Renewable Energy in Water Desalination: Route of Technology, Vulnerabilities and Solutions Towards Cyber Intrusion

Aya Elshinawy[1] and Dr. Abdulla Ismail[2]

[1]Graduate Student, Dept. of Electrical Engineering, Rochester Institute of Technology, Dubai, UAE
[2]Professor, Dept. of Electrical Engineering, Rochester Institute of Technology, Dubai, UAE

---***---

Abstract - *The diminishing of fossil fuels is inclining day by day which poses a huge dilemma that possesses a challenge for researchers to try and unlock the key for technologies where energy is sustainable. Mankind was created in a self-sustaining planet where the Sun is the peak of the energy chain which branches out many renewable and sustainable energy sources. Scientists have been exploring the possibilities of exploiting the energy of the sun in many ways including, photovoltaics for electricity generation, solar thermal applications for heating as well as electricity generation, energy storage applications and Desalination. Water scarcity is one of the most problematic issues in the world, specifically in the Middle East, as fresh water is very rare and geographically allocated in specific regions. The energy sector is complicated and fraught with uncertainty. Geopolitical, economic, environmental, technological, and social factors are all present. Integration of RES in desalination plants triggers an additional vulnerability to cyber security threats. This report offers a comprehensive approach to cyber-attacks in desalination plants powered by RES and suggested solution are proposed that encompass the lessons learnt from many researchers within the last 30 years.*

Key Words: **Renewable Energy Systems (RES), Water Desalination Plants, Cyber Security, Cyber Attacks.**

1.INTRODUCTION TO WATER DESALINATION PLANTS

Desalination is a series of industrial processes performed to remove all or part of excess salts and minerals from water. Several methods of desalination were developed [1]. The most common processes can be classified under two main types as shown in Figs. 1.1, 1.2, 1.3 and 1.4, thermal processes and membrane processes.

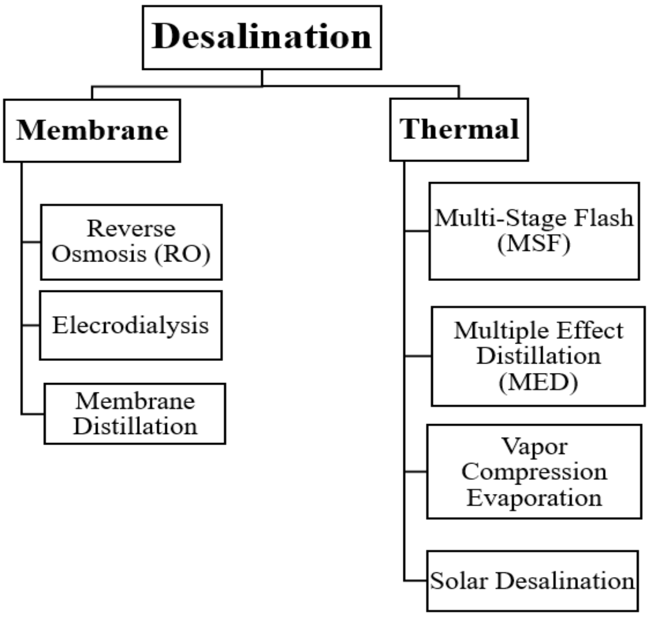

Fig. 1.1 Classification of water desalination processes.

1.1 Membrane Processes

The membrane technologies depend mainly on using permeable membranes that water can pass through, while separating the salt. They separate water and salt into two different regions with different concentrations.

There are three different methods in this category as described next.

1.1.1 Reverse Osmosis

In reverse osmosis process, pressurized water is separated through a membrane without heating. The solvent is forced to flow from low solvent concentration to high solvent concentration opposite to the natural flow by applying pressure larger than osmotic pressure. Because of its simplicity and cheap energy cost in compared to distillation-based thermal processes, RO technology is used in more than half of the world's deployed desalination plants. Because of advancements in RO technology in terms of membrane material and energy usage, which has permitted a drop in the cost of pure water production, the market for RO-based desalination has experienced a constant growth. The semipermeable membrane known as the RO membrane, which preferentially permits water molecules to flow across it while inhibiting the passage of salts under the influence of externally applied pressure, is at the core of RO-based separation.

