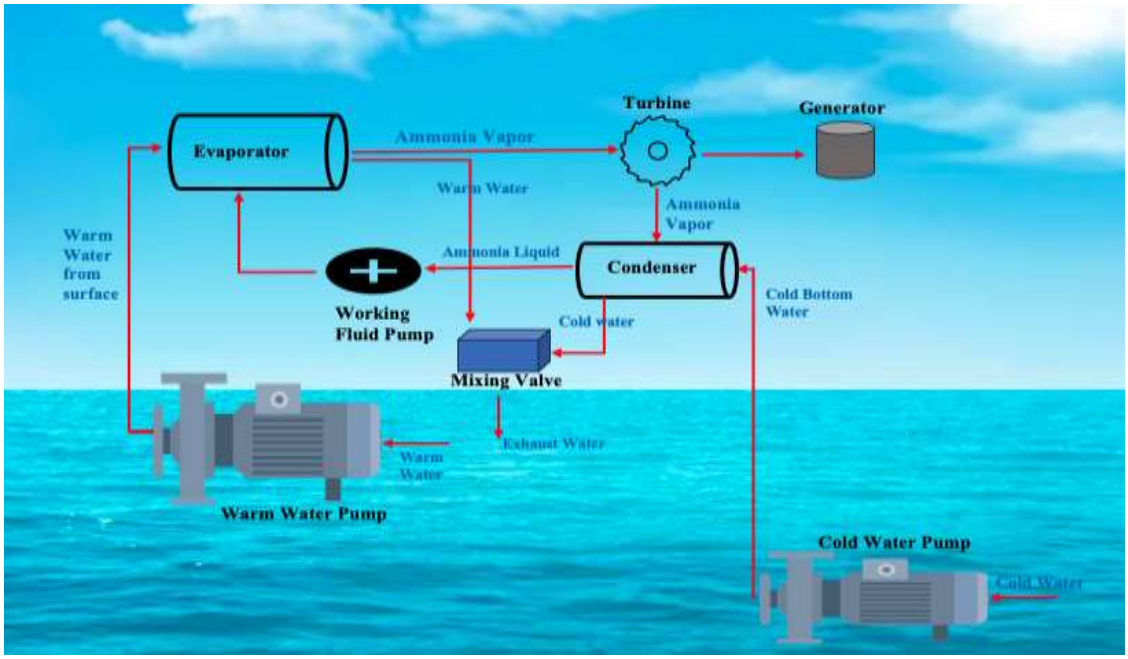

Figure 7. Closed cycle OTEC

- Hybrid System – A Hybrid OTEC system combines the benefits of both open-cycle and closed-cycle systems. In this process, the steam generated from the flash evaporation of warm seawater in an open-cycle system is then utilized as heat to drive a closed-cycle system. The warm seawater is first flash evaporated, similar to the open-cycle system, and then cooled with the cold-water discharge. This results in the generation of electricity in a closed-cycle system, as well as the production of fresh water.

Advantages

OTEC systems offer several advantages as a renewable energy source [58]:

- Clean energy – OTEC systems utilize the ocean's vast thermal energy, offering a nearly inexhaustible, renewable energy source. Furthermore, these systems generate significantly fewer greenhouse gas emissions and other pollutants compared to power generation methods reliant on fossil fuels. This makes OTEC an environmentally friendly and sustainable energy option.
- Reliable – Unlike solar power plants that cease to produce energy during night-time and wind turbines that require specific wind conditions to generate electricity, OTEC systems can consistently produce energy around the clock, regardless of the time of day or weather conditions. This makes OTEC a reliable and continuous source of renewable energy.
- Environmentally friendly – Ocean thermal energy plants, located offshore and away from human settlements, minimize interaction between dense populations and the energy

facility. As these plants do not require fossil fuels for production, they contribute to a cleaner environment and atmosphere, promoting the adoption of sustainable energy sources.

- Freshwater production – OTEC systems can be designed to produce fresh drinking water as a by-product of the electricity generation process, potentially benefiting water-scarce regions.

Disadvantages

A few disadvantages of OTEC include [58]:

- Location Limitations: Similar to other energy generation methods, ocean thermal energy harnessing is limited to specific locations. This can be a disadvantage for countries without a coastline.
- High Initial Costs: The cost of procuring and installing the necessary equipment for OTEC systems is relatively high. In a time when living standards are high in many countries, the establishment of ocean thermal energy plants might be limited to certain nations. Additionally, it may require a large number of professionals to set up the plant.
- Navigation Interference: While ocean thermal plants may appear to float on the water, they have extensive and massive structures beneath the surface. Large ships may face difficulties navigating near these floating facilities, leading to potential disruptions in maritime transport.
- Minimal Temperature Difference: The temperature difference between surface water and deep water can be quite small, resulting in moderately efficient electricity generation. This may prove to be very costly for small electricity businesses that rely on this form of energy production, as it might not yield the desired efficiency.
- Large Turbines and Expensive Fluids: Ocean thermal energy plants may require sizable turbines due to the low pressure in the boiling process using propene. This presents a disadvantage as the cost of such large turbines can be prohibitively expensive, making the overall project financially challenging.
- Impact on Marine Life: Ocean thermal energy plants involve pipes extending to the deepest parts of the ocean, which can potentially disrupt marine life. Additionally, small marine organisms may be inadvertently drawn into the pipes due to the pumping action of the water.

Ocean Current Technologies

Ocean current energy is a type of marine renewable energy that involves harnessing the kinetic energy of ocean currents to generate electricity. There are several factors that contribute to ocean currents, such as surface winds, temperature gradients, rotation of the earth, the topography of the ocean floor, and salinity gradients, and can flow for thousands of kilometres across the world's oceans [59].

The technology used to harness energy from ocean currents typically involves underwater turbines or similar devices, which are similar in design to those used for extracting energy from tidal currents. However, there are differences between tidal technologies and current technologies.

The main difference between tidal and current energy technologies lies in the energy source they harness. Tidal energy technologies take advantage of the gravitational forces of the moon and sun on the Earth's tides, while marine current technologies harness the kinetic energy of ocean currents, which are driven by factors like surface winds, temperature gradients, and salinity gradients. Another critical difference between the two technologies is their predictability. Tidal energy is more predictable than ocean current energy, as the timing and amplitude of the tides can be accurately predicted many years in advance. In contrast, the strength and direction of ocean currents can vary considerably over time and depend on factors, including weather patterns.

Tidal energy systems, such as tidal barrages or tidal turbines, can also generate more power than ocean current technologies due to the greater force of the tides. However, tidal energy systems can significantly impact the marine environment more than marine current technologies, as they can affect the natural movement of water and marine life.

Overall, both tidal and current technologies possess the potential to perform a crucial role in the transition to a sustainable and renewable energy future, and ongoing research and development in both fields will be critical to unlocking their full potential.

Technologies:

The following are some of the various types of ocean current technologies available:

1- Horizontal Axis Current Turbine (HACT) – A type of underwater turbine designed to generate electricity from ocean currents. They consist of a rotor that is mounted on a horizontal axis and is driven by the flow of the ocean current. The rotor is connected to a generator that converts the kinetic energy of the rotating blades into electrical energy. HACTs are similar in design to wind turbines, except that they are designed to operate in underwater environments and are optimized to take advantage of the unique characteristics of ocean currents [60-62].

2- Vertical Axis Current Turbine (VACT) – VACTs are similar in design to HACTs. The main difference is that they have a vertical axis, which allows them to operate in currents flowing in any direction. This makes VACTs more flexible and adaptable to a broader range of ocean current conditions compared to HACTs [63-64].

3- Ocean Current Energy Conversion Systems (OCECs) – A marine current energy system converts the kinetic energy of ocean currents into electricity. The movement of the ocean water drives the rotation of the turbine's rotor, which in turn powers a generator to produce electricity. The principle behind the Ocean Current Energy Conversion System (OCECS) is similar to that of a wind energy conversion system (WECS). However, instead of harnessing the energy from wind, the OCECS harnesses the energy from ocean currents [65].

4- Oscillating Hydrofoil (OH) – This technology utilizes ocean currents to generate electricity. They consist of a flat blade-like hydrofoil that is mounted on a pivot and moves in a back-and-forth motion due to the flow of the ocean current. The motion of

the hydrofoil drives a generator that converts the kinetic energy of the oscillating motion into electrical energy [66].

Barriers and Drivers

Ocean current technologies present both pros and cons. The advantages include:

1. Ocean current technologies utilize renewable energy sources, reducing dependence on non-renewable sources.
2. Consistent energy source
3. Compared to other forms of energy generation, current technologies have a relatively low environmental impact.

Disadvantages [66]:

1. High deployment costs – Investing in current energy technologies can be costly, making it a challenging investment for countries.
2. High Maintenance and repair cost – Due to the harsh underwater environment, maintaining and repairing ocean current technologies can be difficult and expensive.
3. Impact on Marine Life and Ocean-based Activities – Interference with marine life is one of the potential disadvantages of current technologies. Marine life can be impacted by the physical presence of ocean current turbines and the underwater noise generated by the turbines. In addition, these technologies can also interfere with other ocean-based activities, such as fishing and shipping.
4. Fluctuations in energy output – The energy output of ocean current technologies can fluctuate depending on changes in ocean currents, which can result in fluctuations in the amount of energy generated.
5. Corrosion resistance – Corrosion resistance is a potential disadvantage of marine current generators due to the harsh underwater environment. The saltwater and corrosive agents in the ocean can cause damage to the materials used in ocean current technologies, reducing their lifespan and efficiency.

Despite these challenges, ocean current technologies have the potential to play an essential role in the future of renewable energy.

Salinity Gradients/Osmotic Energy Technologies

Salinity gradient energy technologies harness the energy generated by the difference in salt concentration between freshwater and seawater. This difference creates a chemical pressure differential, known as osmotic pressure, which can be harnessed to generate electricity using semi-permeable membranes. Due to its high salt concentration, seawater has a greater osmotic pressure than freshwater. The two main types of these technologies are Reverse Electrodialysis (RED) and Pressure-Retarded Osmosis (PRO), and they can be used in deltas or fjords to drive turbines and produce power [67].

Type of Technologies:

- Pressure Retarded Osmosis (PRO) – Generates electricity by utilizing the osmotic pressure difference between freshwater and seawater through reverse electrodialysis or pressure-retarded osmosis, which drives a turbine and converts the chemical pressure differential into electrical energy. Similarity to reverse electrodialysis technologies, PRO technologies take advantage of the difference in salt concentration between freshwater and saltwater to generate energy.
- Reverse Electrodialysis (RED) – Such kind of technology utilises anion and cation exchange membranes in order to mix water bodies with different salinities in order to produce electricity. By feeding saltwater and freshwater through these membranes, ions are transported in opposing directions, creating poles like a battery.

Advantages and Disadvantages:

Salinity gradients energy technologies have several advantages, including:

- Salinity gradient technology is a sustainable and renewable source of electricity generation.
- Salinity gradient technology generates electricity in a sustainable and renewable manner without emitting harmful greenhouse gases or pollutants, making it a clean and environmentally friendly energy source.
- Salinity gradient technology operates continuously and consistently making it a reliable source of energy that can generate electricity on a 24-hour basis, seven days a week.

However, there are some advantages to these technologies. The main disadvantage of salinity gradient technologies is the potential impact on the physical and biological environment. Mixing freshwater and seawater can alter the balance of the ecosystem and harm organisms at the intake or release points. Additionally, there may be concerns about diverting freshwater resources for power generation, especially in areas with water scarcity. More research is needed to understand this technology's potential environmental and socio-economic impacts fully [67-68].

2.2. Marine Renewable Energy Technologies in Asia Pacific Region

The Asia Pacific region has seen significant growth in the development and deployment of marine renewable energy technologies in recent years. Some of the marine renewable technologies that are being applied or under development in the region based on countries include:

China

Offshore Wind Energy Operations

China is the global leader in offshore wind from a technology and generation capacity perspective. As outlined in the Global Wind Energy Council (GWEC) report in 2020, the Asia Pacific region is predicted to play a leading role in the rapidly expanding offshore wind energy

market. Based on the report, the region's global offshore wind market share will increase from 24% in 2019 to 42% by 2025. Currently, China dominates the Asian offshore wind market, with a market share of over 70%. However, its market share is expected to drop in the long-term outlook period as more utility-scale offshore wind projects are commissioned in emerging markets such as Taiwan, Japan, South Korea, and Vietnam. The report indicates that China, Taiwan, South Korea, Japan, and Vietnam will be the top five markets for new installations in the region over the next decade. Predicted installations in these countries are estimated to be 52 GW, 10.5 GW, 7.9 GW, 7.4 GW, and 5.2 GW, respectively, which highlights the immense potential for growth in the offshore wind energy market in the region [69].

In 2021, the global wind energy market saw significant growth, with a total installed capacity of 830 GW. Out of this capacity, the majority, 93%, was made up of onshore wind systems, totalling 774.3 GW, while the remaining 7% consisted of offshore wind farms, with a capacity of 55.7 GW.

As reported by S&P Global, IHS Markit's Petrodata Fieldsbase currently lists 695 offshore wind projects worldwide. APAC hosts 46% of all offshore wind projects globally, of which 24% are in mainland China. The Chinese offshore wind industry leads the region, accounting for 52% of APAC's projects.

According to the latest Global Wind Report, 2022 saw a significant growth in wind installations, particularly for the fast-growing offshore wind sector, with a total of 94 GW of wind energy capacity installed globally, including 21 GW of offshore wind [36].

Regions that have already developed or are in the process of developing offshore wind in China are [70]:

- Guangdong
- Guangxi
- Hainan
- Hong Kong
- Jiangsu
- Shanghai
- Zhejiang
- Fujian
- Liaoning
- Tianjin
- Hebei
- Shandong

China has 403 offshore wind farm projects, with 124 currently operating and 6 already generating electricity due to the sufficient progress in construction. In addition, 14 projects are in the building phase, while another 14 have either been granted consent or have applied for it [71]. A list of some fully commissioned offshore wind plants with a capacity of more than 100 MW is presented in Table (2):

Table 2. Fully commissioned offshore wind farms in China

Name	Capacity (MW)	Region	Commenced Date
CGN Shanwei Jiazi II	900	Guangdong, Shanwei	Dec-2022
CGN Shanwei Jiazi I	503.1	Guangdong, Shanwei	Nov-2022
Shenquan - phase 2	502	Guangdong, Jieyang	Dec-2022
Shandong Energy Bozhong A	501	Dongying	Dec-2022
CGN Shanwei Jiazi II	403	Guangdong, Shanwei	Dec-2022
CTGNE Yangjiang Shapa - phase II	400	Guangdong, Yangjiang	Nov-2021
Rudong H10	400	Jiangsu, Nantong, Rudong	Dec-2021
Rudong H6	400	Jiangsu, Nantong, Rudong	Dec-2021
SPIC Rudong H7	400	Jiangsu, Nantong, Rudong	Dec-2021
SPIC Rudong H4	400	Jiangsu, Nantong, Rudong	Nov-2021
SPIC Binhai North H2	400	Jiangsu, Yancheng, Binhai	Jun-2018
Cangnan #4	400	Zhejiang, Wenzhou, Cangnan	Sep-2022
Zheneng Shengsi 2	400	Zhejiang, Zhoushan, Shengsi	Nov-2021
Rudong H2	350	Jiangsu, Nantong, Rudong	Dec-2021
Shenquan-phase 1	315.5	Guangdong, Jieyang	Nov-2021
Longyuan Jiangsu Dafeng (H4)	302.4	Jiangsu, Yancheng, Dafeng	Dec-2021
SPIC Jiangsu Dafeng H3	302.4	Jiangsu, Yancheng, Dafeng	Dec-2018
Guohua Dongtai 4 H2	302.4	Jiangsu, Yancheng, Dongtai	Dec-2019
Zhugensha H2	302	Jiangsu, Yancheng, Dongtai	Oct-2021
Huaneng Sheyang H1	301.5	Jiangsu, Yancheng, Sheyang	Dec-2021
Longyuan Sheyang H2	301.5	Jiangsu, Yancheng, Sheyang	Ap 2021
CECEP Yangjiang Nanpeng Island	300	Guangdong, Yangjiang	Nov-2021
CTGNE Yangjiang Shapa - phase I	300	Guangdong, Yangjiang	Dec-2021
CTGNE Yangjiang Shapa - phase III - A1	300	Guangdong, Yangjiang	Dec-2021
CTGNE Yangjiang Shapa - phase V	300	Guangdong, Yangjiang	Dec-2021
CTGNE Yangjiang Shapa - phase IV	300	Guangdong, Yangjiang	Dec-2021
Zhanjiang Xuwen-South	300	Guangdong, Zhangjiang	Nov-2021
Zhuhai Jinwan	300	Guangdong, Zhuhai	Apr 2021
Laoting Bodhi Island	300	Hebei, Tangshan	Jun-2020
Huaneng Guanyun - phase 1	300	Jiangsu, Lianyungang, Guanyun	Jul-2021
Rudong H8	300	Jiangsu, Nantong, Rudong	Dec-2021
CSIC Jiangsu Rudong H3-1	300	Jiangsu, Nantong, Rudong	Aug-2021
Rudong H5	300	Jiangsu, Nantong, Rudong	Oct-2021
Jiangsu Longyuan Chiang Sand H1 300MW	300	Jiangsu, Nantong, Rudong	Jul-2018
Rudong Demonstration Project - Expansion Project	300	Jiangsu, Nantong, Rudong	Dec-2015
Jiangsu Rudong Jiangjiasha H2	300	Jiangsu, Nantong, Rudong	Dec-2020
SPIC Binhai South H3	300	Jiangsu, Yancheng, Binhai	Jan-2021
Dafeng H6	300	Jiangsu, Yancheng, Dafeng	Dec-2021
CTGNE Jiangsu Dafeng H8-2	300	Jiangsu, Yancheng, Dafeng	Dec-2021
Three Gorges New Energy Jiangsu Dafeng	300	Jiangsu, Yancheng, Dafeng	Oct-2019
Dalian Zhuanghe #3 CTGNE	300	Liaoning, Dalian, Zhuanghe	Nov-2020
Huaneng Dalian Zhuanghe II	300	Liaoning, Dalian, Zhuanghe	Dec-2021
Three Gorges Shandong Changyi Laizhou Bay-phase 1	300	Shandong, Weifang, Changyi	Dec-2022
Zhejiang Jiaxing 2	300	Zhejiang, Zhoushan, Jiaxing	Dec-2021

Zhanjiang Xuwen-North	300	Guangdong, Zhangjiang	Nov-2021
Huadian Fujian Fuqing Haitan Strait	299.2	Fujian, Fuzhou, Fuqing	Nov-2021
Shengsi 5 + 6	282	Zhejiang, Zhoushan, Shengsi	Aug-2021
Guodian Xiangshan 1 - phase 1	254.2	Zhejiang, Ningbo, Xiangshan	Dec-2021
Guodian Zhoushan Putuo District 6 Zone 2	252	Zhejiang, Zhoushan, Putuo	Dec-2021
Qidong H1	250.5	Jiangsu, Nantong, Qidong	Dec-2021
Datang International Shantou Lemen I	245	Guangdong, Shantou	Dec-2021
CGN Pingtan Island	240	Fujian, Fuzhou, Pingtan	Dec-2021
CGN Daishan 4	234	Zhejiang, Zhoushan, Daishan	Dec-2020
Dafeng H5	206.4	Jiangsu, Yancheng, Dafeng	Dec-2021
Fengxian - phase 1	206.4	Shanghai, Fengxian	Dec-2021
Guangdong Yudean Zhanjiang Wailuo-phase 3	206.4	Guangdong, Zhangjiang	Dec-2021
Xiangshui Demonstration	202	Jiangsu, Yancheng, Xiangshui	Jan-2017
Fujian Sanchuan Putian City Flat Bay zone F	200	Fujian, Putian, Xiuyu	Jun-2021
Fujian Sanchuan Shicheng Fishing Port	200	Fujian, Putian, Xiuyu	Jul-2021
Guangdong Yudean Zhanjiang Wailuo-phase 2	200	Guangdong, Zhanjiang, Xuwen	Dec-2021
Rudong H14	200	Jiangsu, Nantong, Rudong	Dec-2020
Longyuan Jiangsu Dafeng (H7)	200	Jiangsu, Yancheng, Dafeng	Jun-2019
Guohua Dongtai 5	200	Jiangsu, Yancheng, Dongtai	Nov-2021
Rudong H15	200	Jiangsu, Nantong, Rudong	Nov-2021
Guangdong Yudean Zhanjiang Wailuo-phase 1	198	Guangdong, Zhanjiang, Xuwen	Dec-2021
Huaneng Rudong 300MW - North	156	Jiangsu, Nantong, Rudong	Sep-2017
Huadian Yuhuan 1 North	154	Zhejiang, Taizhou, Yuhuan	Dec-2021
CGN Rudong Demonstration	152	Jiangsu, Nantong, Rudong	Sep-2016
Rudong H13	150	Jiangsu, Nantong, Rudong	Nov-2021
Huadian Yuhuan 1 South	146	Zhejiang, Taizhou, Yuhuan	Feb-2022
Zhuhai Guishan Demonstration-phase 1	120	Guangdong, Zhuhai, Xiangzhou,	May-2021
Huaneng Dafeng - phase 2	103.5	Jiangsu, Yancheng, Dafeng	May-2020
Sheyang Longyuan South H2-1 expansion	103.5	Jiangsu, Yancheng, Sheyang	Apr-2021
Donghai Bridge Offshore Wind Farm - phase II	102.2	Shanghai	Oct-2015
Shanghai Donghai Bridge I	102	Shanghai	Jun-2010
Shanghai Lingang Demonstration - 2	100.8	Shanghai	Dec-2016
CTGNE Yangjiang Shapa - phase III - A2	100	Guangdong, Yangjiang	Dec-2021
CSIC Jiangsu Rudong H3-2 100MW	100	Jiangsu, Nantong, Rudong	Aug-2021
Shanghai Lingang Demonstration - 1	100	Shanghai	Jul-2019

Wave Technologies

China has been developing and investing in wave power technology as part of its broader efforts to enhance the share of clean energy in the country's energy mix. China has several ongoing research projects and pilot wave energy converter installations along its extensive coastline.

Tidal Technologies

Several pilot projects are underway in this country to harness tidal energy. China has identified significant tidal energy resources in the South China Sea, Yellow Sea and East China Sea. In May 2022, the first solar-tidal photovoltaic power plant began to generate electricity in China.

It is a significant milestone in China's development and construction of a marine renewable energy system. The power plant, located in Wugen Township, Wenling city, has an impressive installed capacity of 100 MW and is owned by China Energy Investment Corporation, a leading energy giant. It establishes a new model for coordinated photovoltaic and tidal power generation, which represents a breakthrough for China in the integrated use of marine energy and multidimensional development of new energy [72].

China has a long history with tidal barrages, dating back to the 1950s. Over the course of seven decades, the country constructed more than 100 small-scale tidal barrages. However, only two of them, Jiangxia and Haixia in Zhejiang province, remain operational today. Most of these installations faced various challenges, including technical difficulties, planning issues, and operational factors, which led to their eventual discontinuation [73].

Jiangxia Tidal Power Station (江厦潮汐电站) is located in the Zhejiang province of China, near the city of Taizhou. It is one of the few operational tidal power stations in the country. The plant was commissioned in 1980 and has a total installed capacity of 3.9 MW, making it one of the largest tidal power stations in the world at the time of its construction. Jiangxia plant is the fourth largest tidal power plant in the world after the Sihwa Lake Tidal Power Plant in Korea, La Rance in France and Annapolis in Canada [74-75].

Australia

Offshore Wind Energy Technologies

Australia possesses numerous locations that could potentially accommodate offshore renewable energy infrastructure. These areas offer promising opportunities for the development and implementation of such technologies. Currently, there are 50 offshore wind farm projects planned in Australia, but none of them are operational, in the process of being connected to generate electricity, or in the construction phase [71]. Below is a list of these projects:

Table 3. List of offshore wind projects in Australia

Name	Status	Capacity (MW)	Region	Start Date
Azure Floating Wind Farm	Early Planning	1000	VIC	
Barwon Floating Wind Farm	Early Planning	1000	VIC	
Bass - 1A Offshore Wind Farm	Early Planning	500	TAS	Dec-2026
Bass - 1B Offshore Wind Farm	Early Planning	500	TAS	Dec-2026
Bass - 2 Offshore Wind Farm	Early Planning	2000	TAS	
Bass Coast North Floating Wind Farm	Early Planning	1000	VIC	
Bass Coast South Floating Wind Farm	Early Planning	1000	VIC	
Bass Strait - Mistral Floating Farm	Early Planning	11000	VIC	
Bass Strait Offshore Wind Farm	Early Planning	4000	VIC	
Blue Marlin Offshore Wind Farm	Early Planning	2000	VIC	Aug-1905
Bunbury Offshore Wind Farm	Early Planning	2000	WA	Jan-2036
Cape Winds Offshore Wind Farm	Early Planning	495	VIC	
Cape Extension Offshore Wind Farm	Early Planning	1600	SA	
Eastern Rise Floating Wind Farm	Early Planning	1700	NSW	
Eden Offshore Wind Farm	Early Planning	2000	NSW	Jan-2036

Gippsland Declared Area Farm	Early Planning	10000	VIC	
Great Eastern Offshore Wind Farm	Early Planning	2500	VIC	
Great Southern Offshore Wind Farm	Early Planning	1500	VIC	Jan-2033
Greater Gippsland Offshore Wind Farm	Early Planning	2085	VIC	Dec-2032
Hunter Coast Floating Wind Farm	Early Planning	1650	NSW	Dec-2033
Illawarra Offshore Wind Farm	Early Planning	2000	NSW	Jan-1931
Indigo Floating Wind Farm	Early Planning	1000	NSW	
Kingston Offshore Wind Farm	Early Planning	600	SA	
Kingston Extension Floating Wind Farm	Early Planning	1000	SA	
Latitude 36 Floating Wind Farm	Early Planning	1000	NSW	
Leeuwin Offshore Wind Farm	Early Planning	3000	WA	
Mid-West Offshore Wind Farm	Early Planning	1100	WA	
Midwest Offshore Wind Farm	Early Planning	3000	WA	Jan-2031
Newcastle Floating Wind Farm	Early Planning	3000	NSW	
Novocastrian Offshore Wind Farm	Early Planning	2000	NSW	Jan-2031
Perth Array Offshore Wind Farm	Early Planning	1000	WA	
Port Kembla (Green Energy Partners)	Early Planning	8000	NSW	
Portland Floating Wind Farm	Early Planning	750	VIC	
Samphire Offshore Wind Farm	Early Planning	3000	WA	Jan-2033
Seadragon Offshore Wind Farm	Early Planning	1500	VIC	Jan-2030
South Pacific Floating Wind Farm	Early Planning	1575	NSW	Dec-2032
Southern Queensland (Green Energy Partners)	Early Planning	2000	QLD	
Southern Winds Offshore Wind Farm	Early Planning	1155	VIC	Dec-2032
Spinifex Offshore Wind Farm	Early Planning	1000	Portland	Jan-2027
Star of the South	Early Planning	2200	VIC	Jan-2030
Myalup Offshore Wind Farm	Early Planning	300	WA	Jan-2027
Myalup Extension Offshore Wind Farm	Early Planning	1600	WA	
Ulladulla Offshore Wind Farm	Early Planning	2000	NSW	Dec-2035
Velella Offshore Floating Wind Farm	Early Planning	3000	WA	
Western Australia (Green Energy Partners)	Early Planning	1000	WA	
Western Victoria (Green Energy Partners)	Early Planning	1000	VIC	

Wave Technologies

Australia has a number of wave energy projects underway, focusing on developing cost-effective and reliable wave energy technologies. A list of all projects is presented below [76-77].

Table 4. List of all wave energy projects in Australia

Projects	Start Date	End Date	Total cost	Lead Organisation	Location	Description
Perth Wave Energy Project	Apr-2012	Dec-2017	$39.87m	Carnegie Clean Energy Limited	WA	This project is the first grid-connected-industrial-scale wave system in the world capable of producing desalinated water. The Perth Wave Energy Project is a renewable energy initiative aimed at harnessing the power of ocean waves to generate electricity.
Oceanlinx Wave Energy Demonstrator	Jun-2012	Jun-2014	$6.58m	Oceanlinx	Port MacDonnell, SA	This project was not successful.
BPS bioWAVE Ocean Pilot	Jun-2012	Sep-2018	$23.78m	BioPower Systems Pty Ltd	Port Fairy, VIC	The BPS bioWAVE Ocean Pilot project in Australia is a joint initiative between BioPower Systems (BPS) and the Australian Renewable Energy Agency (ARENA) aimed at demonstrating the feasibility of the bioWAVE technology. The bioWAVE wave energy converter device uses a unique oscillating water column technology to generate electricity from ocean waves. The project is expected to provide valuable data on the performance of the technology and

						accelerate the development of wave energy as a reliable and sustainable source of electricity.
Carnegie CETO 6 Technology	Jun-2014	Oct-2019	$5.3m	Carnegie Clean Energy Ltd.	Albany, WA	Carnegie CETO 6 Technology is a type of wave energy converter developed by Carnegie Clean Energy in Australia. Carnegie has developed a larger version of the technology, known as CETO 6+ or CETO 7, which has plans for commercial-scale wave energy projects. While still in early development, wave energy has potential as a renewable energy source.
Australian Wave Energy Atlas	Jul-2014	Feb-2018	$3.28m	CSIRO	Hobart, TAS	It focused on creating an atlas that simplifies the evaluation process for wave power projects in Australia.
Ocean Wave-Power Machines	Aug-2014	Dec-2018	$1.5m	Swinburne University	Melbourne, VIC	
Energy Cost Study for Bombora Wave Energy Converter	Nov-2015	Apr-2016	$421k	Bombora Wave Power	Perth, WA	
Wave Energy Cost Reduction	Apr-2016	Dec-2021	$3.6m	University of Western Australia	Perth, WA	The project aims to research the most efficient configurations for wave energy device arrays to minimize installation and infrastructure costs, while maximizing power output. This will involve exploring various factors such as the optimal number, size, and location of wave energy devices.
Garden Island Microgrid Project	Aug-2016	Dec-2020	$7.49m	Carnegie Clean Energy Ltd.	Garden Island, WA	This project will use a combination of solar power, battery storage, and wave energy to provide reliable and resilient power for the base. It will serve as a demonstration project for the potential of microgrids to provide sustainable, cost-effective energy solutions in remote locations.

Tidal Technologies

A few tidal energy projects are currently in development phase in Australia. This country has a number of innovative technologies in both wave and tidal energy. However, the main challenges are capital costs and damage from harsh ocean conditions. These projects face a major global financing challenge, while tidal energy is also susceptible to environmental concerns. Table (5) presents a list of tidal energy projects in Australia that have been reported by the Australian Renewable Energy Agency (ARENA) [77]:

Table 5. List of Tidal Projects in Australia

Projects	Start Date	End Date	Total Cost	Lead Organisation	Location	Description
Tidal Turbine Reef Feasibility Study	Nov-2016	Sep-2018	$620k	Worley Parsons	Perth, Western Australia	Research is designed to evaluate the potential of a new type of tidal energy generator called the Tidal Turbine Reef (TTR). The study will assess the technical, environmental, social, and financial aspects of the TTR and determine whether it can be developed at an economically viable Levelized Cost of Electricity (LCOE).
Tidal Energy in Australia	Jun-2017	Jan-2021	$5.85m	University of Tasmania	Tasmania	The project aims to create a detailed map of the country's tidal energy resource and assess its potential contribution to Australia's energy needs. The project will also evaluate the economic feasibility of developing commercial-scale tidal energy projects and provide valuable information to support the growth of Australia's emerging tidal energy industry.
Ocean Energy Systems Technology Collaboration Program	Mar-2018	Feb-2024	$619k	CSIRO	National	

UniWave200 King Island Project – Wave Swell	Mar-2019	Dec-2023	$12.3m	Wave Swell Energy	King Island, Tasmania	This project has deployed its 200kW wave energy project on King Island, Tasmania. On January 10, 2021, the unit was installed at Grassy, King Island. On June 18, 2021, it exported its first power into the King Island grid [95].

South Korea

Wind Technologies

There are 125 offshore wind farms in this country, with eight currently operating and generating electricity. None of the other projects has advanced enough in their construction phase to connect turbines and produce power. One project is in the building phase, and three projects have either received consent or have applied for consent [71]. Table (6) presents a list of fully commissioned offshore wind farms in South Korea.

Table 6. Fully commissioned offshore wind farms in South Korea

Name	Capacity (MW)	Region	Commissioned Date
Gunsan Port - KEPRI Suction Bucket Demonstrator	3	Jeollabuk-do, Gunsan	Jan-2017
Gunsan 4.3 MW Demo Offshore Wind Farm	4.3	Jeollabuk-do, Gunsan	Jul-2021
Hyundai 5.5MW Test Turbine	5.5	Jeju	Apr-2014
Southwest Offshore Demonstration Offshore Farm	60	Jeollabuk-do, gochang	Jun-2020
Tamra Offshore Wind Farm	30	Jeju	Nov-2017
Woljeong Demonstration Offshore Wind Farm	5	Jeju	Jul-2012
Yeonggwang Baeksu Offshore Wind Farm	8	Yeonggwang, Jeollanam-do	Jul-2022
Yeonggwang Offshore Wind Farm	34.5	Yeonggwang, Jeollanam-do	Jan-2019

Wave Technologies

It has several wave energy projects underway and is also investing in the development of advanced wave energy technologies.

Tidal Technologies

South Korea has been actively developing this technology in recent years. It has several tidal power plants, including the Sihwa Lake Tidal Power Station, one of the world's largest. The Sihwa Lake Tidal Power Station, located near Seoul, began operating in 2011 and has a capacity of 254 megawatts.

In addition to the Sihwa Lake Tidal Power Station, South Korea has also developed other tidal power plants, including the Uldolmok Tidal Power Plant and the Incheon Tidal Power Plant. Uldolmok Tidal Power Plant is located in Uldolmok, Jindo County, and was commissioned by the South Korean government on May 14, 2009. The project has an installed capacity of 1 MW, which generates 2.4 GWh annually, providing enough power to meet the needs of approximately 430 households. In June 2011, an additional 500 kW was commissioned, further increasing its capacity.

The Incheon Tidal Power Plant is another large tidal power plant proposed for Incheon Bay, South Korea. The plant is designed to have a generating capacity of up to 1,320 MW, making it one of the largest tidal power plants in the world. It is planned to have 44 water turbines, each rated at 30 megawatts. It is expected that the plant will generate up to 2.41 TWh a year.

These projects demonstrate South Korea's commitment to developing renewable energy sources and reducing its reliance on fossil fuels.

While South Korea is not a pioneer in tidal power plant technology, it has made significant strides in recent years and is now recognized as one of the world's leaders in this field.

Japan

Wind Technologies

On the 22nd, Japan's first large-scale commercial offshore wind power plant commenced operation in the Noshiro Port area of Noshiro City, with an output of 84MW. The particular purpose company "Akita Offshore Wind Power" (AOW), based in Akita City and led by the general trading company Marubeni (Tokyo), is undertaking a project to construct 20 offshore wind turbines at Noshiro Port and 13 offshore wind turbines at Akita Port [78]. A new wind farm situated off the port of Akita commenced commercial operations on January 31, 2023, boasting an output capacity of 55 MW. The development of offshore wind power generation facilities continues to be a crucial component of the Japanese Government's goal to attain carbon neutrality by 2050. Offshore wind power projects will likely maintain their momentum throughout 2023 and beyond [79].

Wave Technologies

Japan is also exploring the potential of wave energy, with a few projects underway to test and develop different wave energy technologies.

Ocean Thermal Energy Conversion (OTEC)

This country has been a leader in the development of OTEC technology and has conducted several successful OTEC experiments in the past. One of the most significant OTEC projects in Japan is the Kumejima OTEC Demonstration Facility, which was completed in 2013. The facility, located on the island of Kumejima, Okinawa, is a joint project between Toshiba Corporation and the Japanese government. The facility has an installed capacity of 100 kilowatts and uses warm surface water from the ocean to vaporize ammonia, which drives a turbine to generate electricity.

Taiwan

Wind Technologies

This country has 137 offshore wind projects. Three of them are operating**,** six have been completed enough to connect the turbines and generate electricity, one is in the construction phase, and one is either consented or has applied for consent [71]. Table (7) contains information about operating projects, or projects near to completion.

Table 7. Offshore wind farms: Operating and Nearing Completion in Construction

Name	Status	Capacity (MW)	Region	Full Commissioning Date
Changfang - phase 2	Under Construction	446.5	Changhua	Dec-2023
Changhua Demonstration	Operating	109.2	Changhua	Aug-2021
Formosa 1 OWF - phase 1		8	Miaoli	Apr- 2017
Formosa 1 OWF - phase 2		120	Miaoli	Jan-2020
Changfang - phase 1	Partial Generation/Under Construction	95	Changhua	Dec-2024
Formosa II		378	Miaoli	Jun-2023
Greater Changhua 1 - Southeast		605.2	Changhua	Apr-2023
Greater Changhua 2a - Southwest		294.8	Changhua	Apr-2023
Xidao - phase 1		47.5	Changhua	Dec-2024
Yunlin		640	Yunlin	Oct-2023

Wave Technologies

Taiwan is also investing in wave energy, with several projects underway to test and demonstrate the viability of different wave energy technologies.

Malaysia

Ocean Thermal Energy Conversion (OTEC)

Japan and Malaysia have since 2019 been cooperating on OTEC research and development though a Science and Technology Research Partnership for Sustainable Development (SATREPS) Program. The joint project includes a variety of fields and activities such as human resource development through onsite training. In addition, the major component of the project is the development of a novel OTEC cycle, dubbed “hybrid-OTEC.” The Facility sub-project objectives include the design and demonstration of a 3kW Hybrid OTEC System, with jointly-designed equipment manufactured in Japan to be transported to a locally constructed facility at I-AQUAS at Universiti Putra Malaysia (UPM) [17-18].

Vietnam

Wind Technologies

Vietnam boasts 126 offshore wind farm projects, with 29 currently in operation, while none have advanced sufficiently in construction to connect turbines and generate electricity. 5 projects are under construction, and 6 have either received consent or are in the process of obtaining it [100]. In Table (8), we provide information on currently operating offshore wind farms in Vietnam.

Table 8. Offshore wind power technologies in Vietnam

Name	Capacity (MW)	Region	Full Commissioning Date	Description
Bac Lieu - phase I (intertidal) Offshore Wind Farm	16	Bạc Liêu	May-2013	Bac Lieu - phase 1 is developed by Cong Ly Construction-Traditing-Tourism Co. Ltd. The site is located in Bac Lieu district, Bac Lieu province and comprises 10x1.6 MW turbines.