The problems associated with RO processes are mainly, scaling, baron removal and brine disposal. During seawater filtration via a membrane, the concentration of certain marginally soluble salts, such as divalent and multivalent salts, rises. To begin with, as the salts' solubility limit hits supersaturation, they tend to precipitate and create a scale on the membrane surface, reducing the productivity of the RO process. Anti-scalants are a frequently used approach for preventing scaling caused by salts such as silica, iron, barium sulfate, calcium carbonate, gypsum, and others. The presence of these salts in varying concentrations is determined by the feed water source. The anti-scaling chemicals raise the threshold for the production of scale on the membrane surface. Organic polymers, surface active reagents, organic phosphonates, and phosphates, which are often employed anti-scalants, interfere with the kinetics of crystal nucleation [1]. Secondly, boron removal by RO membranes is one of the trendiest subjects that is still a difficulty today. According to WHO recommendations and according to rules, the maximum quantity of boron allowed in drinking water is 0.5 mg/L. The efficacy of the RO method for boron removal has not proven sufficient, owing to the nature of the element in water.

Lastly, brine or brine-blowdown is a desalination plant reject with an extremely high salinity compared to seawater. In addition to high amounts of TDS, brine may contain additional components such as halogenated organic compounds, anti-scalants, antifoulants, corrosive materials, acid, and so on . Brine disposal technologies in use include direct discharge into the sea, surface discharge, evaporation ponds, and well injection. The disposal of such highly concentrated saline fluid on land or sea poses a significant environmental risk. Direct discharge into the sea has an impact on the microalgal population, plant life, and the creation of sludge. Brine disposal through evaporation ponds is often used for inland RO desalination facilities, i.e., in dry and semi-arid places where marine discharge is not practicable and solar energy is abundant. Unfortunately, evaporation ponds take up too much room, and surface discharge may have an impact on soil and plant production [1].

1.1.2 Electrodialysis

Electrodialysis (ED) is an electrochemical separation process based on the fact that all salts dissolve in water as ions, either positive (cations) or negative (anions), and they move towards electrodes which have opposite charge. An ion exchange membrane is charged electrically to be used as a separator under the effect of an electric potential. The membranes are cation- or anion-selective, which means that they can be structured to allow either cations or anions to pass [2]. A membrane must have the following general properties: a) a high transport number of counterions, b) a high mechanical strength, c) a cheap cost, d) a high chemical stability and durability, e) a low electrical resistance, and f) a low salt diffusion coefficient. There are several advantages of electrodialysis as a form of desalination and these include:

- less membrane fouling or scaling due to electrodialysis reversal,
- excellent water recovery rates, even with high sulfate content raw water,
- the increased chemical and mechanical stability of membranes results in a longer life span,
- the procedure requires less raw water pre-treatment and may readily be modified to different feed water quality; hence, the cost will be reduced,
- possible to clean manually without damaging the membrane properties

Despite all of its advantages, ED has a few drawbacks in the desalination field, making it a less appealing option in recent years. As a result, RO has mostly supplanted ED desalination techniques. One of the ED process's shortcomings is its restricted applicability. The ED technique is typically only appropriate for brackish water with a salinity of less than 12,000 mg/L TDS. Because the salinity of the water to be treated is directly related to power consumption, the cost of ED desalination is substantially greater than that of RO when the salinity of the water surpasses 12,000 ppm TDS. Moreover, non-toxic components such as viruses or bacteria are not eliminated from the feed stream [2].