Bac Lieu - phase II (intertidal) Offshore Wind Farm	83.2	Bạc Liêu	Jan-2016	
V1-1 - Truong Long Hoa (intertidal) Offshore Wind Farm	48	Trà Vinh	Nov-2021	This plant developed by Tra Vinh 1 Wind Power Co., Ltd., and has a capacity of 48 MW and comprises 12 turbines, each with an output of 4.2 MW. The wind farm is included in the "Plan for development of wind power in Trà Vinh period to 2020, with a vision to 2030.
V1-2 - Truong Long Hoa (intertidal) Offshore Wind Farm	48	Trà Vinh	Oct-2021	This farm features 12 turbines, each with an output of 4.0 MW. With a total investment exceeding 2.232 billion VND, the facility is expected to generate 162-168 GWh annually. A potential 48 MW expansion, requiring an additional investment of 2.181 trillion VND, is slated to commence construction in Q4-2023 and reach commercial operation by Q2-2024. In 2017, the project was sold to Sermsang Power Group (80% ownership) and Truong Thanh Vietnam (20% ownership), resulting in a name change to Trà Vinh 2.
Ca Mau (intertidal) phase 1 Offshore Wind Farm	190	Ca Mau	Dec-2022	Phase 1 of the project has a capacity of 190 MW and is expected to be connected to the grid by October 15, 2022. Meanwhile, Phase 2 has a capacity of 185 MW and is scheduled for grid connection on June 30, 2023.

Marine renewable energy technologies, such as wave and tidal energy, are relatively new sources of renewable energy that are gaining traction in many countries around the world. While the Asia Pacific region has historically had limited marine renewable energy systems in place, there has been a growing interest in developing these technologies in recent years.

When we consider some of the major countries in the Asia Pacific region, such as Japan, South Korea, China, and Australia, we can see that each of these countries has made significant strides in the development of marine renewable energy technologies. For example, South Korea has developed several tidal power plants. China has also shown interest in developing its marine renewable energy potential and has invested in research and development in this area. Meanwhile, Australia is home to several wave energy projects that are currently under development.

Although marine renewable energy technologies are still in their early stages in the Asia Pacific region, there is a growing trend toward their adoption and deployment.

3. Research Design

This section aims to conduct a literature review and identify the most pertinent studies within the field of cybersecurity research in Marine Renewable Energy Systems. By conducting a comprehensive review of relevant literature, the study seeks to identify gaps in current research and establish a solid foundation for the research design framework.

3.1. Framework of Literature Review

This study conducts an integrated systematic review to comprehensively assess diverse perspectives of cyber-attacks in Marine Renewable Energy Systems. Systematic reviews are a rigorous approach to analysing literature that facilitates the identification of trends, knowledge gaps, and changes in a particular research area. Through the systematic review, this study presents a comprehensive overview of research on cybersecurity in MRE systems and identifies areas that require further investigation.

Based on the systematic review outcomes, this study synthesized critical findings and emerging trends in cybersecurity in MRES. The use of a systematic literature review methodology can enable the identification of potential cyber threats and attacks that may occur in marine power plants. By analysing the relevant literature, we can gain insights into the types of threats and attacks that have been experienced in the past, as well as those that are emerging or have the potential to emerge in the future. Furthermore, a systematic review of the literature would be helpful in the development of practical solutions to prevent and mitigate cyber threats in marine technologies. This study's findings can inform the design of robust cybersecurity strategies that integrate the latest technologies and best practices to ensure the security and resilience of energy systems against cyber-attacks.

This study has the following significant objectives:

1. Identify the most common types of cyber-attacks in MRE systems and assess their impact on the energy infrastructure;
2. Assess the socio-economic and financial impact of attacks;
3. Evaluate cybersecurity practices in MRES;
4. Develop a comprehensive cybersecurity strategy for MRES that integrate the latest technologies and best practices to ensure the security and resilience of the energy infrastructure against cyber-attacks;
5. Evaluate the regulatory and policy frameworks related to cybersecurity in MRES and provide recommendations for improvements to ensure the security and resilience of the energy infrastructure against cyber-attacks.

Figure 8. illustrates the framework of the literature review applied in this study.

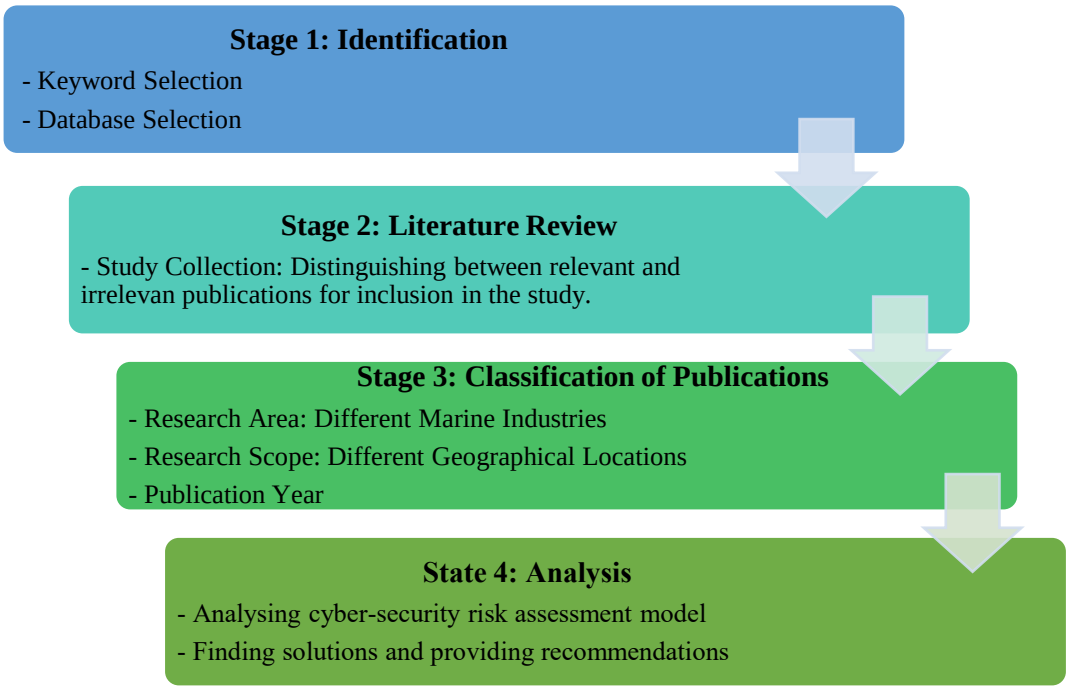

Figure 8. The framework of literature review

The methodology of conducting a comprehensive literature review is crucial to ensure the validity and reliability of the research findings. In the first step of the literature review process, a structured keyword search was conducted across various search engines, academic journals, and industrial websites. The selection criteria were established based on the research objectives, and the relevant sources were screened and analysed. This search aimed to identify relevant articles and studies on the topic under investigation.

Keywords are relevant to the field of cyber-attacks in MRES, including "Marine Renewable Energy", "Marine Renewable System", "Renewable Energy", "RE", "Renewable Systems", "Cyber Attack", "Cyber Security", "Ocean Energy", "Ocean Energy Sources", "Marine Energy Sources", "Marine Energy Attacks", "Cyber Threat", "Offshore Wind Energy", "Wave Energy", "Tidal System", "Thermal System", and "Renewable Transition" were considered in the search process. The search is aimed to identify relevant studies and articles that focus on the interplay between marine renewable energy systems and cyber security.

At the last stage of our research process, after the selection of studies, a systematic literature review commences by determining which publications are worth considering and which should be excluded. In this stage, we meticulously review the available literature and carefully select the most relevant studies to commence our analysis. Our selection criteria are based on the relevance and quality of the studies, as well as their alignment with our research objectives. The selected studies are deemed to provide the most valuable insights and information necessary to guide our analysis. This was a critical step in our research as it helped ensure that our analysis results were based on the most robust and relevant data and evidence available.

Following the completion of the literature review process, a comprehensive cybersecurity assessment of MRE systems will commence in the next stage.

4. Literature Review

4.1. Comprehensive Review of Cybersecurity Threats and Attacks

Below is a list of key terminologies in cybersecurity to help you better understand the field [80-81]:

- Cybersecurity – A set of techniques and procedures to safeguard operations, computer systems, IT networks, and data against unauthorized access, theft, damage, or other malicious attacks. These measures encompass implementing secure hardware and software, adopting encryption and authentication protocols, and creating policies and procedures for incident management and response. Cybersecurity aims to protect the confidentiality and integrity of information and systems while reducing potential harm to individuals, organizations, and society.
- Cyber Resilience – This refers to the capability of an organization to withstand and quickly recover from disruptive cybersecurity incidents while maintaining continuous business operations. It involves a combination of technical and organizational measures that enable an organization to detect, manage, and recover from cybersecurity incidents effectively and efficiently.
- Cyber-security Event – It describes a state or action in a system, service, or network that may indicate a potential breach of a security policy, a failure of safeguards, or an unknown security situation.
- Cyber-security Incident – An undesirable or unpredictable cybersecurity incident, or a series of such incidents, that have either affected business operations or has a high likelihood of impacting business operations.
- Cyber Attack – It is a deliberate attempt to harm computer information systems, networks, infrastructures, personal devices, or smartphones. This can be carried out by a cyber-attacker, who seeks unauthorized access to data, functions, or restricted system areas with potentially malicious intent.
- Operational Technology (OT) – It refers to the use of technology to monitor and control physical devices, processes, and events in an industrial or operational environment.
- Authentication – It refers to the procedure of authenticating a user, device, or system to grant or deny access to a particular resource or service.
- Cyber Threat – A threat is any potential danger or vulnerability that could harm computer systems, data, operation systems or networks.
- Firmware – It is a type of software permanently embedded into a device's hardware. It provides low-level control and management functions necessary for the device to operate and serves as the underlying instructions that control its essential operation.

Type of Cyber Attacks:

Cyber-attacks aim to compromise a computer system, network, or device to steal sensitive information, disrupt operations, or cause other harm. There are several ways to accomplish this, including exploiting vulnerabilities in software or systems, using malware, or carrying out social engineering attacks. The consequences of a cyber-attack can range from financial losses and business disruption to damage to reputation and loss of sensitive data. There are different types of cyber-attacks, a few of the most common are listed below:

- **Malware** – It refers to malicious software, including ransomware, viruses, worms and spyware. These types of software often gain entry through vulnerabilities, such as when a user clicks on a dangerous link or email attachment, which then installs the malicious software.
- **Ransomware** – It is malicious software that encrypts a victim's files and demands payment to decrypt them. It can cause significant consequences such as loss of access to data, business disruption, and financial losses. Protecting against ransomware includes regularly backing up data, using antivirus software, and avoiding suspicious links. If affected, it's important to contain and mitigate the impact by disconnecting from the network, restoring from backups, and reporting the incident. Malware refers to a broad category of harmful software, while ransomware specifically encrypts a victim's files and demands payment for the decryption key.
- **Phishing** – This attack refers to the act of sending fraudulent communications that seams are originated from a trustworthy source, usually through email. The objective is to steal sensitive information such as credit card details and login credentials or to install malware on the device. Phishing is a growing cyber threat and has become increasingly prevalent in recent times.
- **Denial-of-service (DoS) attacks** – This attack makes a computer or resource network inaccessible by overwhelming traffic from multiple sources. DoS attacks aim to disrupt the normal functioning of a system or network, preventing users from using it. Various methods can be used to launch DoS attacks, such as exploiting vulnerabilities in a system, overloading a network with traffic, or installing malware to infect and control multiple devices.
- **Man-in-the-middle (MitM) Attacks** – This attack occurs when an attacker intercepts data transmitted between networks or computers. An attacker can spy on the communication of two parties, often without being detected, by placing themselves "middle" between them. A message can also be modified before it is sent to the intended recipient by the attacker. MitM attacks can be prevented by using VPNs or encrypting access points.
- **A Structured Query Language (SQL) injection** – This injection occurs when malicious code is inserted into a SQL-based server and forces the server to reveal information that it would normally keep confidential. SQL injections can be executed through the submission of malicious code into a search box on a vulnerable website or through other means.

- **Zero-day exploit** – This type of cyber-attack leverages an unknown software vulnerability to gain unauthorized access to systems or steal sensitive data. Since these attacks are difficult to detect, they are highly valuable to attackers and can have serious consequences for individuals and organizations. Protection against zero-day exploits requires keeping software up to date, utilizing antivirus and firewall solutions, and implementing effective security measures.

In light of the wide range of marine activities relevant to the energy sector, cybersecurity threats can be classified into numerous groups.

1. Human error or human ignorance
2. Fraud
3. Attacks to facilitate crime
4. Navigational attacks
5. Operational attacks
6. Indiscriminate attacks
7. Compound attacks
8. Infrastructure attacks
9. Future concerns
10. Hybrid aggression

4.2. Overview of Cyber Threats and Vulnerabilities in Marine Industries

Given the multitude of potential challenges posed by cyber-attacks, extensive research has been conducted to explore the various possibilities, types of threats, and solutions to these malicious activities in marine industries. The marine industry plays a critical role in the growth and stability of the global economy, generating significant economic output and providing employment opportunities for millions of people. As the industry continues to embrace technological advancements and innovation, it is also becoming increasingly vulnerable to cyber threats that can have far-reaching consequences. These threats can not only compromise the safety and security of the industry's operations but also disrupt its efficiency, leading to financial losses and reputational damage. To safeguard the marine industry from these cyber risks, it is crucial to continuously assess and address vulnerabilities, implement robust security measures, and promote awareness and preparedness among industry stakeholders. The primary sectors of the marine industry that have received extensive attention in the study of cyber-attacks are:

1. Shipping and logistics – This sector play an essential role in the global economy, connecting businesses and consumers around the world. Moreover, this sector handles a significant amount of sensitive information, including personal data and financial transactions, which makes it a prime target for cyber-attacks. The loss or theft of this information could lead to substantially profit losses and damage to reputation, not only for shipping and logistics companies but also for their clients and partners. Cyber-attacks in the shipping industry can also have significant implications on the freight being transported, including supply-chain disruptions, delays, cargo theft or loss, and freight misrouting.

2. Ports and terminals – This sector is a critical segment of the global supply chain and handles sensitive, confidential data and critical infrastructure, making them vulnerable to cyber-attacks. Cyber-attacks on ports and terminals threaten the security of sensitive information, can lead to operational disruptions, and potentially cause widespread economic disturbance. The consequences of a successful attack include financial losses, business interruption, and damage to reputation. The increasing reliance on technology in ports and terminals makes them more susceptible to cyber threats, making them even more critical for the industry to address these risks. Given the critical role of this sector, numerous studies have focused on analysing the potential consequences and solutions to cyber-attacks in this sector. By proactively addressing these risks, the ports and terminals can help ensure their operations' safety, security, and efficiency and the continued growth of the global economy.
3. Offshore Oil and Gas – With vast assets and critical infrastructure, offshore oil and gas is a precious target for cyber attackers. Cyber-attacks in the offshore oil and gas industry can compromise the safety and security of offshore operations, disrupt efficiency, and impact profitability. They also pose a significant risk to human safety if industrial control systems are compromised.

Google Scholar, an academic search engine, yielded 205 pieces of literature focusing on the analysis of cyber security and attacks in various sectors within the marine industry. The distribution of studies published per year is displayed in Table (9). The majority of these studies primarily focused on cyber-attacks within maritime industries, offering a comprehensive overview of the various types of attacks. Further analysis was then dedicated to exploring cyber-attacks within marine transportation systems, ports, and terminals. However, it is noteworthy that only eight studies specifically addressed cyber-attacks in marine renewable energy systems, indicating a concerning lack of research attention in this particular context. As evidenced by the table, there has been a steady increase in the number of studies conducted in this particular context year after year.

Table 9. Distribution of studies in the context of cybersecurity analysis in marine industries

Marine Sectors	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Maritime industries	1	1	1	1	3	2	2	6	12	10	7	14	15	2	77
Marine Transportation System						1	1	9	6	4	4	4	7	1	37
Port and Terminals				2		1	2	2	5	1	8	9	6		36
Ships			1	1				1	4	2	4	2	4		19
Logistics and Supply Chain			1	1				2	2		4		1	1	12
offshore Oil and Gas Assets							1		1	1	3	1	3		10
MRES										1	4	1	2		8
Marine Navigation Technologies							1	1	1			2	1		6
Total Studies	1	1	3	5	3	4	7	21	31	19	34	33	39	4	205

According to the International Association of Ports and Harbors (2021), stakeholders in port facilities worldwide have reported a marked rise in cyber-threat activities, especially since the onset of the COVID-19 pandemic. From February to May 2020, marine industry experienced a fourfold increase in cyber-attacks, with attacks against operational technology (OT) systems rising by 900% since 2017 [82]. The potential consequences of these threats and vulnerabilities can be severe, including economic losses, harm to reputation, as well as physical harm to human life and the environment. According to Jones et al. [83], there are multiple threats associated with marine-based cyber-attacks, including financial loss, business disruption, damage to reputation, environmental degradation, property damage, incident response cost, and fines and/or legal issues. Consequently, marine cybersecurity has become a very important issue both nationally and internationally.

Cyber-attacks are a growing concern within electricity generator industries, as they can have far-reaching consequences for critical infrastructure. As part of the power sector, the marine renewable energy industry has also encountered its fair share of cyber-attacks. One notable example is the cyber-attack that occurred in 2015, where the BlackEnergy3 malware targeted the Ukraine grid control centre. This malicious attack resulted in a widespread power outage, impacting over 220,000 customers in Ukraine.

The EDP cyber-attack is another noteworthy incident among recent cyber-attacks targeting the power industry. In 2020, Energias de Portugal (EDP), a major energy company based in Portugal, experienced a significant cyber-attack. The attack utilized ransomware known as Ragnar Locker, which targeted the company's corporate network and critical systems. The EDP Group is a prominent electric power generation and distribution player, focusing on renewable energy and IT sectors. With over 11,500 employees, it serves 11 million customers and ranks as the world's 4th largest wind energy producer. However, the company faced a cyber-attack resulting in the theft of 10 terabytes of data, including sensitive customer information and employee credentials. The attackers demanded 1580 Bitcoin, or roughly $10 million. The cyber-attack on the EDP Group resulted in significant disruptions to operations and financial losses and posed potential risks to customer data and privacy. This incident served as a stark reminder of the potential consequences of cyber-attacks on the reputation and functioning of major electricity industry players like the EDP Group. It underscored the importance of implementing strong cybersecurity defences and taking proactive measures to mitigate future risks in the industry. Table (10) resents a list of some notable examples of real cyber-attacks in the power and electricity industries:

Table 10. Cyber-attacks in power industries

Year	Country	Names of Attack	Target	Attack	Consequence	Reference
2015	Ukrainian		Grid control centres	BlackEnergy3 malware	A significant power outage, affecting more than 220,000 customers in Ukraine.	139,140
2015-2017	US	Dragonfly 2.0	Western energy sector	Spear phishing, Trojan-ware, watering hole attacks, and data theft	Spear phishing involves sending targeted emails to deceive individuals into disclosing sensitive information or installing malware. Trojan-ware is malicious software that masquerades as legitimate software to gain unauthorized control over systems. Watering hole attacks compromise websites frequented by the target to infect visitors' devices with malware. Attack led to the unauthorized access and theft of sensitive information	141

2016	Ukraine		Industrial control systems used in power grid	Industroyer or Crash Override malware	The cyber attackers had the capability to disrupt the electricity supply, leading to a significant power outage that affected approximately one-fifth of Kiev, the capital city of Ukraine.	
2018	Ukraine		Chlorine power plant	VPN Filter malware	Attack was successfully prevented.	142,143
2020	Portugal		Energias de Portugal (EDP)	Ragnar Locker ransomware	The cyber-attack resulted in the theft of 10 terabytes of sensitive data, including customer information and employee credentials.	144,145
2021	Brazil	Darkside ransomware gang	Copel Brazilian Utility company	Ransomware	Copel, as the largest company in the state of Paraná, was targeted by a cyber-attack. The attackers have stolen over 1,000GB of data, including sensitive infrastructure access information, personal details of top management, and customer information. They allegedly gained access to Copel's privileged access management solution and obtained plaintext passwords across the company's local and internet infrastructure. The hackers also assert possession of network maps, backup schemes, domain zones, and the Active Directory database containing user objects and password hashes. Despite the breach, Copel's main systems remained unaffected, ensuring normal functioning of electricity supply and telecommunications services. The extent of the attack's impact on different segments of Copel's network and whether encryption was deployed remains unclear.	146, 147
2021	Brazil		Centrais Eletricas Brasileiras (Eletrobras) electric utility company	Ransomware	Eletrobras, the largest power utility company in Latin America, experienced a ransomware attack at its Eletronuclear subsidiary. The incident impacted the administrative network servers but had no effect on the operations of the nuclear power plants, Angra 1 and Angra 2. The plants operate separately from the administrative network for security reasons, ensuring no disruption to the electricity supply in the National Interconnected System. Upon detection, Eletronuclear suspended certain systems, isolated the malware, and minimized the attack's impact. Details regarding a potential data breach were not provided in the press release, but it is common for ransomware operators to steal data before encrypting the network.	146, 147
2021	Denmark		Vestas wind turbine company		Attackers breached Vestas' IT systems, leading to the company shutting down systems across various units and locations to contain the attack. The company said that the attack did not have a significant impact on its manufacturing, construction, or service operations.	148, 149
2022	Germany		Nordex	Conti ransomware	Nordex, a leading global developer and manufacturer of wind turbines, faced a cyber-attack that resulted in the shutdown of its IT systems and remote access to managed turbines. This incident occurred recently and impacted the company's operations, forcing them to take preventive measures to mitigate further risks.	150, 151
2022	Spain		Iberdrola energy company	Data breach	During the cyber-attack, the personal information of approximately 1.3 million customers, including ID numbers, home addresses, email addresses, and phone numbers, was stolen. However, financial data such as bank account details and credit card numbers were not compromised.	152
2022	Australia		Energy Australia	Ransomware malware	The attack led to unauthorized access to the company's online platform, affecting 323 residential and small business customers. Customer details, including names, addresses, email addresses, bills, phone numbers, and partial credit card information, were compromised.	153

The rise of cybersecurity incidents in the marine industry has prompted a growing interest from both civilian and military researchers to investigate the capabilities of worldwide marine cybersecurity platforms. Governments are investing significant resources into understanding

the level of these threats and what measures can be taken to mitigate them. In addition to governmental support, academics are also actively engaged in addressing this issue and conducting research to understand problems better. Overall, the community is deeply concerned about the development of these threats and is working together to find practical solutions.

The maritime energy sector encompasses a broad range of activities that present diverse cybersecurity concerns. To better understand and address these concerns, it is useful to categorize them into distinct areas. This analysis identifies ten key areas of cybersecurity concern that are particularly relevant to the maritime energy sector, providing examples of each [88]:

- Human error or negligence
- Fraudulent activity
- Cyber-attacks for criminal purposes
- Navigational attacks
- Critical Risks to Human Life and Safety
- Operational attacks
- Indiscriminate attacks
- Compound attacks
- Infrastructure attacks
- Emerging concerns
- Hybrid attacks

By categorizing cybersecurity concerns in this way, it is possible to develop targeted strategies and responses that address the unique challenges presented by each area, thereby enhancing the overall security and resilience of the maritime energy sector.

Despite the growing importance of the marine renewable energy sector, limited research has focused on cyber security in this area. This is a concern given that the sector is becoming increasingly reliant on technology, making it vulnerable to cyber-attacks that could compromise its operations' safety, security, and efficiency. Given the critical role that marine renewable energy will play in meeting the world's energy needs in the coming years, it is essential to increase research and investment in this area to ensure that the sector is equipped to address the challenges posed by cyber security.

4.3. Identification of MRES Asset and Equipment

MRES includes a wide range of equipment and infrastructure used to generate, store, and transmit renewable energy from ocean resources to electricity. MRE system assets include [154-158]

- **Generation Facilities –** This section is a crucial part responsible for capturing renewable energy sources and converting them to electrical energy. It is composed of different types of devices and systems, depending on the type of renewable energy used, like turbines and convertors.

- **Energy Storage Systems –** This section is responsible for storing the energy generated by the generation facilities in MRES. Energy storage is critical because renewable energy sources such as wind and solar are often intermittent, meaning that they do not provide a continuous supply of energy. Energy storage allows excess energy to be stored and used when demand is high or renewable energy sources are unavailable. The electrical grid will be more stable and reliable with a balanced supply and demand of electricity.
- **Subsea Infrastructure –** Underwater equipment and structures are designed and constructed for the installation and operation of offshore renewable energy systems, such as subsea cables, foundations, and anchors.
- **Transmission Facilities –** This subsection transports the electricity generated by marine renewable generators to onshore locations or other parts of the electrical grid using subsea cables, transformers, and other equipment. Transmission facilities typically include long-distance power lines that are designed to carry electricity at high voltages over long distances (100 kV or more).
- **Distribution Systems –** This subsection provides electricity to end users, such as homes and businesses. During this process, distribution substations convert high-voltage electricity from transmission lines into lower voltages for end users. Once the electricity is converted, it is transported along distribution lines that carry it to homes and businesses. These distribution lines are typically located underground or on utility poles and are connected to distribution transformers that further adjust the voltage to meet the specific needs of each end-user.
- **Monitoring and control systems –** This section involves the regular monitoring and maintenance of the renewable energy systems to ensure that they operate reliably and efficiently over time.
- **IT systems –** This section includes devices such as computers,
- **Network and Communication Devices –** These devices used in MRES include a range of hardware and software components that enable the real-time monitoring and control of systems. This includes sensors, data loggers, communication networks, and specialized software applications that collect, transmit, and analyse data on various parameters such as wave height, wind speed, and energy production. In addition, communication equipment such as computers, mobiles, modems, routers, Wireless/Bluetooth, Cellular, and switches facilitate the transfer of data between different components of the system and enable remote access to the renewable energy systems. Overall, the Communication and Monitoring Equipment in MRES is critical in ensuring the safe and efficient operation of the renewable energy systems, as it enables real-time monitoring, control, and optimization of the system, helping to minimize potential risks and environmental impacts while maximizing energy production.

It is crucial to determine potential cybersecurity risks and threats associated with each of these assets and equipment, and with the overall MRE system, to implement effective security measures and protect the energy infrastructure.

4.4. General Cyber Attacks and Vulnerabilities in MRES

Renewable energy poses new threats to power grid security. The integration of renewable energy systems into the larger energy grid increases the potential attack surface, making cybersecurity measures more complex to implement. In the energy sector, companies must identify where their projects and operations are vulnerable to threats before threat actors find them. Companies require an accurate, comprehensive, and up to date understanding of their control and information systems – including the connected supplier and third-party systems.

The following outlines a range of potential attacks that may target Marine Renewable Energy (MRE) systems [89-95]:

Physical Access

Physical access cyber-attacks, such as the introduction of a virus via a portable storage medium (USB), the installation of equipment from an untrusted supply chain, or insider attacks, can have far-reaching consequences. The use of portable storage devices, such as USB drives, can introduce malicious software into a system, which can then be used to compromise critical infrastructure. Similarly, importing and installing equipment from a compromised or untrusted supply chain can introduce vulnerabilities into the system, potentially leading to cyber-attacks. Insiders with access to critical systems can also pose a significant threat, as they have knowledge of the system's vulnerabilities and can exploit them for their gain.

Inferior authentication

Cyberattacks of this type can make power plants and other infrastructure systems more vulnerable to cyberattacks. This vulnerability arises when authentication mechanisms, such as passwords or access control systems, are insufficiently strong or easily bypassed. These vulnerabilities can be exploited to gain unauthorized access to power plants, steal sensitive data, or cause equipment failures and other operational interruptions.

Load Redistribution (LR) attack

LA attack is a type of attack caused by false data injection (FDI) attack. In a practical power system, generators are dispatched at regular intervals of 5-15 minutes to minimize operational costs. Load data used in security-constrained economic dispatch (SCED) is typically based on short-term load forecasts that use historical or real-time load measurements as input. However, attackers may deliberately inject false data that passes the bad data detection (BDD) mechanism in order to alter the load information for SCED and modify the enforcement of branch flow limits. Such attacks can have significant consequences, including increased operational costs, compromised system stability, and potential equipment damage or failure. Hence, It is critical to develop effective countermeasures to detect and prevent these types of attacks, including improved BDD mechanisms and enhanced system monitoring and control capabilities [89-91].

Remote Code Execution (RCE) Attack

It is a type of cyber-attack that can cause severe damage to power plant systems. In an RCE attack, the attacker gains unauthorized access to a computer system and can remotely execute malicious code on the targeted computer. This attack can allow attackers to take control of

critical infrastructure systems, steal sensitive data, or cause equipment failures and other operational disruptions.

Network intrusion

It is a type of cyber-attack that involves an attacker gaining unauthorized access to the network of a system, like an offshore wind farm. To accomplish this, various methods can be used, such as exploiting vulnerabilities in software, phishing attacks to steal login credentials, or malware to gain remote control of the network. After gaining access to the network, an attacker can carry out various malicious activities, including stealing confidential information, such as intellectual property. They can also cause damage to the turbines or control systems, potentially leading to disruptions in energy production and financial losses. In some cases, attackers may also use the network as a launching pad to carry out further attacks on other systems, potentially compromising the security of the wider energy grid.

Endpoint Exploitation Attack

Hacking into internet facing endpoints such as closed-circuit television (CCTV) located at the substation.

Cyber-attacks through supply chain in renewable energy sector

Cyber-attacks through the supply chain in the renewable energy sector target vulnerabilities in the various components and services required to design, build, and operate renewable energy systems. To prevent supply chain attacks, organizations must implement robust security measures, including risk assessments, vendor management, and third-party security audits.

Remote Access

MRE systems, like wave power plants or offshore wind farms, are usually situated in far-off ocean waters, distant from coastal communities and infrastructure. Given their remote location in ocean waters, MRE systems often require remote access for various purposes, including monitoring performance, conducting maintenance activities, or implementing system improvements and updates. However, remote access to MRE systems can introduce cybersecurity vulnerabilities and threats. Unauthorized access or compromised remote connections can potentially lead to unauthorized control, manipulation of system settings, or even disruption of operations.

Old Facilities Vulnerability

Old facilities can be vulnerable to cyber-attacks due to outdated equipment and software, as well as the lack of security updates and patches. For instance, there are old wind parks, including communication systems, never designed with the “security by design” mindset like the IEC/ISO 62443 standard. This vulnerability can be exploited by an intruder to gain access to the control systems of these facilities and potentially cause equipment failures or disrupt the power plant's operation.

Decentralised Wind Farm

Operational technology/industrial control systems (OT/ICS) of wind farms are decentralised, with operations being controlled remotely at remote operations control centres and local workstations. This decentralisation of control systems requires the connected network links and equipment to be adequately secured and access to the individual elements of the controlling systems to be closely managed in a secure way.

4.5. Impact Assessment of Cyber Attacks on MRES

Effective evaluation of cybersecurity risk in MRES requires a careful assessment of the potential consequences of a cyberattack. This assessment involves the measurement of the impact that a cyberattack would have on the various components of the MRE system, including assets and networks, as well as the end-users. The impact of a cyberattack can vary depending on a variety of factors, including the extent of infiltration to the networks and control systems, the types of information affected, and the criticality of the affected assets. Consequences are presented below [87]:

- Disruption of energy generation and transmission
- Damage to equipment and infrastructure
- Environmental damage
- The loss of data
- Compromised safety and security of the MRES system
- Financial losses
- Increased Costs
- Reputational damage
- A reduction in trust and confidence
- Potential impact on national security and critical infrastructure
- Delayed or cancelled MRES projects due to cybersecurity concerns

4.6. Best Practices to Manage Cybersecurity Risks in All Marine Technologies

To ensure the resilience and reliability of MRE systems, it is vital to adopt best practices for securing systems against potential cyber threats and vulnerabilities. A few notable best practices include the following [96]:

Training in cyber-security awareness for employees

Cyberattacks frequently exploit human errors to achieve their objectives. Numerous organizations, including government agencies, have succumbed to malware due to unsuspecting employees clicking on malicious email attachments or connecting compromised USB drives to computers. Cybersecurity awareness training teaches employees to avoid these mistakes. Cultivating robust and secure computing habits (cyber hygiene) can frequently spare an organization from wasted time, financial loss, aggravation, and harm to its reputation [97].

Creating a cybersecurity awareness training program for employees is critical to protect MRE systems from cyber threats. Cybersecurity training aims to enhance employees' awareness of potential threats and risks while introducing effective practices for safeguarding themselves, the organization, and their devices, ultimately fostering a culture of security and vigilance

within the workplace. These are crucial subjects and guidelines to consider when cultivating a solid foundation in cybersecurity risk awareness [97-99]:

1. Cybersecurity introduction – Clarify the significance of cybersecurity and its effects on the organization, its employees, and their individual lives.
2. A Concise Summary of Diverse Cyber Threats – Familiarize employees with various cyber threats and vulnerabilities, including phishing, ransomware and malware. Clarify the potential impact of attacks on the organization and each employee's responsibility in mitigating these risks.
3. Establishing Guidelines for Email, Internet, Social Media, and communication portals – A clear set of guidelines for browsing and social media usage on company devices, as well as the use of company email addresses, is essential. Employee browsing habits can pose significant risks to organizations in combating cyber threats. Cybersecurity training should emphasize the importance of avoiding unsafe clicks and being extra vigilant when receiving social media emails requesting a login. Teach employees how to identify phishing emails, malicious attachments, and suspicious links. Emphasize the importance of verifying sender information and not sharing sensitive data through unsecured channels. Some websites pose more significant risks, so it is vital to include training on restricted websites and social networks during work hours. Additionally, consider investing in software that identifies and alerts users to potentially dangerous emails and websites.
4. Passwords and Authentication – Passwords serve as the primary gateway to the digital realm, and cybercriminals employ numerous methods to attempt to decipher them. One of the main techniques that hackers use to obtain crucial passwords involves making informed and strategic guesses until they succeed. The most crucial passwords pertain to both professional and personal email accounts, as well as social network profiles. If a cybercriminal manages to obtain access to someone's email password, they can freely use the "Forgot My Password" feature on almost any account associated with that email. Its important for industries to train employees on creating and managing strong, unique passwords for their accounts. Promote the adoption of password managers and multi-factor authentication to enhance account security. Multifactor Authentication (MFA), commonly known as two-factor authentication (2FA), refers to an extra electronic authentication layer required for accessing a device, website, or application. MFA is based on a combination of three elements to verify a user's identity: knowledge (something the user knows), possession (something the user has), and inherence (something the user is).
5. Social media and online behaviour – Inform employees about the risks associated with social media and sharing too much information online. Explain how cybercriminals can use this information to target the organization and its employees.
6. Security policies and procedures – Ensure that employees are familiar with the organization's security policies and procedures. Conduct regular reviews and updates to keep them relevant and effective.

7. Data protection and privacy – Train employees on handling sensitive data, such as customer information, financial data, and intellectual property. Explain the relevant data protection laws and regulations that the organization must follow.
8. Physical Security – Discarding passwords on sticky notes around your workspace is dangerous, as many attacks occur through digital means, and securing sensitive physical documents is essential for your company's security. Being aware of the risks associated with leaving documents, unattended computers, and passwords in office or home spaces can mitigate security threats. Adopting a 'clean-desk' policy substantially lowers the risk of unattended documents being stolen or copied. Emphasize the necessity of safeguarding physical access to devices like laptops, smartphones, and USB drives. Illustrate how unauthorized access to these devices may result in data breaches and various security incidents.
9. Mobile device security – Educate employees on securing their mobile devices with passcodes, biometric authentication, and security software. Explain the risks associated with public Wi-Fi networks and the importance of updating apps and operating systems.
10. Remote Work Practices – The growing adoption of remote work in 2021 led many companies to implement full-time work-from-home policies. While remote work can boost productivity and work-life balance, it also increases security risks. To address these concerns, personal devices used for work should be secured with locks and antivirus software, and remote employees must be educated on safe practices. As remote work is expected to persist into 2023, even with office reopening, training employees on managing their cybersecurity remains essential to mitigating the evolving threat landscape and keeping security at the forefront.
11. Public Wi-Fi Safety – Employees working remotely and on-the-go may require additional training on using public Wi-Fi securely. Fake public Wi-Fi networks, sometimes found in coffee shops, can expose users to unsecured servers. Power plant organizations can raise awareness and reduce risks by educating employees on safe public Wi-Fi use and recognizing potential scams.
12. Identifying and Reacting to Cyber Threats Training – Phishing techniques have evolved beyond obvious scams, such as large cash rewards in exchange for bank details. For instance, employees might receive an email about a suspicious login attempt on their Google account, which could lead them to a fake page where entering their credentials gives hackers access. Other dubious activities include urgent requests, impulse clicks, or corrupted PDF links. Employees should have an incident response plan, such as notifying the IT team immediately upon spotting a suspicious email, avoiding clicks, and deleting or forwarding the email to a secure inbox for analysis. Always stay vigilant for unknown senders.

Protect Networks:

Protecting networks is crucial for MRE systems to ensure their data and systems' confidentiality, integrity, and availability. Several network security solutions are available that

help protect networks from various threats. Some of the fundamental network protection solutions are presented below [105]:

1. Comprehensive Network Defence – The most effective solution for network protection involves identifying, preventing, reducing, and protecting all network connections to Industrial Control Systems (ICS) assets. This method ensures that generators and MRE systems have a comprehensive awareness of their network topology, device inventory, and data flows within their control system environment. By minimizing unnecessary connections and reducing the attack surface, MRE systems can limit potential entry points for cyber threats. Securing these connections through encryption, security controls, and regular monitoring further enhances the control systems' overall security posture, helping safeguard critical infrastructure and industrial assets from potential cyber-attacks.
2. Firewall – A firewall is a crucial network security device that monitors incoming and outgoing network traffic. By enforcing predefined security rules, it can allow or block data packets. Essentially, firewalls act as a protective barrier between trusted internal networks and untrusted external networks, such as the Internet, to prevent unauthorized access and attacks.
3. Intrusion Detection and Prevention Systems (IDPS) – IDPS solutions monitor network traffic for suspicious activities or malicious behavior, sending alerts and/or automatically blocking identified threats. These systems help prevent unauthorized access, malware, and other cyber threats.
4. Virtual Private Networks (VPNs) – VPNs create a secure, encrypted connection between devices or networks, allowing secure communication over the internet. VPNs are useful for remote workers, branch offices, or securely connecting multiple networks.
5. Endpoint Security – Endpoint security solutions protect individual devices like computers, laptops, or mobile phones connected to a network. These tools include antivirus, anti-malware, and personal firewalls to defend against threats targeting end-user devices.
6. Network Access Control (NAC) – NAC solutions enforce access policies and control which devices can access a network, based on factors like user identity, device type, and security posture. NAC helps prevent unauthorized devices from gaining access to sensitive resources.
7. Data Loss Prevention (DLP) – DLP tools monitor data movement and usage, preventing unauthorized access or transfer of sensitive data. These solutions can help organizations comply with data protection regulations and safeguard intellectual property.
8. Network Segmentation – Dividing a network into smaller, isolated segments can limit the spread of threats and reduce potential damage. This can be achieved using VLANs, subnets, or software-defined networking (SDN) solutions.