1.1.3 Membrane Distillation

Membrane distillation is a thermally driven separation technology, combines the use of membrane and evaporation process. A micro-porous hydrophobic membrane benefits from the temperature gradient between the incoming solution, and the space on the other side of the membrane, whereby a vapor pressure difference is created. This pressure difference leads the produced vapor to pass through the membrane and condensate on the other side, whereas the liquid cannot transfer due to the hydrophobicity of the membrane [3]. Although MD is fundamentally less energy efficient than RO, its capacity to treat high-salinity brines that RO cannot treat with low-grade thermal energy rather than electricity is particularly beneficial. MD has the potential to provide sustainable water treatment in regions where low-grade or renewable heat sources, such as waste heat from industrial operations or solar thermal collectors, are easily accessible. The MD process has a significant advantage in that it may employ low-grade waste heat or renewable energy to minimize its energy costs. Whereas standard thermal distillation techniques need the feed water to be boiled, the MD process may function at a low input temperature (as low as 40 °C). Using these heat sources on-site, MD can be a very cost-effective technique for treating hypersaline solutions and other difficult fluids. Despite significant work on MD over the last 30 years, there is still ambiguity about its general viability and efficacy.

1.2 Thermal Desalination Processes

Thermal desalination process simply depends on the principle of evaporation and condensation. Saline water is heated until it evaporates. Later, this vapor condensate as fresh water while the salt is left behind [4].

There are three methods in this category, explained as follows.

1.2.1 Multi-Stage Flash Distillation

A Multi stage flash plant consists of a series of containers with a heat exchanger and a condensate collector in each container. These containers are called stages. After the hot end of the heat exchanger, there is a vessel called the brine heater as can be seen in Fig. 1.2 below [5].

The incoming feed water goes to the brine heater passing through the heat exchanger tubes. Thus, the tubes are cooled, and water is heated up in turn. This reduces the amount of heat needed in the brine to increase the water temperature. When the feed water reaches the brine heater, it is heated to a temperature less than the boiling temperature. Then, it flows through the sequenced stages. Each stage has different pressure lower than ambient pressure. This low pressure causes the water to boil so much faster and flashing to steam. This steam is converted to fresh water by the condenser tubes that run through each stage.

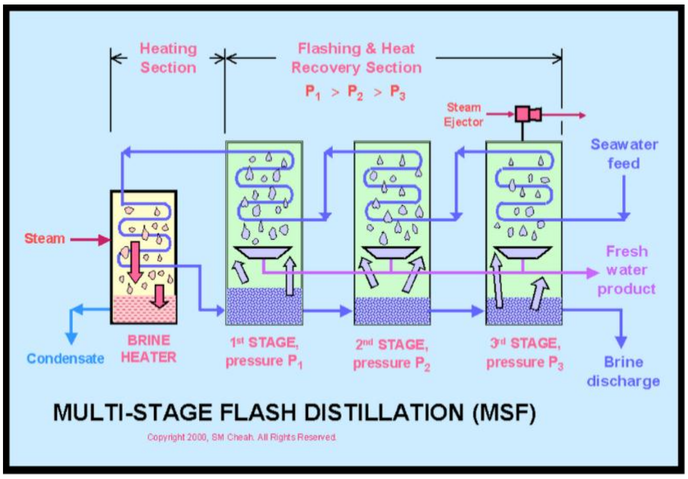
Heating Section
Flashing & Heat Recovery Section
$P_1 > P_2 > P_3$
Steam Ejector
Seawater feed
Steam
Fresh water product
Condensate
BRINE HEATER
1st STAGE, pressure P_1
2nd STAGE, pressure P_2
3rd STAGE, pressure P_3
Brine discharge
MULTI-STAGE FLASH DISTILLATION (MSF)
Copyright 2000, SM Cheah. All Rights Reserved.