9. Security Information and Event Management (SIEM) – SIEM solutions aggregate and analyse data from various sources across a network, including logs and events, to provide real-time monitoring, detection, and reporting of security incidents.
10. Security Orchestration, Automation, and Response (SOAR) – SOAR platforms streamline and automate security processes, integrating various security tools and technologies. This helps security teams respond more quickly and efficiently to threats.
11. Regular Updates and Patch Management: Keeping software, firmware, and operating systems up to date with the latest security patches is essential for network protection. Establishing a patch management process helps ensure vulnerabilities are addressed promptly.
12. These network protection solutions should be combined with strong security policies, employee training, and regular security assessments to create a comprehensive network security strategy.

These network protection solutions should be combined with strong security policies, employee training, and regular security assessments to create a comprehensive network security strategy.

Secure Vulnerable Infrastructure:

Establishing a risk management framework is crucial for enhancing the security of the vulnerable infrastructure. This comprehensive framework enables MRE technologies to assess and analyse risks associated with their infrastructure effectively. Organizations can strengthen their security posture by providing guidance on risk acceptance, risk avoidance, risk transfer, or risk control. The risk management framework plays a pivotal role in safeguarding critical assets and ensuring the resilience of an organization's infrastructure against potential threats.

Infrastructure and Technology Upgrades:

Enhance infrastructure and operational technology (OT), which are critical to daily energy operations. When integrating new OT systems with information technology (IT) networks, confirm that both systems can be easily secured and updated.

Safeguarding Connected Devices:

Implement robust security measures to protect all connected devices within the network, including IoT devices, computers, laptops, smartphones, and tablets, to minimize vulnerabilities and prevent unauthorized access or data breaches. Employ strong authentication mechanisms, encryption, regular software updates, and continuous monitoring to ensure a secure and resilient environment for all devices connected to your network.

4.6.1. Offshore Wind Technologies - Threats and Best Practices

Wind plants are at risk of cyber-attacks that can cause serious harm to power systems. The extent of damage to wind farms is dependent on the specific areas that are targeted. If wind plant control systems are successfully attacked, it could compromise the stability of the system,

leading to potential disruptions in energy market operations and have a negative impact on grid reliability. While cyber-attacks on communication networks can be less aggressive and disrupt data transmission, which can hinder the real-time monitoring and control of wind turbines. To effectively address cybersecurity in offshore wind power generators, the initial step involves identifying cyber threats and vulnerabilities. It is essential to gain a comprehensive understanding of the infrastructure and various components within wind systems and identify potential attacks that could target each specific section. Figure (9) illustrates a schematic diagram of infrastructure of an offshore wind power plant.

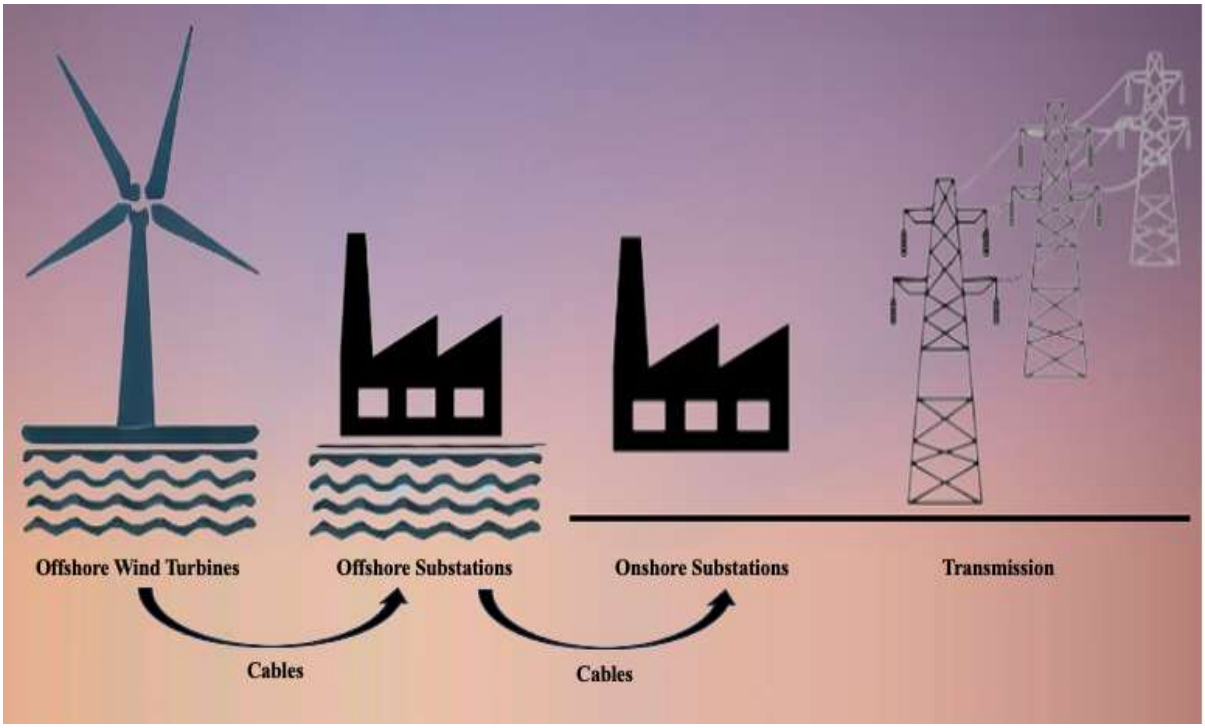

Figure 9. Offshore wind farms

As depicted in Figure (9), the infrastructure of offshore wind generators consists of sections which are presented below:

1. **Foundation and Substructure –** In the offshore environment, the foundation structure is crucial to provide stability and support for the wind generators. It can either be a fixed foundation like monopiles or jackets, or a floating foundation designed for deep-water installations.
2. **Offshore Wind Turbines –** Over extensive land and water territories, many wind turbines are strategically established in offshore and onshore wind farms, capturing the immense power of the wind to generate electricity. Wind farms are comprised of numerous wind turbines strategically positioned on sturdy foundations. Each turbine consists of a tower supporting a nacelle at its uppermost part. The tower is constructed on a robust concrete foundation. Atop the tower, the nacelle houses critical mechanical components such as the gearbox, generator, and control systems. The rotor, which includes a hub and aerodynamically designed blades, captures the kinetic energy of the wind. As the wind

blows, the blades rotate, propelling the motion of the rotor. The hub is linked to the primary shaft, which operates at a lower speed, and this shaft is linked to the high-speed shaft via a gearbox. Ultimately, the high-speed shaft transfers rotational energy to the generator. The generator transforms mechanical energy into electrical energy. This energy is then transmitted through the drivetrain, optimizing energy capture and maximizing the efficiency of the turbine. Collectively, these turbines contribute to the overall generation capacity of the offshore wind farm, working in harmony to harness the power of the wind and generate electricity [117]. Figure (10) illustrates a visual representation outlining the key components and structure of a wind turbine.

Figure 10. Offshore wind turbine

Currently, offshore wind turbines operate dynamically and self-adjust based on the wind conditions in their surroundings. These turbines can adjust their position in accordance with the prevailing wind direction, optimize their rotational speed for maximum efficiency based on the incoming wind speed, and control the pitch of the blades around their long axis to initiate, halt, and regulate both speed and power output. These operational adjustments are predominantly carried out autonomously, relying on sensors installed on the turbine to make informed decisions regarding its functioning. The outputs of weather forecasting models have been used to forecast wind plant power output and grid operational needs [106]. These sensors designed to collect real-time data on a range of

parameters, including wind speed, air pressure, temperature, wind direction, air density, vibration, and rotor position. Accurate measurements play a pivotal role in the smooth operation of the wind farm. By facilitating control, maintenance, and safety protocols, these sensors assist turbine controllers in optimizing performance and minimizing risks. A diverse range of sensors are considered in turbines for various reasons due to their crucial role like wind speed sensors, wind direction sensors, accelerometers, temperature sensors, and torque sensors.

3. **Offshore Substations –** An offshore substation, which is situated in the sea or ocean, serves as a vital structure or platform. Its primary purpose is to collect the electricity generated by the wind turbines and facilitate its transformation by adjusted voltages. The offshore substation serves as a connection point between the wind turbines and the onshore grid.
4. **Subsea Cables –** Submarine or undersea cables play a vital role in the infrastructure of offshore wind power plants. Subsea cables in offshore wind farms can be categorized into two types: communication cables and power cables. Communication cables transmit data and communication signals between different components of the wind farm infrastructure, including wind turbines, substations, control centres, and monitoring devices. They play a crucial role in facilitating real-time monitoring, control, and data exchange, enabling operators to manage and optimize the wind farm's performance efficiently. On the other hand, power cables, known as export cables, transmit the electricity generated by turbines to the onshore grid or offshore substations. These cables are designed to handle high voltages and currents, allowing for the efficient and reliable transmission of renewable energy over long distances, often underwater, to connect with the larger power grid.
5. **Onshore Substation –** The onshore substation is the final connection pinpoint between the offshore wind farm and the onshore power grid. Located on land, it plays a crucial role in receiving the electricity transmitted through export cables from the offshore substation. The onshore substation then modifies the voltage to prepare it for injection into the grid. Additionally, onshore substations also function as command and control centres for the wind farm. The onshore substation incorporates two Supervisory Control and Data Acquisition (SCADA) networks, an operations control network dedicated to managing wind turbine operations and a transmission control network responsible for overseeing power collection and injection into the grid. The substation's operational network includes information technology, networking infrastructure, safety and backup systems, and heating, ventilation, and air conditioning (HVAC) systems. The transmission control network is physically separated from the operations side for enhanced security and safety. Robust physical security measures, including locks, cameras, motion sensors, remote alert systems, reinforced construction, and fences, are implemented in transmission control facilities. Generally, the onshore substations are a critical hub for managing and controlling electricity transmission from the offshore wind farm to the onshore power grid while maintaining a secure and efficient operational environment [117-118].

   SCADA is a widely used computer system in the automation industry and regional infrastructure. Its key functions include control, monitoring, and data transmission. In the

context of offshore wind turbines, offshore/onshore substations, local/national grids, and internet connectivity, SCADA plays a crucial role. It oversees, commands, scans, stores, and manages interfaces within these components, enabling efficient operation and management of the entire system [110]. For example, they enable real-time monitoring of actual parameters provided by sensors like wind speed and transfer it to control centres. Data is collected from turbines and transmitted to the control centre for analysis and decision-making. Typically, in offshore wind power plants, the SCADA system is located in onshore substations. SCADA networks use both wired and wireless communication technologies, and they rely on protocols. It also establishes communication with the turbines through a dedicated communications network, predominantly relying on optical fibers. The network infrastructure includes equipment like routers, switches, and data servers. Operators rely on SCADA networks to monitor turbine performance, identify maintenance needs, optimize power production, and deliver the secure and reliable operation.

Attacks and Corresponding Solutions

Offshore wind power technologies face various vulnerabilities that require proactive prevention measures to mitigate potential attacks. Table (11) provides a summary of potential attacks and vulnerabilities in wind technologies, along with corresponding best practices for mitigating each attack.

Table 11. Compendium of Potential Attacks and Recommended Solutions:

Component	Threats and Vulnerabilities	Solutions
Attacks on Turbine	While offshore wind farms are relatively less accessible than onshore installations, it is important to note that they are not entirely impervious to unauthorized access. Attackers can still find ways to reach offshore wind farms, albeit with greater difficulty compared to onshore sites.	• Enhance Physical Security Measures • Bolster the physical security of turbine areas by enhancing the locks, fences, and CCTV cameras installed on the turbine doors. • Improve the physical barriers around the turbine areas by reinforcing fences, installing barriers or bollards, and implementing security lighting. These measures act as strong deterrents against unauthorized access and enhance the overall security of the turbine site.
Physical Access to Onshore Substations	While substations benefit from strong physical security measures, they are not impervious to physical breaches. Malicious insiders or determined attackers can still find ways to penetrate substations, exploiting their vulnerabilities.	• Enhancing security with perimeter fencing • Remote surveillance • Infrared lighting • Optimizing security with video analytics
Sensors & Control Centres	• Sensors malfunctions • Network congestion • Attacker on power-flow measurements	• An efficient Built-in Data Diagnostics (BDD) mechanism is crucial to ensure reliable data acquisition in the offshore wind generators.
SCADA System	Attacks against SCADA system: • Attack on wind turbine control panel • Attack to control centre LAN • Attacks to remote-control in substation • Attack on communication links	• The utilization of outdated communication protocols without security enhancements poses significant risks in terms of cyber-attacks. To mitigate these risks, it is crucial to update and upgrade protocols based on the latest and most secure standards. By adopting newer protocols, organizations can enhance the security of their communication systems and protect against potential cyber threats.
Subsea Cables	Subsea communication cables can be vulnerable to threats, including network intrusions, data breaches, and service disruptions.	• Protection of cables • Enhancing remote monitoring services

A detailed analysis of attacks and corresponding solutions is presented below:

1. Attacks targeting turbine

The current physical security measures in place for wind turbines are relatively basic and vulnerable. Turbine doors are commonly secured with easily bypassed padlocks, making unauthorized access relatively simple. Even if advanced security mechanisms are employed, such as alarms notifying a control centre of unauthorized entry, the remote location of turbines can significantly delay response times for investigations [117].

In a series of experiments, two researchers from the University of Tulsa have revealed the digital vulnerabilities of wind turbines by physically accessing wind turbines and conducting attacks. The researchers quickly bypassed the turbine's lock, entered the unsecured server box, and connected a Raspberry Pi minicomputer to the turbine's control system. The two men then closed the door and walked back. They used a computer, wrote a command, and stopped a turbine from working. Over two years, two researchers have conducted a systematic series of hacks on wind farms across the US to show the vulnerabilities of the wind farms [119].

Through direct physical access to the internal components of the wind turbines, the researchers were able to execute a range of attacks. These attacks not only targeted the specific wind turbine they gained access to but also extended to all other turbines connected to the same network within the wind farm. By demonstrating the potential for such cascading effects across the network, the researchers highlighted the significance of securing not just individual turbines but the entire interconnected infrastructure of wind farms.

The wind turbines that the researchers accessed were secured with basic five-pin locks or padlocks that could be easily bypassed using common tools like bolt cutters.

> Jason Staggs, one of researchers, said: “A simple tumbler lock was all that stood between us and the wind farm control network,”. “Once you have access to one of the turbines, it’s game over.”

Additionally, the researchers discovered that they could connect to their minicomputers via Wi-Fi from a distance of up to fifty feet. They emphasized that alternative radio protocols, such as GSM, could have been employed to carry out attacks from much greater distances, spanning hundreds or even thousands of miles. These findings underscore the need for enhanced physical security measures to protect wind turbines from unauthorized access and potential cyber threats.

Although Tulsa researchers turned off only one turbine, they mentioned that their methods could easily disable an entire wind farm, potentially cutting off hundreds of megawatts of power.

> <u>The best practices:</u>

While offshore wind farms are relatively less accessible than onshore installations, it is important to note that they are not entirely impervious to unauthorized access. Attackers can still find ways to reach offshore wind farms, albeit with greater difficulty compared to onshore sites.

This highlights the need for enhanced physical security measures that offer stronger protection against unauthorized entry, as well as the development of efficient response protocols to address incidents in a timely manner. Wind farm operators must prioritize the implementation of authentication measures within their control systems' internal communications, rather than solely relying on isolation from the internet. Additionally, bolstering physical security with stronger locks, fences, and surveillance cameras on the turbine doors would significantly increase the difficulty of physical attacks. These proactive security measures are essential to safeguard wind farms and mitigate potential risks to the integrity and reliability of the system.

2. Physical access to onshore substations

While substations benefit from strong physical security measures, including locks, cameras, motion sensors, reinforced construction, and fences, they are not impervious to physical breaches. Malicious insiders or determined attackers can still find ways to penetrate substations, exploiting their vulnerabilities. Given that substations are often situated in remote locations and may lack on-site personnel, response times to breaches can be delayed. Implementing ballistic-resistant barriers around the entire perimeter of larger power substations can pose significant cost challenges due to their expansive footprint. Also, the majority of substations rely on a chain-link fence for protection, which can be vulnerable to rifle shots, posing a security concern.

Once inside a substation, an attacker can employ similar techniques used to access the wind farm control network. They can introduce hidden, difficult-to-detect devices, plant malware to monitor and disrupt wind farm operations, and potentially cause damage to the wind farm's assets. Unauthorized access to a substation holds more severe consequences than breaching a wind turbine since it provides the attacker with potential control over both the operations control system and the transmission control system [117].

The best practices:

Protecting substations against physical breaches and implementing robust security measures are crucial to safeguard the integrity and reliability of wind farm operations. Here are a few examples of such measures:

- Enhancing Security with Perimeter Fencing – Perimeter fencing prevents unauthorised access and protects equipment to minimize loss. Additionally, a secure perimeter increases the difficulty of accessing the facility by vehicles.
- Remote surveillance – When monitored by off-site professionals, this type of surveillance enables swift response to security breaches triggered by alarms. Additionally, cameras play a crucial role in capturing evidence of any criminal activity that may occur within the wind farm.
- Infrared lighting – Incorporating infrared lighting as an additional security measure significantly enhances surveillance capabilities during evening and night-time hours. By providing sufficient illumination, infrared lighting enables cameras to monitor and record activities effectively, ensuring comprehensive surveillance coverage round-the-clock.

- Optimizing Security with Video Analytics - The integration of an intelligent video analytics platform with existing operational systems offers several benefits for wind farm security. This advanced technology helps minimize the occurrence of false alarms, enabling security personnel to focus their attention on genuine security risks within the wind farm. By accurately detecting and analysing potential threats, video analytics enhances the effectiveness and efficiency of security monitoring, ensuring a more proactive approach to safeguarding the wind farm.

3. Sensors and Control Centres

The Wind Farm Control Centre (WFCC) and local controller of the turbine can make crucial decisions and make the necessary adjustments to the turbine parameters by utilizing the sensor measurement. The control centres validate new measurements using their Bad Data Detection Algorithms (BDDA). After validating the measurements, they can be utilized to establish fresh power generation setpoints for the turbines [107]. Sensors, control centres, as well as the network responsible for transmitting data and control commands are vulnerable to cyberattacks, such as [107, 108, 109]:

- Sensors malfunctions - Turbines are susceptible to malfunctions that can occur unexpectedly, leading to the generation of inaccurate or unreliable information.
- Network congestion - The control centre of the wind farm collects data from the sensors in turbines through cellular or wireless technology. However, data corruption may occur during the transmission of sensor measurements. Various factors, including high demand from other devices, limited bandwidth, or interference, may cause congestion. These issues associated with network congestion can potentially affect the accuracy and reliability of the received sensor data, compromising the effectiveness of the wind farm control system.
- A sophisticated attacker can manipulate power-flow measurements in a manner that eludes existing BDDA, resulting in an undetectable attack from the perspective of the system operator. These types of attacks are commonly referred to as Undetected False Data Injection (UFDI) attacks. In the context of a wind farm, an adversary could execute similar UFDI attacks by strategically modifying a carefully chosen set of sensor measurements, leading to the transmission of false meteorological data to control Centres (CC) while evading the BDD process.

<u>The best practices:</u>

Given the mentioned threats and vulnerabilities associated with the sensors, it is crucial to implement an efficient Built-in Data Diagnostics (BDD) mechanism to ensure reliable data acquisition in the offshore wind generators. By employing a robust BDD mechanism, the control centre can proactively identify and mitigate potential issues such as data corruption caused by network congestion or other factors. By adopting a proactive approach to data diagnostics, the wind farm control system's performance and effectiveness are strengthened. This approach enhances the accuracy and reliability of the sensor data acquired.

4. Attacks against SCADA system:

Cybersecurity threats targeting SCADA systems in offshore wind farms present notable risks, impacting operations and security. The potential consequences for wind farms are far-reaching, affecting functionality, safety, and overall reliability.

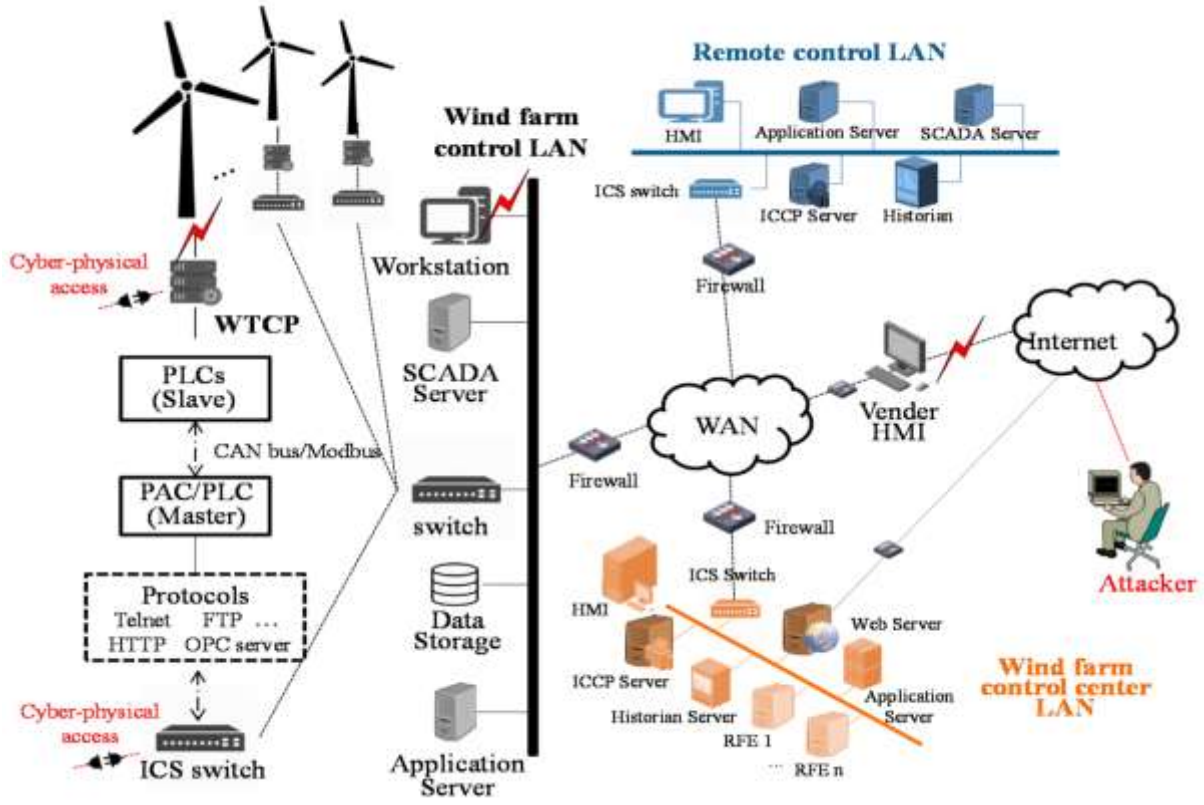

Figure 11. SCADA network in a wind farm. Source: [111]

The primary cyber security risks in wind farms stem from cyber-physical access to the core equipment of the wind farm's SCADA. In Figure (11), you can see the different ways that someone could try to gain control of a wind turbine. This could happen if they manage to intrude into [111-113]:

1. The wind turbine control panel (WTCP) - WTCP is responsible for controlling, managing, and overseeing wind farms. It has a screen that displays and operates keys. However, its accessibility at the tower base makes it vulnerable to unauthorized access. If an attacker bypasses the firewall, they can directly reach the WTCP and exploit vulnerabilities or crack the pin to connect their intrusion device. This grants the attacker control privileges over the WTCP, allowing them to launch buffer overflow attacks and send malicious commands to the wind turbine under its control.
2. Attack to control centre LAN- To carry out the attack, the intruder must first gain access to the web server, typically located within the demilitarized zone (DMZ) of the network. Once the attacker has breached the second firewall that separates the DMZ from the control centre LAN, the next objective is to reach the ICCP server responsible for communication with backup control centres. The subsequent steps resemble those of

attacks on the backup remote control LAN, involving obtaining user privileges on the application server and operator console. However, it is important to note that the attacker must exploit distinct vulnerabilities within the control centre LAN, distinguishing it from intrusions into the backup remote control LAN.

3. Attacks to remote-control LAN in the substation – Remote control centre is a vital communication hub, facilitating coordination between the main control centre and wind farms for remote monitoring and control purposes. As the remote control primarily communicates with the main control centre, it typically does not host a web server within its LAN. However, if the attacker successfully bypasses the firewall, they can gain access to the remote-control network. Subsequently, the intruder can exploit vulnerabilities in the application server linked to the ICCP server, aiming to acquire user privileges. Once these privileges are obtained, the attacker can access the operator console and issue trip commands under an authorized identity. These attack steps emphasize the importance of safeguarding the remote-control LAN against unauthorized access and vulnerability exploitation.
4. Attack on Communication Links - Within the SCADA/EMS system, vulnerable communication links include those connecting the control centre LAN to the wind farm's local control LAN and the links between WTCPs and wind turbines. Attackers may exploit these links through man-in-the-middle (MITM) attacks. Since optical fibers are commonly employed for wind farm communication, surreptitious taps can be installed on the cables, allowing for the injection of additional light and false information into the communication links. Furthermore, attackers may eavesdrop on and analyse the transmitted light information to obtain necessary data. By monitoring and analysing the traffic patterns in the communication links, the attacker can gain insights into the operations. This knowledge enables them to send fabricated measurement data to the operators in the main wind control centre or local control room, potentially leading to erroneous decisions or compromising the integrity of the system.

<u>The best practices:</u>

- The utilization of outdated communication protocols without security enhancements poses significant risks in terms of cyber-attacks. To mitigate these risks, it is crucial to update and upgrade protocols based on the latest and most secure standards. By adopting newer protocols, organizations can enhance the security of their communication systems and protect against potential cyber threats.

5. Attacks on Subsea Cables

Subsea cables are generally vulnerable to both physical and cyber threats. Attackers can intentionally damage subsea cables as a form of physical attack. Physical attacks on subsea cables can disrupt communication services, cause service outages, and incur significant repair costs. Subsea cables are vulnerable not only to physical threats but also to cyberattacks. The main focus of cyberattacks on subsea cables is to target the communication networks and systems connected to the cables. Subsea communication cables can be vulnerable to threats,

including network intrusions, data breaches, and service disruptions. Network intrusions involve unauthorized access attempts to the communication networks and control systems associated with the subsea cables, allowing malicious actors to manipulate data transmissions or gain control over the cable infrastructure. Data breaches target sensitive information transmitted through the cables, potentially compromising privacy and facilitating espionage activities. Disruption of service attacks aim to disrupt normal operations by targeting critical network infrastructure, causing service outages or introducing delays in data transmission, with significant economic and social implications for industries relying on reliable communication services.

The best practices:

- Protection of cables – Protective measures, such as burying subsea cables or using sleeves, can protect cables from external threats and potential damage.
- Enhancing remote monitoring services – Implementing remote monitoring and surveillance systems, such as underwater cameras, sensors, and acoustic monitoring equipment, enhances the security of subsea cables. These systems continuously monitor the surrounding area, detecting any physical disturbances or suspicious activities near the cables. In the event of a potential threat, real-time alerts are generated, enabling prompt response and mitigation actions.

4.6.2. Solar Technologies - Threats and Best Practices

Solar modules are strategically arranged to absorb sunlight and convert it into electricity efficiently. This process involves using photovoltaic cells to capture photons and generate direct current (DC) electricity. The generated electricity from solar panels is fed into the grid for everyday consumption, with a net meter recording the energy supplied and consumed. Grid-connected systems consist of two primary components: a solar panel array and a grid-interactive inverter. These components are interconnected with the switchboard and electricity meter, enabling seamless integration of solar power into the grid [120]. The performance of offshore solar power plants is similar to onshore solar farms. Offshore solar technology refers to the deployment of solar energy systems in marine environments, typically on floating platforms or structures. The exploration of solar energy as an alternative power source in the marine environment has been limited and infrequent. Recently, marine solar technologies have undergone significant development [121]. Figure (12) illustrates a schematic diagram of typical offshore solar power plant.

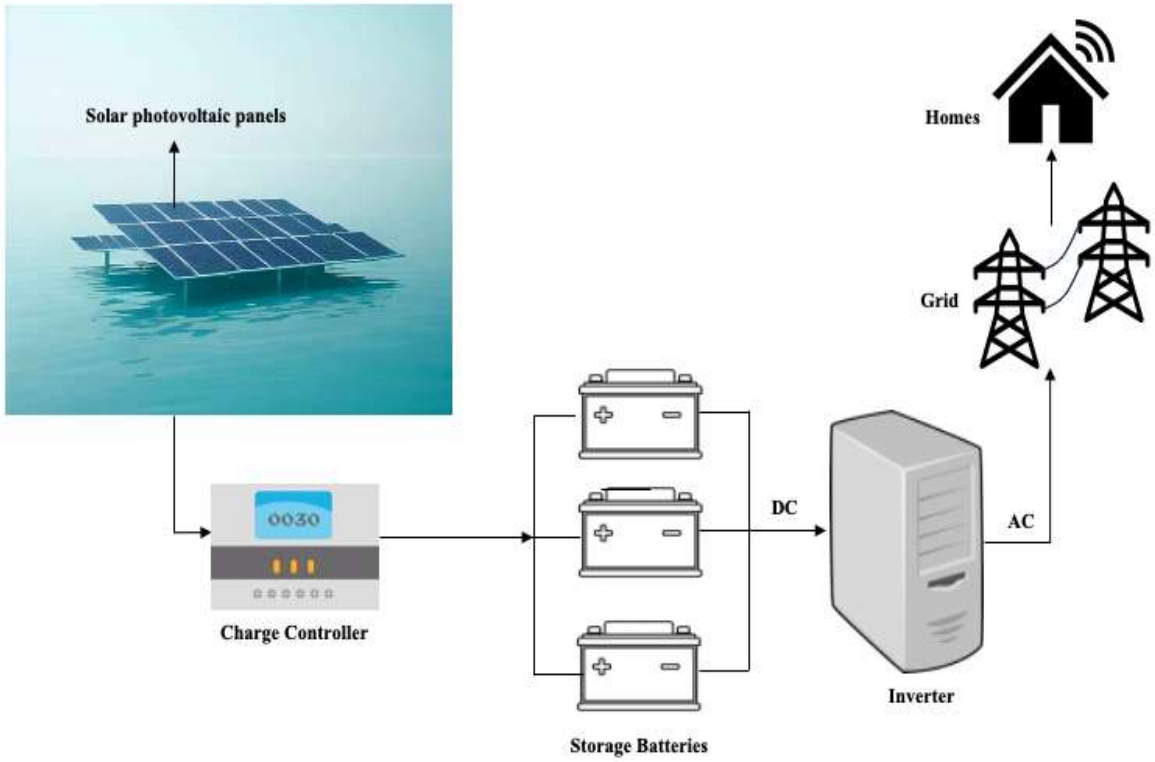

Figure 12. Offshore solar power plant

Solar power plants, being critical infrastructure, are susceptible to cyber-attacks that can disrupt operations, compromise data, and lead to financial and safety risks.

Below are important considerations regarding cyber-attacks on solar power plants:

1. The converters in solar plants are essential for converting the generated direct current (DC) from solar panels into alternating current (AC) for grid integration. However, these devices are vulnerable to cyber-attacks, which can result in power generation disruptions and impact the overall efficiency of the solar plant. Solar energy technologies are susceptible to cyberattacks, especially through inverters and control devices, which play a critical role in managing the electric power grid. Particularly, when these operating-technology (OT) devices, such as solar photovoltaic inverters, are connected to the Internet, they become more susceptible to cyber threats compared to standalone OT devices. It is essential to implement robust security measures to prevent, detect, and respond to unauthorized access or attacks on these devices. Cyberattacks can have severe consequences, including physical impacts such as power outages and fires. Therefore, comprehensive cybersecurity measures are necessary to safeguard the integrity and reliability of solar power systems [122].

   Researchers and manufacturers are actively implementing robust cybersecurity measures to enhance the security of the inverter systems. The information flow within the grid is highly intricate and multifaceted. In converters, market and load management systems establish communication with balancing authorities that are linked to utilities. These management systems connect to SCADA systems and, ultimately, the power plant controller (PPC), creating multiple points of vulnerability to cybersecurity risks within the chain. Site

operators rely on PPC to manage various aspects of plant operations, including revenue, grid stability, compliance, and production levels. The PPC communicates with the plant's SCADA system and field devices, such as inverters, through a power plant network using widely used communication protocols like Modbus and TCP. The SCADA system acts as a security gateway, regulating the flow of information between the plant and inverter networks by allowing or restricting access as needed. The plant control and SCADA systems, comprising both hardware and software, are located in a dedicated enclosure within a substation adjacent to the solar plant. These systems establish connections with the inverter and other field devices using a network infrastructure consisting of fibber-optic cables. Cyber-attacks have the potential to target various points [123].

Hackers can implant malicious malware on the communication board of the inverter, gain unauthorized access through the port of the enclosure housing the fibber-optic cables, or infiltrate the plant control network. These actions pose significant cybersecurity risks to solar power plants. Cybersecurity incidents can lead to circuit breaker tripping, disrupting power generation and impacting the overall power output of the project. Furthermore, attack on inverters can result in voltage fluctuations within the grid, posing additional risks and potential damage [122-123].

The best practices:

- Additional protection measures are implemented in the power plant control system for further safeguards. If the door to the fibre optic network enclosure is opened, the SCADA system can alert operators through an intrusion alarm.
- Plant controls can be accessed and restricted based on a defined list of authorized users and their respective IP addresses.
- Network port settings can be configured to allow only specific types of devices to exchange information, blocking any unauthorized access.
- Implementing separate IP networks for individual inverters ensures secure communication and prevents direct communication between inverters.
- Utilizing a secure SCADA system as the central communication hub filters traffic and ensures all communication occurs through a secure channel.
- Continuous monitoring of inverter configurations by the plant control system helps prevent unauthorized changes that could impact the plant's reliability.
- Renewable plant control systems have built-in alert mechanisms to notify operators immediately of any detected changes to inverter settings, enhancing the system's overall security.

2. A microgrid is a localized electricity grid that incorporates renewable energy generation, such as solar panels and wind turbines, along with battery energy storage. It serves as a small-scale power system that can operate independently during power outages, providing energy generation and storage at a local level. In the context of an offshore solar power plant, the microgrid connects the solar panels to various components, including energy

storage systems, inverters, and control systems. This enables efficient energy distribution, load management, and grid synchronization. The microgrid enhances the plant's ability to operate independently or in conjunction with the main power grid, ensuring stability, flexibility, and resilience for the offshore solar power plant [124, 125]. With the growing digitization and interconnection of the microgrids, ensuring cybersecurity has become a paramount concern [122].

Improperly designed microgrids can be at a higher risk of communication failures and cybersecurity incidents. Unlike power substations with redundant communication networks, many microgrids lack such design to address potential points of failure. Additionally, the extensive implementation of ICT infrastructure in inverter-based smart power systems makes them susceptible to significant external threats like cyberattacks from hackers [126].

A robust microgrid control system plays a critical role in effectively managing energy in solar systems. Its main purpose is to optimize energy control by accurately forecasting and regulating energy generation, consumption, and storage within the system. However, cyber-attacks targeting microgrid control systems pose severe risks, potentially causing significant damage and disruptions to the overall operation of microgrids. Microgrids face the risk of cyberattacks, encompassing attacks on availability, integrity, and confidentiality. Each of these attack types is described below [127, 131]:

- Availability – The purpose of this attack is to restrict or delay access to data, and in the context of a microgrid, this can also extend to the availability of power in addition to data. These types of attacks are called Denial of Service (DoS) attacks. In the context of microgrids, DoS attacks not only involve blocking access to essential resources but also intentionally delaying critical message exchange, which can disrupt the overall operation and functionality of the microgrid. Such attacks can hinder the timely exchange of crucial information within the microgrid system, potentially impacting its performance and reliability.
- Integrity – Attacks on integrity involve manipulating or compromising the accuracy and trustworthiness of data. In the context of microgrids, integrity violations can include interfering with the quality of power. There are various ways in which integrity attacks can occur. Examples of integrity attacks include feeding inaccurate price data to the controller through DNS hijacking, faking a microgrid disconnect signal, sending false commands to the microgrid controller leading to unwanted islanding, and altering the settings of protection relays to cause trip erroneously.
- Confidentiality - Attacks on confidentiality aim to gain unauthorized access to privileged information, including sensitive operational data that should not be accessible to unauthorized entities. In the context of microgrids participating in markets, these attacks can result in the theft of valuable data.

Hence, it is crucial to recognize the risks, comprehend the vulnerabilities, and incorporate effective mitigation measures in the design of microgrids to ensure their resilience against cybersecurity threats. By systematically addressing these vulnerabilities during the design

phase and implementing disaster preparedness strategies, microgrids can become dependable, resilient, and sustainable solutions.

The best practices:

Below are some proposed solutions to enhance the cybersecurity of microgrids [132-133]:

- To enhance the resilience of the cyber layer in microgrids, implementing advanced control systems and analytics software can effectively mitigate communication disruptions. This entails deploying sophisticated technologies and software solutions that strengthen the control systems' capabilities and ensure seamless data transmission and management within the microgrid.
- Installing a compliant control system is one effective measure to enhance the information security and resilience of a microgrid. This ensures that the microgrid meets industry standards and best practices, making it more robust and resilient against cyberattacks. The microgrid can effectively protect its infrastructure, data, and operations from potential cyber threats by implementing a control system with proper security measures.
- Encryption is a critical security measure to protect data in microgrids and other online activities. The process entails jumbling the data to the extent that individuals cannot decipher it without permission. Encrypting data, especially when using a VPN, make the connection secure, preventing cybercriminals from intercepting and understanding the transmitted data. Encryption relies on sophisticated algorithms, known as ciphers, and requires a decryption key or logic to decode the encrypted message. AES (Advanced Encryption Standard) is widely regarded as the most robust encryption standard currently available, providing an added layer of protection to sensitive information in microgrids.

4.7. Theoretical Foundations and Models for Cybersecurity in MRE

Cybersecurity Frameworks and Models that are applied in the Energy sector, which can then be specifically adapted for MRE. Some of these frameworks are the NIST Cybersecurity Framework [134], ISO/IEC 27001 [135], and CIS Controls [136].

Identifying cybersecurity best practices in the context of MRE involves understanding and implementing effective frameworks and standards that have been developed to safeguard IT infrastructures.

A. Key Concepts

- NIST Cybersecurity Framework (CSF) – The framework was developed by the United States' National Institute of Standards and Technology. The Cybersecurity Framework is a comprehensive set of guidelines designed to assist private sector organisations in the effective management and reduction of cybersecurity risk [134]. The framework represents an essential tool in cyber risk management by providing a high-level taxonomy of cybersecurity outcomes. This taxonomy organises the complex and ever-changing landscape of cybersecurity into a manageable structure, facilitating a clear understanding of potential threats, vulnerabilities, and impacts. Beyond this, the NIST CSF also proposes a systematic methodology to assess and manage these outcomes. The framework encourages organisations to identify their unique risks, protect their infrastructure with

appropriate safeguards, detect incidents early, respond rapidly to minimise impacts, and recover efficiently from damages.