Fig. 1.2 MSF desalination process stages [6]

MSF accounts for 90% of overall thermal output and 42% of total global desalination production. As a result, it is one of the most widely utilized desalination systems [5]. It is the most dependable of all desalination systems. MSF operates at top brine temperatures (TBT) ranging from 90°C to 120°C. The greatest temperature to which saltwater in a cogeneration system is heated in the brine heater by low-pressure steam. Some of the processes advantages over other desalination techniques are, it provides high-quality product water by recovering 25 %-50% in a high-temperature recyclable (recirculate) MSF plant, the total dissolved salts (TDS) of MSF processes are less than 50 mg/L and it requires very little preparation of the feed water. Furthermore, the plant process and cost are not affected by salt level and heat energy may be obtained by combining it with electricity generation, a process known as cogeneration. On the other hand, MSF is an energy-intensive procedure, it also requires a significant capital commitment and has a bigger environmental and material imprint. Also it is worth noting that corrosion issues emerge when inferior materials are employed and its maintenance necessitates the shutdown of the entire facility as well as, it has a poor recovery ratio (product rate/seawater feed rate).

1.2.2 Multi-Effect Distillation

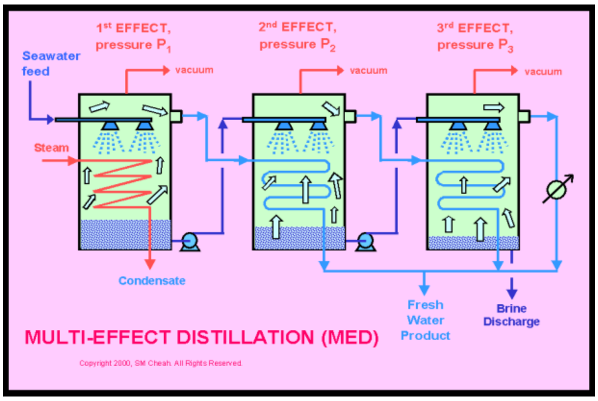
1st EFFECT, pressure P_1
2nd EFFECT, pressure P_2
3rd EFFECT, pressure P_3
Seawater feed
vacuum
vacuum
vacuum
Steam
Condensate
Fresh Water Product
Brine Discharge
MULTI-EFFECT DISTILLATION (MED)
Copyright 2000, SM Cheah. All Rights Reserved.

Fig. 1.3 MED desalination process stages [6].

During this process, the feed of saline water undergoes multiple boiling in a series of evaporators called effects. It is based on the precept of evaporation and condensation by the reduced pressure in the different effects without adding heat as can be observed in Fig. 1.3, except to the first effect.

In the first effect, the seawater is sprayed onto evaporator tubes and heated by steam that is externally supplied to them. Then, it is heated up to the boiling point. Some of the water evaporates and flows into the tubes of the next effect. while this vapor gives heat to remaining feedwater that is also supplied to the next effect to evaporate it, it condenses forming fresh water [6]. Advantages of MED include, energy efficiency because it uses waste heat created throughout the process to generate extra steam, which can then be utilized to heat the following step. When compared to alternative desalination systems, this results in lower energy use. As well as, cost-effectiveness. MED offers lower operational costs than other desalination technologies such as reverse osmosis (RO) because to decreased energy consumption and the ability to recover waste heat generated during the process. MED's durability allows it to stand out withing desalination techniques. MED systems are noted for their extended longevity and durability, with some units surviving up to 30 years. This is due to the fact that MED employs basic and dependable technology that is simple to maintain. Since MED has a high water recovery rate, a greater proportion of the feed water is transformed into clean water. This is because MED achieves significant amounts of water recovery through numerous phases of evaporation and condensation. MED does not require any chemicals for the desalination process, making it a more ecologically friendly alternative when compared to other desalination systems that do.

MED poses some challenges in its applications, such as, its high energy consumption. Since MED takes a substantial amount of electricity to function, it may be costly to run. This is due to the fact that the process includes heating and evaporating water in numerous stages to produce purified water, which consumes a significant amount of energy. Another challenge, similar to RO is , scaling. MED is susceptible to scaling, which happens when mineral deposits form on the distillation unit's heat transmission surfaces. Scaling can impair system efficiency and raise maintenance expenses.