As such, the NIST CSF is more than a simple checklist; it is an adaptable guide that can be tailored to an organisation's unique needs, size, risk profile, and industry sector. It fosters an ongoing, interactive process of improving an organisation's cybersecurity posture, making it an essential tool in the current digital landscape.

- ISO/IEC 27001 – This is an internationally recognised standard that outlines how to effectively manage information security. It offers an encompassing framework that supports establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving an Information Security Management System (ISMS). The ISMS is a robust instrument for managing risk, strengthening cyber resilience, and promoting operational excellence. It achieves this by implementing a comprehensive approach to information security that includes technological measures and the analysis of relevant individuals and policies [135].

  The application of ISO/IEC 27001 allows organisations to become more aware of their specific cyber risks, allowing them to proactively identify vulnerabilities. Once identified, organisations can implement strategies to mitigate these risks, increasing their overall resilience in the face of growing and evolving cyber threats. This proactive and holistic strategy toward information security management makes ISO/IEC 27001 a vital tool in the cybersecurity of Marine Renewable Energy.

- CIS Controls – The Critical Security Controls, designed by the Centre for Internet Security (CIS), represent a comprehensive set of recommended actions to strengthen cyber defence. The controls are precisely designed to tackle not just generic threats but specifically target and mitigate the most pervasive and dangerous attacks that we witness in today's digital age [136]. The distinct advantage of CIS Controls is their practical, actionable nature. Rather than providing vague or abstract guidance, the CIS Controls consist of concrete measures that organisations can implement directly [137]. Each control corresponds to a particular threat or vulnerability and offers specific solutions to counteract it.

Additionally, the controls are ranked by their effectiveness against the current threat landscape. This allows organisations to prioritise their implementation of controls based on their unique risk profiles and resource availabilities. As such, the CIS Controls provide a strategic guide to enhance an organisation's cyber defence and a tactical, action-oriented approach to respond to immediate threats. Their structured yet flexible design makes them an essential tool for any organisation serious about strengthening its cybersecurity.

B. Advantages, Disadvantages, and Challenges

Using NIST Cybersecurity Framework [134], ISO/IEC 27001 [135], and CIS Controls [136], we compare the trade-offs between three major cybersecurity frameworks as shown in Table (12). It highlights their individual strengths and weaknesses, allowing MRE organisations to make more informed decisions about which approach best suits their specific security needs, resources, and compliance capabilities.

Table 12. Advantages, disadvantages, and challenges of cybersecurity frameworks

	NIST CSF	ISO/IEC 27001	CIS Controls
Advantages	Flexible and comprehensive	Structured process, certification	Specific, actionable controls
Disadvantages	Voluntary, resource-intensive	Time-consuming, costly	May not cover all aspects
Challenges	Understanding risk profile	Maintaining compliance	Keeping up to date

1) NIST Cybersecurity Framework (CSF):

- Advantages – The NIST CSF is flexible, comprehensive, and prioritises continuous improvement. It is widely adopted and recognised due to its effective structure for managing cybersecurity risks.
- Disadvantages – It is a voluntary framework and does not provide a certification, which may limit its recognition in certain circumstances. Implementation might be resource-intensive for smaller organisations.
- Challenges – It requires a good understanding of the organisation's risk and cyber security posture to effectively implement.

2) ISO/IEC 27001:

- Advantages: ISO/IEC 27001 provides a structured management process and is recognised globally. It offers a certification, which can demonstrate commitment to information security to stakeholders.
- Disadvantages: The certification process can be time-consuming and costly. It may also require considerable changes in organisation's processes.
- Challenges: Maintaining ISO/IEC 27001 compliance requires ongoing effort and commitment to information security management.

3) CIS Controls:

- Advantages: CIS Controls provide specific and actionable ways to prevent most common cyber-attacks. They can be effectively implemented even by organisations with limited resources.
- Disadvantages: The controls may not cover all aspects of a comprehensive information security management system.
- Challenges: Staying up to date with the latest versions of the controls and effectively implementing them requires ongoing effort.

These comparisons can help organisations in the Marine Renewable Energy sector to choose the appropriate cybersecurity framework that best fits their specific needs, resources, and capabilities.

C. Comparative Analysis

In Table (13) we compare the resources required to implement and maintain each standard (NIST Cybersecurity Framework [134], ISO/IEC 27001 [135], and CIS Controls [136]), how

well each standard can scale with the growth of an organisation, and how frequently each standard is updated to respond to new threats and developments in cybersecurity in the Marine Renewable Energy sector.

Table 13. Comprehensive comparative analysis of cybersecurity frameworks and standards

	NIST CSF	ISO/IEC 27001	CIS Controls
Scope	Broad cyber risk management	Information security management	Specific cyber defence actions
Compliance	Voluntary	Requires certification	Voluntary
Implementation	Flexible approach	Structured management process	Defined set of actions
Target Audience	All organisations	All organisations	All organisations
Focus	Managing cyber risks	Comprehensive information security	Preventing cyber attacks
Resources Required	Can be resource-intensive	Requires considerable resources for certification	Lower resource requirements
Scalability	Highly scalable	Highly scalable	Best suited for small-medium organisations
Update Frequency	Regular updates	Regular updates	Regular updates

D. Analysis Relevant to the Marine Renewable Energy Sector

The MRE sector has some unique characteristics and challenges that make cybersecurity particularly important. Energy generation systems are often distributed over large areas, making them potentially vulnerable to various attacks. Furthermore, the systems involve a mixture of information technology (IT) and operational technology (OT), each with its own unique vulnerabilities. It's crucial to identify which cybersecurity framework or combination of frameworks can best address these challenges.

1) NIST CSF: The NIST CSF provides a broad-based approach to managing cybersecurity risks, including both IT and OT risks. It can be customised to the organisation's risk profile, making it flexible for diverse systems seen in the MRE sector.
2) ISO/IEC 27001: ISO/IEC 27001 provides a structured management system for information security, encompassing people, policies, and technology. It can help MRE organisations implement solid cybersecurity practices across both their IT and OT environments.
3) CIS Controls: The CIS Controls provide specific and actionable steps to prevent common cyber-attacks. While they mainly focus on IT systems, many controls can also be applied to OT systems in the MRE sector.

Using NIST Cybersecurity Framework [134], ISO/IEC 27001 [135], and CIS Controls [136], we compare (Table 14) three major cybersecurity frameworks in the context of their applicability to the Marine Renewable Energy sector. These frameworks are evaluated on three critical dimensions: the protection of critical infrastructure, the focus on technological aspects of cybersecurity, and the applicability to distributed systems.

The NIST CSF scores excellently in protecting critical infrastructure and its applicability to distributed systems while maintaining a high focus on technological elements. ISO/IEC 27001, while having a high technological focus, performs well in protecting critical infrastructure and applicability to distributed systems [138]. The CIS Controls, known for its high technological

focus, exhibits fair capability in protecting critical infrastructure and good performance in applicability to distributed systems.

This analysis, therefore, provides vital insights for MRE organisations in selecting an appropriate cybersecurity framework that aligns well with their specific needs and operational context.

Table 14. Comparison of cybersecurity frameworks for marine renewable energy sector

	NIST CSF	ISO/IEC 27001	CIS Controls
Critical Infrastructure Protection	Excellent	Good	Fair
Technological Focus	High	High	Very High
Applicability to Distributed Systems	Excellent	Good	Good

Based on the unique needs of the MRE sector, organisations can choose the cybersecurity framework that best aligns with their specific requirements and system characteristics.

These frameworks and standards can provide a basis for developing specific cybersecurity best practices for Marine Renewable Energy. Their distinctions and finesses offer flexibility and adaptability in defining and implementing strategies that best meet the unique cybersecurity needs of this industry.

5. Conclusion

This study has provided a comprehensive overview of cyber-attacks and vulnerabilities in marine renewable energy systems (MRES), focusing on the Asian Pacific region. By examining a wide range of research and studies, we have identified various potential threats and vulnerabilities that threaten the security and reliability of these technologies. The findings underscore the critical importance of addressing cybersecurity concerns in MRES.

The cyber-attack risk becomes more pronounced with the increasing adoption of marine renewable technologies. Hence, implementing best practices for preventing and mitigating these attacks is crucial. Through our analysis, we have identified several critical best practices that can enhance the resilience of marine renewable technologies against cyber threats.

Several critical practices can be adopted to prevent cyber-attacks in MRE systems, including: 1) Ensuring employees receive comprehensive training in cybersecurity awareness, equipping them with the necessary knowledge and skills to recognize and respond to potential threats effectively. 2) To protect MRE systems, it is imperative to establish robust network security measures that guarantee data and systems' integrity, confidentiality, and availability. Various network security solutions are available to defend against diverse threats, such as firewalls, intrusion detection systems, and encryption protocols. 3) Implementing a risk management framework is vital for enhancing the security of vulnerable infrastructure in the MRE sector. This framework facilitates practical risk assessment and analysis, guiding risk acceptance, avoidance, transfer, or control. It ensures that organizations can strengthen their security posture by effectively managing risks associated with their infrastructure. 4) Moreover, it is essential to prioritize the security of connected devices within the network. Robust security measures, including strong authentication mechanisms, encryption, regular software updates, and continuous monitoring, should be implemented to safeguard all connected devices, including IoT devices, computers, smartphones, and tablets.

The study also delves into specific solutions tailored to each marine technology within the MRE sector, offering detailed insights into addressing vulnerabilities effectively. Additionally, the exploration of theoretical foundations and models for cybersecurity in MRE highlights critical frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, which serve as essential references for establishing robust cybersecurity practices in MRES.

By implementing these practices and leveraging relevant frameworks, the MRE industry can bolster its cybersecurity defences, ensuring these valuable renewable energy systems' resilience, integrity, and continued growth.

6. References

1. Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø.J. and Nesheim, D.A., 2021. A retrospective analysis of maritime cyber security incidents. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.
2. Edenhofer, O., Pichs-Madruga, R., Sokona, Y., Seyboth, K., Kadner, S., Zwickel, T., Eickemeier, P., Hansen, G., Schlömer, S., von Stechow, C. and Matschoss, P. eds., 2011. Renewable energy sources and climate change mitigation: Special report of the intergovernmental panel on climate change. Cambridge University Press.
3. Owusu, P.A. and Asumadu-Sarkodie, S., 2016. A review of renewable energy sources, sustainability issues and climate change mitigation. Cogent Engineering, 3(1), p.1167990.
4. Energy Matters, 2022, What are the different types of renewable energy?, Published by 16 August 2022, https://www.energymatters.com.au/renewable-news/what-are-the-different-types-of-renewable-energy/
5. Office of Energy Efficiency & Renewable Energy, Renewable energy, https://www.energy.gov/eere/renewable-energy
6. EDF Energy, 2022, Types of renewable energy, https://www.edfenergy.com/energywise/renewable-energy-sources
7. Alrikabi, N.K.M.A., 2014. Renewable energy types. Journal of Clean Energy Technologies, 2(1), pp.61-64.
8. Govinda Bhutada, 2022, What Are the Five Major Types of Renewable Energy?, Published by 8 June 2022, https://elements.visualcapitalist.com/what-are-the-five-major-types-of-renewable-energy/
9. Tromly, K., 2001. Renewable energy: An overview. https://www.nrel.gov/docs/fy01osti/27955.pdf.
10. U.S. Department of Energy, 2015, Biomass Basics: The Facts About Bioenergy, Published April 2015, https://www.energy.gov/sites/prod/files/2015/07/f24/biomass_basics.pdf
11. Centre for renewable and sustainable energy studies, Biomass energy, https://www.crses.sun.ac.za/files/services/schools/biomass_energy/Biomass%20Energy%2018%20Final.pdf
12. Kumar, M., 2020. Social, economic, and environmental impacts of renewable energy resources. Wind solar hybrid renewable energy system, 1. DOI: 10.5772/intechopen.89494
13. OECD/IEA, 2016, Energy Technology Perspectives 2016, Towards Sustainable Urban Energy Systems, https://iea.blob.core.windows.net/assets/37fe1db9-5943-4288-82bf-13a0a0d74568/Energy_Technology_Perspectives_2016.pdf
14. Owusu, P.A. and Asumadu-Sarkodie, S., 2016. A review of renewable energy sources, sustainability issues and climate change mitigation. Cogent Engineering, 3(1), p.1167990.
15. Kumar, M., 2020. Social, economic, and environmental impacts of renewable energy resources. Wind solar hybrid renewable energy system, 1. DOI: 10.5772/intechopen.89494
16. Timmons, D., Harris, J.M. and Roach, B., 2014. The economics of renewable energy. Global Development And Environment Institute, Tufts University, 52, pp.1-52.
17. Turkenburg, W.C. and Faaij, A., 2000. Renewable energy technologies (pp. 219-72). UNDP/UNDESA/WEC: Energy and the Challenge of Sustainability. World Energy Assessment. New York: UNDP, 219-272.
18. Clean Energy Council, 2022, Clean Energy Australia Report 2022, https://assets.cleanenergycouncil.org.au/documents/resources/reports/clean-energy-australia/clean-energy-australia-report-2022.pdf

19. World Nuclear Association, 2021, Renewable Energy and Electricity, https://world-nuclear.org/information-library/energy-and-the-environment/renewable-energy-and-electricity.aspx
20. IRENA, 2017, GEOTHERMAL POWER TECHNOLOGY BRIEF, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2017/Aug/IRENA_Geothermal_Power_2017.pdf
21. Manwell J. F. Mc Gowan J. G. Rogers A. L. 2009 Wind energy explained: theory, design and application 2nd edition, Wiley, England
22. Gipe, P., 1995. Wind energy comes of age (Vol. 4). John Wiley & Sons.
23. Cao, W., Xie, Y. and Tan, Z., 2012. Wind turbine generator technologies. Advances in Wind Power, 1(1), pp.177-204. http://dx.doi.org/10.5772/51780
24. International energy Agencu (IEA), 2011, Technology Roadmap Geothermal Heat and Power, https://iea.blob.core.windows.net/assets/f108d75f-302d-42ca-9542-458eea569f5d/Geothermal_Roadmap.pdf
25. Zhang, Q., Watanabe, M. and Lin, T., 2010. Rural Biomass Energy Book 2020. Asian Development Bank.
26. International Energy Agency (Ed.), 2011. Deploying Renewables 2011: best and future policy practice, Renewable energy Markets & policies. OECD/IEA, Paris.
27. IBERDROLA, 2022, Do you know how offshore wind farms work?, https://www.iberdrola.com/sustainability/how-does-offshore-wind-energy-work
28. National Renewable Energy Laboratory (NREL), 2010, Large-Scale Offshore Wind Power in the United States, Published by September 2010, https://www.nrel.gov/docs/fy10osti/49229.pdf
29. American Geosciences Institute, What are the advantages and disadvantages of offshore wind farms?, https://www.americangeosciences.org/critical-issues/faq/what-are-advantages-and-disadvantages-offshore-wind-farms
30. U.S. Department of Energy, Environmental Impacts and Siting of Wind Projects, Published by Environmental Impacts and Siting of Wind Projects, https://www.energy.gov/eere/wind/environmental-impacts-and-siting-wind-projects
31. IBERDROLA, 2022, What is wind energy, how is it converted into electricity and what are its advantages?, https://www.iberdrola.com/sustainability/renewables-energy-wind-power
32. The National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA), 2021, Offshore Wind Energy, https://www.nopsema.gov.au/sites/default/files/2021-11/Offshore%20wind%20energy%20brochure_0.pdf
33. International Renewable Energy Agency, 2022, Wind Energy, https://www.irena.org/Energy-Transition/Technology/Wind-energy#:~:text=Wind%20turbine%20capacity%20has%20increased,and%208%2D12%20MW%20offshore.
34. National Renewable Energy Laboratory (NREL), 2020, The Leading Edge: April 2020 Wind Energy Newsletter, https://www.nrel.gov/wind/newsletter-202004.html
35. International Energy Agency, 2022, Wind Electricity, Published by September 2022, https://www.iea.org/reports/wind-electricity
36. Global Wind Energy Council (GWEC), 2022, Global Wind Report 2022, https://gwec.net/wp-content/uploads/2022/04/Annual-Wind-Report-2022_screen_final_April.pdf
37. Samad, A. and Suchithra, R., 2021. Marine power technology—wave energy. In Sustainable Fuel Technologies Handbook (pp. 241-267). Academic Press.
38. Sannasiraj, S.A. and Sundar, V., 2016. Assessment of wave energy potential and its harvesting approach along the Indian coast. Renewable Energy, 99, pp.398-409.
39. Anaa Lavaa, 2021, What Is Wave Energy: A Complete Guide, Published by 21 February 2021, https://www.linquip.com/blog/what-is-wave-energy/

40. Jordan Flagel, 2021, Sustainable Tech: Is Wave Energy the Next Renewable We Should Be Looking Towards for the Future?, Published by 3 November 2022, https://www.linq-consulting.com/post/is-wave-energy-the-next-renewable
41. Neill, S.P. and Hashemi, M.R., 2018. Fundamentals of ocean renewable energy: generating electricity from the sea. Academic Press.
42. Dernis Mediavilla, 2020, Wave Energy Technologies, Published October 2020, https://pamec.energy/about-pamec/our-scope/wave-energy/
43. Al Shami, E., Zhang, R. and Wang, X., 2018. Point absorber wave energy harvesters: A review of recent developments. Energies, 12(1), p.47.
44. Jordan Flagel, 2021, Sustainable Tech: Is Wave Energy the Next Renewable We Should Be Looking Towards for the Future?, Published by 23 September 2021, https://www.linq-consulting.com/post/is-wave-energy-the-next-renewable
45. World Economic Forum, 2022, Wave energy: can ocean power solve the global energy crisis?, Published by 22 March 2022, https://www.weforum.org/agenda/2022/03/wave-energy-ocean-electricity-renewables/#:~:text=Many%20countries%20%2D%20including%20Australia%2C%20China,are%20currently%20developing%20wave%20energy.
46. International Renewable Energy Agency (IRENA), 2020, Tidal Energy Technology Brief,
47. National Geographic, Tidal energy, https://education.nationalgeographic.org/resource/tidal-energy/
48. Pacific Northwest National Laboratory (PNNL). Tidal – Capturing tidal fluctuations with turbines, tidal barrages, or tidal lagoons. Published 16 February 2016. https://tethys.pnnl.gov/technology/tidal
49. NSCI Technology, 2019, Tidal Energy and How it Works, Published by 19 November 2019, https://nsci.ca/2019/11/19/tidal-energy-and-how-it-works/
50. Charlie Lai, 2022, Tidal Energy: Advantages, Disadvantages, and Future Trends, Published 5 August 2022, https://earth.org/what-is-tidal-energy/
51. International Renewable energy agency (IRENA), 2020, Innovation Outlook Ocean Energy Technologies, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2020/Dec/IRENA_Innovation_Outlook_Ocean_Energy_2020.pdf?rev=c5025e856b1f4a4c8eda2b8e5b10c974
52. Yekang Ko and Derek K. Schubert, 2011, South Korea's Plans for Tidal Power: When a "Green" Solution Creates More Problems. report. Nautilus Institute. Published by November 29, 2011. https://nautilus.org/napsnet/napsnet-special-reports/south-koreas-plans-for-tidal-power-when-a-green-solution-creates-more-problems/
53. Scarlett Evans, 2019, La Rance: learning from the world's oldest tidal project, Published by 28 October 2019, https://www.power-technology.com/features/la-rance-learning-from-the-worlds-oldest-tidal-project/
54. De Laleu, V., 2009, October. La Rance Tidal Power Plant. 40-year operation feedback–lessons learnt. In BHA Annual conference.< www. british-hydro. org/downloads/La% 20Rance-BHA-Oct (Vol. 202009).
55. Energy Information Administration (EIA), 2022, Hydropower explained – Tidal Power, Published by 10 August 2022, https://www.eia.gov/energyexplained/hydropower/tidal-power.php#:~:text=The%20Sihwa%20Lake%20Tidal%20Power,MW%20of%20electricity%20generation%20capacity.
56. International Renewable Energy Agency, 2014, Ocean Thermal Energy Conversion Technology Brief
57. Digger King, Ocean Thermal Energy Conversion, https://www.alternative-energy-tutorials.com/geothermal-energy/ocean-thermal-energy-conversion.html