Moreover, corrosion is another limitation to MED. The MED process's high temperatures and salt levels can cause corrosion of the equipment. This can result in leaks and other problems that compromise the system's efficiency and safety. MED required regular maintenance to guarantee peak performance. Cleaning and replacing components may be required, which may be time-consuming and costly. Lastly, its environmental effect, the high energy consumption of MED might have a detrimental environmental impact, especially if the energy is generated from fossil fuels. Furthermore, if the brine created as a byproduct of the process is not properly disposed of, it can be detrimental to marine life.

1.2.3 Vapor-Compression Evaporation

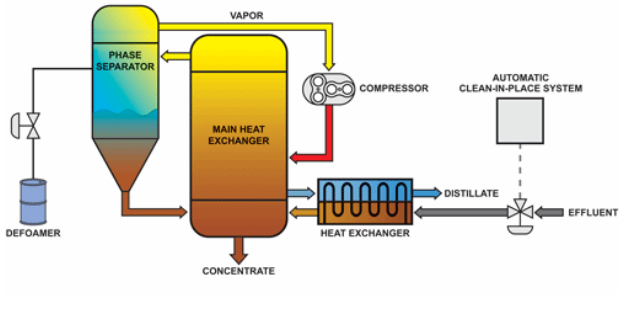

Fig. 1.4 VCE desalination process stages [8]

In the Vapor-compression evaporation (VCE) technique, water vapor is removed from the evaporator and compressed to a higher pressure. This increase of pressure leads the condensation temperature to increases too, which means that this condensed vapor will have enough heat that can be used to evaporate more water from the mother feed. Vapor compression can be done mechanically using a mechanical compressor, or thermally be a steam jet. The leftover saline water is recirculated by a pump, so that more fresh water can be obtained as shown in Fig. 1.4 [7].

VCE is an energy-efficient technique since it employs mechanical compressors to provide the pressure needed to evaporate the water. As a result, it consumes less energy than other desalination techniques, like as thermal distillation. It is also a cost-effective desalination technology since it requires less capital investment than other technologies like reverse osmosis (RO). As a result, it is a popular choice in locations with low financial resources. VCE is a straightforward technique that may be carried out with little technological knowledge. The method requires only a few components, making it simple to maintain and run [8].

The water recovery rate of VCE is high, which indicates that a significant portion of the feed water is transformed into clean water. VCE is capable of handling high salinity water, making it an excellent option for desalination of saltwater and other high salinity water sources.

Some of the limitations that accompany VCE are, its restricted scalability. It is not appropriate for large-scale desalination operations since it consumes a lot of energy to run. VCE is susceptible to fouling, which happens when pollutants collect on the heat transfer surfaces of the evaporator. This can degrade system efficiency and raise maintenance expenses [7].

1.3 Comparison of above mentioned desalination technologies

Each desalination method has advantages and disadvantages, and the process chosen is determined by criteria such as feedwater quality, the volume of fresh water required, energy cost, and total system cost. Currently RO is the most popular desalination method as it is quite inexpensive, uses little energy, and provides high-quality water. RO is extensively utilized in small to medium-sized desalination facilities as well as in the production of drinking water. On the other hand, MSF is a method that is appropriate for large-scale desalination facilities that require significant amounts of freshwater. MSF can efficiently generate vast volumes of freshwater. However, ED is frequently used in conjunction with RO to lower the total energy consumption of the process. Although ED is successful in removing ions from water, it requires more energy than other desalination techniques, therefore, is difficult to act independently as a desalination plant. To address the specific demands of a particular application, a mix of desalination methods is ideally required.

1.4 Challenges and limitations of desalination plants

In addition to the advantages that were stated above on each desalination process independently, it is worth mentioning the current limitations and challenges that the desalination sector faces. Desalination is a high-energy process that requires a large amount of power or fuel to run. This can result in higher operational expenses and higher greenhouse gas emissions. Therefore, leading to pollution as well as, if brine is not properly handled, it can destroy marine life and ecosystems. Additionally, the high capital and operational expenses might make investment in desalination infrastructure difficult to justify. Although desalination is frequently viewed as a solution to water shortage, it can give a false sense of security and hinder investment in more sustainable water management measures, such as water recycling. Lastly, desalination plants are at risk of cyber and physical attacks due to their importance as infrastructures to the economy of the country therefore due to mainly sociopolitical aspects, desalination plants are at key risk of these attacks as detailed in this survey paper [9]. This issue is a key challenge in desalination plants and hence is the driving factor of this report.

2.INTRODUCTION TO RENEWABLE ENERGY SYSTEMS (RES)

Given that carbon dioxide is the primary component of greenhouse gases (GHGs), there is widespread concern about lowering carbon emissions. Numerous countries have begun to build power producing facilities that employ renewable energy sources. The significance of alternative energy sources is linked to climate change issues caused by the over use of fossil fuels. Energy security, economic consequences, and carbon dioxide emission reduction are the three key motivators driving the expansion of renewable energy technology.

The phrase "alternative energy" refers to any kind of energy other than traditional energy sources. Renewable energy sources have received a lot of attention in recent years. The supply of renewable energy is steadily expanding. These technologies may not be cost competitive with traditional fuels in terms of production, but they may be when externalities such as environmental and social impacts are included. It should also be emphasized that economies of scale may play a significant impact in lowering unit manufacturing costs. Transmission and distribution costs, as well as technology, are similar across conventional and renewable energy [10]. Below is a brief introduction of the main renewable energy sources developed around the world:

2.1 Wind Energy

Wind energy is used to generate power by turning the kinetic energy of moving air into electricity [11]. Wind turbines convert wind energy into electricity by utilizing the aerodynamic force of the rotor blades which can be seen in Fig. 2.1, which function similarly to an airplane wing or helicopter rotor blade. As wind blows across the blade, the air pressure on one side drops. Lift and drag are created by the differential in air pressure between the two sides of the blade. The lift force is greater than the drag force, causing the rotor to spin. The rotor is connected to the generator either directly (if it is a direct drive turbine) or via a shaft and a series of gears (a gearbox), which speeds up the rotation and allows for a physically smaller generator. This conversion of aerodynamic force to generator rotation generates electricity [12].

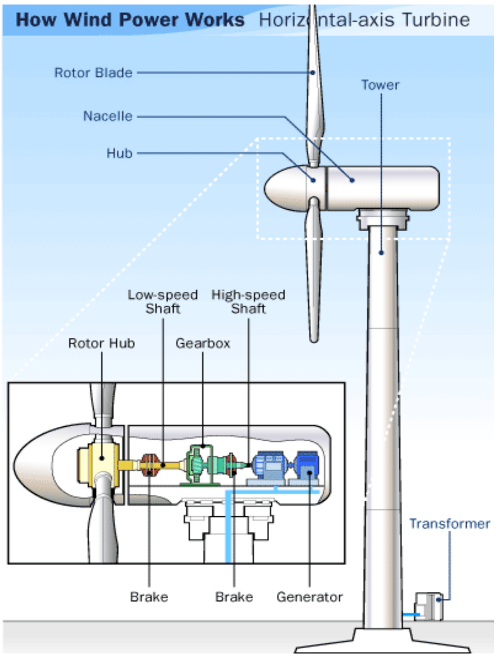

Fig. 2.1 Mechanism of wind turbine [14].

The bulk of wind turbines are classified into two types:

- Horizontal-Axis Turbines: Many people envision horizontal-axis wind turbines when they think about wind turbines. They typically have three blades and run "upwind," with the turbine turning at the top of the tower so the blades face into the wind.
- Vertical-Axis Turbines: There are various types of vertical-axis wind turbines, including the eggbeater-style Darrieus model, named for its French creator. These turbines are omnidirectional, which means they don't need to be pointed into the wind to work [13].