58. Prasanna, 2022, Advantages and Disadvantages of Ocean Thermal Energy | Top 6 Advantages and Disadvantages of Ocean Thermal Energy, Published by 17 January 2022, https://www.aplustopper.com/advantages-and-disadvantages-of-ocean-thermal-energy/
59. CSIRO, Ocean Energy in Australia, https://www.csiro.au/en/research/natural-environment/oceans/ocean-energy
60. Mehmood, N., Liang, Z. and Khan, J., 2012. Diffuser augmented horizontal axis tidal current turbines. Research Journal of Applied Sciences, Engineering and Technology, 4(18), pp.3522-3532.
61. Ma, Y., Lam, W.H., Cui, Y., Zhang, T., Jiang, J., Sun, C., Guo, J., Wang, S., Lam, S.S. and Hamill, G., 2018. Theoretical vertical-axis tidal-current-turbine wake model using axial momentum theory with CFD corrections. Applied Ocean Research, 79, pp.113-122.
62. Ren, Y., Liu, B. and Zhang, T., 2019. Influences of winglets on the hydrodynamic performance of horizontal axis current turbines. Applied Ocean Research, 92, p.101931.
63. Brinck, D. and Jeremejeff, N., 2013. The development of a vertical axis tidal current turbine.
64. Fernandes, A.C., Rostami, A.B., Canzian, L.G. and Sefat, S.M., 2013, June. Vertical axis current turbine (VACT) and its efficiency. In International Conference on Offshore Mechanics and Arctic Engineering (Vol. 55423, p. V008T09A051). American Society of Mechanical Engineers.
65. Nugraha, A.S. and Rijanto, E., 2012. Ocean current energy conversion system in wallacea region using variable speed control approach. Journal of Mechatronics, Electrical Power, and Vehicular Technology, 1(1), pp.27-34.
66. Bobby Zarubin, 2015, Ocean Current Energy: Underwater Turbines, Published by 24 January 2015, http://large.stanford.edu/courses/2014/ph240/zarubin2/
67. Vega, L.A., 2013. Ocean thermal energy conversion. In Renewable Energy Systems (pp. 1273-1305). Springer, New York, NY.
68. International Renewable Energy Agency, 2014, Salinity Gradient Energy Technology Brief, https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2014/Salinity_Energy_v4_WEB.pdf
69. Shuxin Lim, 2020, Market to Watch: Asia Pacific to Become Largest Offshore Wind Market by 2030, Global Wind Energy Council (GQEC), Published by 9 September 2020. https://gwec.net/market-to-watch-asia-pacific-to-become-largest-offshore-wind-market-by-2030/
70. Ministry of Foreign Affair, 2022, China offshore wind - Factsheet for Dutch companies, Published by March 2022, Netherlands Enterprise Agency, https://www.rvo.nl/sites/default/files/2022/03/Rapport-Offshore-wind-China.pdf
71. 4C offshore, 2023, Offshore Wind farms in China, https://www.4coffshore.com/windfarms/china/
72. Lia Jia, 2022, First tidal light complementary photovoltaic power station put into operation, Published by June 2022, http://www.xinhuanet.com/energy/20220601/71346859a4274c64a3b969eeb165c0fe/c.html
73. Han Qing, 2023, China's ocean power stations set to go commercial, Published by 26 January 2023, https://chinadialogueocean.net/en/climate/chinas-ocean-power-stations-set-to-go-commercial/
74. TETHYS, 2022, Jiangxia Pilot Tidal Power Plant, https://tethys.pnnl.gov/project-sites/jiangxia-pilot-tidal-power-plant
75. Ahmed, S., and Abdalla, A., 2015, The Use of Tidal Energy in the World, International Journal of Innovative Science, Engineering & Technology, 3(11).
76. Wave Swell, King Island project, https://www.waveswell.com/king-island-project-2/
77. ARENA, 2023, Projects, https://arena.gov.au/projects/?project-value-start=0&project-value-end=200000000

78. Kitahan Shimposha, 2023, Large-scale offshore wind farm at Noshiro Port begins commercial operation for the first time in Japan, Published by 23 December 2022, http://kyodoshi.com/article/14150
79. Atsumi and Sakai, 2023, Trends in Offshore Wind Power Generation in Japan, Published by 16 February 2023, https://www.lexology.com/library/detail.aspx?g=7ab315b8-28a9-419e-8ce4-75920efebff5
80. IEA, 2021, Enhancing cyber resilience in electricity systems, Published April 2021, https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems
81. Australian Cyber Security Centre (ACSC), Cyber Security Terminology, https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-terminology
82. International Association of Ports and Harbors (IAPH), 2021. IAPH Cybersecurity Guidelines for Ports and Port Facilities. Published by July 2021. https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
83. Jones, K.D., Tam, K. and Papadaki, M., 2016. Threats and impacts in maritime cyber security.
84. Afenyo, M. and Caesar, L.D., 2023. Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, p.106493.
85. Nicaise, V., 2022. Cybermar´etique: a short history of cyberattacks against ports, 25th January Assessed at. https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/
86. Cyberstar, 2022, How Bad Was Maritime Cyber Security in 2021? Consider These 8 Incidents, Published by 15 March 2022, https://www.zkcyberstar.com/2022/03/15/how-bad-was-maritime-cyber-security-in-2021-consider-these-8-incidents/
87. de Peralta, F.A., Watson, M.D., Bays, R.M., Powers, F.E. and Boles, J.R., 2020. Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems.
88. Andy Bochman and Ian Ralby, 2021, Cybersecurity concerns for the energy sector in the maritime domain, Published by 6 December 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/cybersecurity-concerns-for-the-energy-sector-in-the-maritime-domain/
89. Xu, Y., 2020. A review of cyber security risks of power systems: from static to dynamic false data attacks. Protection and Control of Modern Power Systems, 5(1), p.19.
90. Xiang, Y. and Wang, L., 2017. A game-theoretic study of load redistribution attack and defense in power systems. Electric Power Systems Research, 151, pp.12-25.
91. Xiang, Y., Wang, L. and Liu, N., 2017. Coordinated attacks on electric power systems in a cyber-physical environment. Electric Power Systems Research, 149, pp.156-168.
92. Adnan Durakovic, 2022, Wind Firms Cannot Afford to Ignore Increasing Cyber Security Threats – DNV, Published by 8 December 2022, https://www.offshorewind.biz/2022/12/08/wind-firms-cannot-afford-to-ignore-increasing-cyber-security-threats-dnv/
93. Peter Warner, 2020, Increasing Cyber Security In Wind Farms And Other Renewables, Published by 2 November 2020, https://wizardcyber.com/increasing-cyber-security-in-wind-farms-and-other-renewables/
94. Frame Communications, Do you know the costs of windfarm hacking?, https://frame.co.uk/windfarm-network-security/do-you-know-the-costs-of-windfarm-hacking-why-you-need-to-improve-windfarm-cybersecurity/
95. Kim, S., Heo, G., Zio, E., Shin, J. and Song, J.G., 2020. Cyber attack taxonomy for digital environment in nuclear power plants. Nuclear Engineering and Technology, 52(5), pp.995-1001.
96. Mike Hetz, 2021, Managing cyber security risks in the power sector, https://www.ge.com/gas-power/resources/articles/2021/managing-cybersecurity-risks-in-power-sector

97. Martin, M., Reynolds, T., Sanghvi, A., Cox, S. and Elsworth, J., 2021. Power sector cybersecurity building blocks (No. NREL/TP-5R00-79396). National Renewable Energy Lab.(NREL), Golden, CO (United States). file:///Users/arezoo/Downloads/79396.pdf
98. Mike Burgard, 2021, The 5 Elements of a Successful Security Awareness Program, Published by 2 June 2021, https://www.marconet.com/blog/security-awareness-program
99. Jordan Daly, 2023, 12 Essential Security Awareness Training Topics for 2023, https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020
100. Algena Lee, 2021, Asia-Pacific - An offshore wind powerhouse, Published 22 February 2021, https://www.spglobal.com/commodityinsights/en/ci/research-analysis/asia-pacific-an-offshore-wind-powerhouse.html
101. ARENA, 2022, Tidal Energy in Australia, https://arena.gov.au/projects/tidal-energy-australia-assessing-resource-feasibility-australias-future-energy-mix/
102. OTEX News, 2021, Hybrid OTEC Equipment for Malaysia Japan SATREPS Project Completed, Published by 26 April 2021, http://otecnews.org/entities/hybrid-otec-mechanism-for-malaysia-japan-satreps-project-completed/
103. Petterson, M.G. and Kim, H.J., 2020. Can Ocean Thermal energy conversion and seawater utilisation assist small island developing states? A Case study of Kiribati, Pacific Islands Region. In Ocean Thermal Energy Conversion (OTEC)-Past, Present, and Progress. IntechOpen.
104. Ellabban, O., Abu-Rub, H. and Blaabjerg, F., 2014. Renewable energy resources: Current status, future prospects and their enabling technology. Renewable and sustainable energy reviews, 39, pp.748-764.
105. Cybersecurity and Infrastructure Security Agency (CISA), SECTOR SPOTLIGHT: Cyber-Physical Security Considerations for the Electricity Sub-Sector, https://www.cisa.gov/sites/default/files/publications/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf
106. US department of Energy, 2020, Roadmap for Wind Cybersecurity, June 2020, https://www.energy.gov/sites/prod/files/2020/07/f76/wind-energy-cybersecurity-roadmap-2020v2.pdf
107. Datta, A. and Rahman, M.A., 2017, November. Cyber Threat Analysis Framework for the Wind Energy Based Power System. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 81-92).
108. Singh, V.K., Sharma, R. and Govindarasu, M., 2020, August. Testbed-based performance evaluation of attack resilient control for wind farm scada system. In 2020 IEEE Power & Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.
109. Liu, Y., Ning, P. and Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1), pp.1-33.
110. Shih, Y., 2022. Measured wind data in digital: Develop and optimize offshore wind farm SCADA by IEC 60870-5-104 protocol and DMZ. Energy Reports, 8, pp.1231-1242.
111. Wu, H., Liu, J., Liu, J., Cui, M., Liu, X. and Gao, H., 2019. Power grid reliability evaluation considering wind farm cyber security and ramping events. Applied Sciences, 9(15), p.3003.
112. Zhang, Y., Xiang, Y. and Wang, L., 2016. Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. IEEE transactions on smart grid, 8(5), pp.2343-2357.
113. Yan, J., Liu, C.C. and Govindarasu, M., 2011, March. Cyber intrusion of wind farm SCADA system and its impact analysis. In 2011 IEEE/PES Power Systems Conference and Exposition (pp. 1-6). IEEE.

114. Office of Energy Efficiency and Renewable Energy, How do wind turbines work? U.S. Department of Energy, Washington, DC (energy.gov/eere/wind/how-do-wind-turbines-work), 2016.
115. Linsday, J., Briand, D., Hill, R.R., Stinebaugh, J.A. and Benjamin, A.S., 2008. Wind turbine reliability: a database and analysis approach (No. SAND2008-0983). Sandia National Laboratories (SNL), Albuquerque, NM, and Livermore, CA (United States).
116. Sheng, S., 2013. Report on wind turbine subsystem reliability-a survey of various databases (presentation) (No. NREL/PR-5000-59111). National Renewable Energy Lab.(NREL), Golden, CO (United States).
117. Staggs, J., Ferlemann, D. and Shenoi, S., 2017. Wind farm security: attack surface, targets, scenarios and mitigation. International Journal of Critical Infrastructure Protection, 17, pp.3-14.
118. Gonen, T., 2015. Electric power distribution engineering. CRC press.
119. Andy Greenberg, 2017, Researchers Found They Could Hack Entire Wind Farms, https://www.wired.com/story/wind-turbine-hack/
120. Costoya, X., DeCastro, M., Carvalho, D., Arguilé-Pérez, B. and Gómez-Gesteira, M., 2022. Combining offshore wind and solar photovoltaic energy to stabilize energy supply under climate change scenarios: A case study on the western Iberian Peninsula. Renewable and Sustainable Energy Reviews, 157, p.112037.
121. Vo, T.T.E., Ko, H., Huh, J. and Park, N., 2021. Overview of possibilities of solar floating photovoltaic systems in the offshore industry. Energies, 14(21), p.6988.
122. Office of Energy Efficiency and Renewable Energy, 2020, Solar Cybersecurity Basics, https://www.energy.gov/eere/solar/solar-cybersecurity-basics#:~:text=Solar%20energy%20technologies%20can%20be,manage%20the%20electric%20power%20grid
123. Tom Kuster, 2021, The future of cybersecurity: How renewable power plant controls protect inverters from hacks and attacks, https://www.solarpowerworldonline.com/2021/03/renewable-power-plant-controls-protect-inverters-from-hacks-and-attacks/
124. Energy, 2023, Microgrids, https://www.energy.vic.gov.au/renewable-energy/microgrids#:~:text=A%20microgrid%20can%20be%20thought,well%20as%20battery%20energy%20storage.
125. García Vera, Y.E., Dufo-López, R. and Bernal-Agustín, J.L., 2019. Energy management in microgrids with renewable energy sources: A literature review. Applied Sciences, 9(18), p.3854.
126. Tuyen, N.D., Quan, N.S., Linh, V.B., Van Tuyen, V. and Fujita, G., 2022. A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. IEEE Access, 10, pp.35846-35875.
127. Wang, W. and Lu, Z., 2013. Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), pp.1344-1371.
128. Li, Z., Shahidehpour, M. and Aminifar, F., 2017. Cybersecurity in distributed power systems. Proceedings of the IEEE, 105(7), pp.1367-1388
129. Wu, Z., Tazvinga, H. and Xia, X., 2015. Demand side management of photovoltaic-battery hybrid system. Applied Energy, 148, pp.294-304.
130. Liu, X., Shahidehpour, M., Cao, Y., Wu, L., Wei, W. and Liu, X., 2016. Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. IEEE transactions on smart grid, 8(3), pp.1330-1339.
131. Liu, Z., Mohammadzadeh, A., Turabieh, H., Mafarja, M., Band, S.S. and Mosavi, A., 2021. A new online learned interval type-3 fuzzy control system for solar energy management systems. IEEE Access, 9, pp.10498-10508.

132. FORCE, J.T. and INITIATIVE, T., 2010. Guide for applying the risk management framework to federal information systems. NIST special publication, 800, p.37.
133. Faquir, D., Chouliaras, N., Sofia, V., Olga, K. and Maglaras, L., 2021. Cybersecurity in smart grids, challenges and solutions. AIMS Electronics and Electrical Engineering, 5(1), pp.24-37.
134. "Guidelines for smart grid cybersecurity," National Institute of Standards and Technology, USA, Tech. Rep. NISTIR 7628 Revision 1, September 2014.
135. "ISO/IEC 27001 Information security management systems," [Online] https://www.iso.org/standard/27001, 2022.
136. "CIS Critical Security Controls, Version 8," [Online] https://www.cisecurity.org/controls, 2022.
137. S. Gros, "A critical view on CIS controls," 2019.
138. P. P. Roy, A high-level comparison between the NIST cyber security framework and the iso 27001 information security standard. IEEE, 2020.
139. Kim Zetter, 2016, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
140. John Hultquist, 2016, Sandworm Team and the Ukrainian Power Authority Attacks, https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team
141. Threat Hunter Team, 2021, Throwback Attack: Dragonfly 2.0 targets energy sectors, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-dragonfly-2-0-targets-energy-sectors/
142. John Leyden, 2018, Ukraine claims it blocked VPNFilter attack at chemical plant, https://www.theregister.com/2018/07/13/ukraine_vpnfilter_attack/
143. Catalin Cimpanu, 2018, Ukraine Says It Stopped a VPNFilter Attack on a Chlorine Distillation Station, https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/
144. Charlie Osborne, 2020, Energy company EDP confirms cyberattack, Ragnar Locker ransomware blamed, https://www.zdnet.com/article/amazon-tricked-and-trapped-millions-into-prime-subscriptions-says-ftc/
145. Sergiu Gatlan, 2020, RagnarLocker ransomware hits EDP energy giant, asks for €10M, https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
146. Ionut Ilscu, 2018, Eletrobras, Copel energy companies hit by ransomware attacks, https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/#:~:text=Centrais%20Eletricas%20Brasileiras%20(Eletrobras)%20and,key%20players%20in%20the%20country.
147. Abeerah Hashim, 2021, Two Brazil Electric Power Utility Firms Disclosed Ransomware Attack Around The Same Time, https://latesthackingnews.com/2021/02/08/two-brazil-electric-power-utility-firms-disclosed-ransomware-attack-around-the-same-time/
148. Deniz Mustafa, 2021, Danish wind turbine company vestas hit by cyber-attack, https://www.securiwiser.com/news/danish-wind-turbine-company-vestas-hit-by-cyber-attack/
149. Reuters, 2021, Vestas data 'compromised' by cyber-attack, https://www.reuters.com/markets/europe/vestas-data-compromised-by-cyber-attack-2021-11-22/
150. Gail Rajgor, 2022, Wind turbine maker Nordex shuts down systems as cyber-attack hits, https://www.windpowermonthly.com/article/1751954/wind-turbine-maker-nordex-shuts-down-systems-cyber-attack-hits#:~:text=In%20November%202021%2C%20Danish%20turbine,data%20on%20the%20dark%20web.

151. Lawrence Abrams, 2022, Wind turbine firm Nordex hit by Conti ransomware attack, https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/
152. Michael Behr, 2022, Scottish Power Parent Company Iberdrola Hit by Cyber-attack, https://www.digit.fyi/iberdrola-cyberattack-scottish-power/
153. Mostafa Rachwani, 2022, EnergyAustralia latest to be hit by cyber-attack as details of hundreds of customers exposed, https://www.theguardian.com/australia-news/2022/oct/21/energyaustralia-latest-to-be-hit-by-cyber-attack-as-details-of-hundreds-of-customers-exposed
154. HSB Marine, 2023, What Are Marine Renewable Energy Technologies?, https://www.hsbmarine.com/blog/what-are-marine-renewable-energy-technologies
155. Xu G, Shi Y, Sun X, Shen W. Internet of Things in Marine Environment Monitoring: A Review. Sensors (Basel). 2019 Apr 10;19(7):1711. doi: 10.3390/s19071711.
156. Wang, X., Li, L., Palazoglu, A., El-Farra, N.H. and Shah, N., 2018. Optimization and control of offshore wind farms with energy storage systems. *IFAC-PapersOnLine*, *51*(18), pp.862-867.
157. Tina Casey, 2022, The Latest Energy Storage Gizmo Is An "Ocean Battery" With A Bladder, https://cleantechnica.com/2022/01/07/the-latest-energy-storage-gizmo-is-an-ocean-battery-with-a-bladder/
158. WSP, 2023, Marine Infrastructure, https://www.wsp.com/en-au/sectors/marine-infrastructure