Even though wind energy is an efficient source of RES, there are limitations that makes it less competitive in comparison to Solar and Hydroelectric energy sources. To begin with, wind is a variable and intermittent energy source, and its availability varies based on the time of day, season, and weather conditions[14]. Because of this fluctuation, wind energy may need to be supplemented by other energy sources as a major source of electricity. Furthermore, wind turbines must be positioned in places with constant and strong wind patterns in order to be successful. This frequently necessitates their installation in remote places, which can increase installation and maintenance costs and make energy transmission more difficult. In addition, because of their size and aesthetic influence on the environment, wind turbines can be socially controversial. They may also cause noise pollution, which may be an issue for surrounding communities. This can make obtaining permits and community support for wind energy projects challenging. Lastly, wind turbines can endanger birds and other species, especially if they are near migration routes or nesting locations.

2.2 Solar PV

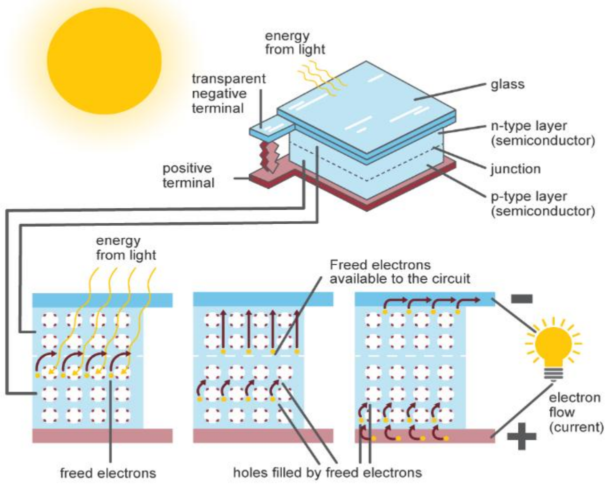
energy from light
transparent negative terminal
glass
n-type layer (semiconductor)
junction
positive terminal
p-type layer (semiconductor)
energy from light
Freed electrons available to the circuit
−
electron flow (current)
+
freed electrons
holes filled by freed electrons

Fig. 2.2 Photovoltaic cell energy production [15].

Photons, or solar energy particles, make up sunlight. These photons have variable levels of energy that correspond to the solar spectrum's various wavelengths. A PV cell is constructed using semiconductor material. Photons that strike a PV cell may bounce off of it, travel through it, or be absorbed by the semiconductor material as demonstrated in Fig. 2.2. Only photons that have been absorbed offer energy to create electricity. When enough sunshine (solar energy) is absorbed by the semiconductor material, electrons are dislodged from the substance's atoms. Particular treatment of the material surface during manufacture makes the front surface of the cell more responsive to dislodged, or free, electrons, which naturally travel to the cell's surface.

The migration of electrons, each carrying a negative charge, toward the cell's front surface causes an electrical charge imbalance between the cell's front and rear surfaces. As a result of this imbalance, a voltage potential is created, similar to the negative and positive terminals of a battery. Electrons are absorbed by the cell's electrical conductors. When conductors in an electrical circuit are linked to an external load, such as a battery, electricity flows across the circuit [15].

Solar PV systems can be used to supply power on a commercial scale, or they can be deployed in smaller clusters for mini-grids or individual use. The cost of creating PV modules has plummeted dramatically in the last decade, making them not only accessible but also sometimes the least costly energy source [16].

Solar PV outperforms other renewable energy sources such as wind, hydro, and geothermal, however, it does have significant challenges and limitations that must be considered. Solar PV systems generate power only during the day when the sun is shining which makes them less reliable than other RES, such as wind and hydro, which can provide electricity around the clock. To provide electricity when the sun is not shining, such as at night, solar PV systems must be linked with energy storage devices. Energy storage solutions can be costly, increasing the entire cost of a solar PV system. In order to produce the same amount of electricity by a wind turbine for example, a solar PV system would require a large amount of land, which can be difficult in locations where land is rare or expensive. Moreover, due to the usage of rare earth metals and other resources, the manufacture of solar panels can have a detrimental environmental impact.

Most conventional and industrial solar PV systems have an efficiency ranging from 20-25%, which means they can only convert a certain quantity of sunshine into power, whereas, wind turbines have recorded efficiencies up to 40% [13]. Lastly, solar PV systems must be maintained on a regular basis to ensure that they are operating properly. This includes cleaning the panels, repairing worn-out components, and monitoring the system's efficiency which can be time and capital consuming.

2.3 Solar Thermal Energy

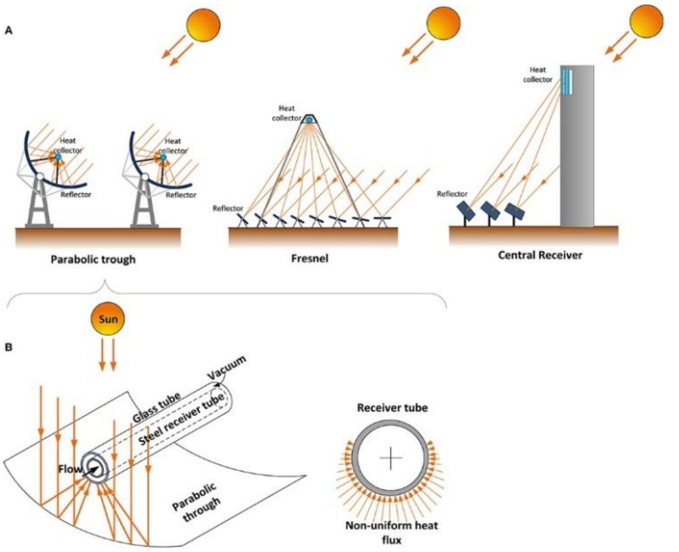

Fig. 2.3 Solar thermal process [17].

Solar thermal power/electric generation systems gather and concentrate sunlight to generate the high temperature heat required for electricity generation. Solar energy collectors, similar to the ones shown in Fig. 2.3, are used in all solar thermal power systems and consist of two major components: reflectors (mirrors) that capture and direct sunlight onto a receiver. In most systems, a heat-transfer fluid is heated and circulated in the receiver before being utilized to generate steam. A turbine converts steam into mechanical energy, which powers a generator to generate electricity. Tracking devices in solar thermal power systems maintain sunlight focused on the receiver throughout the day as the sun moves across the sky. Solar thermal power facilities are often equipped with a broad field or array of collectors that produce heat to a turbine and generator.

Solar thermal power systems may also include a thermal energy storage system component, which allows the solar collector system to heat an energy storage system during the day, and the heat from the storage system is utilized to generate electricity in the evening or when the weather is cloudy [17].

Concentrating solar thermal power (CSP) systems are classified into three types and can be seen in Figure 2.3:

- Linear Concentrating Systems: use long, rectangular, curved (U-shaped) mirrors to gather the sun's energy. The mirrors direct sunlight onto receivers (tubes) running the length of the mirrors. A fluid running through the tubes is heated by the focused sunlight. To generate power, the fluid is routed via a heat exchanger in a standard steam-turbine generator. Linear concentrator systems are classified into two types: parabolic trough systems, in which receiver tubes are positioned along the focal line of each parabolic mirror, and linear Fresnel reflector systems, in which one receiver tube is positioned above several mirrors to allow the mirrors greater mobility in tracking the sun.
- Solar Power Towers: A solar power tower system reflects and concentrates sunlight onto a receiver on top of a tower using a huge field of flat, sun-tracking mirrors known as heliostats. Sunlight may be magnified up to 1,500 times. Water is used as a heat-transfer fluid in some power towers. Because of its improved heat transmission and energy storage characteristics, advanced designers are experimenting with molten nitrate salt. The thermal energy storage capability enables the system to generate power even when it is cloudy or at night.
- Solar Dishes: Solar dish/engine systems employ a mirrored dish resembling a very large satellite dish. To save money, the mirrored dish is often made up of multiple smaller flat mirrors fashioned into a dish shape. The dish-shaped surface focuses and directs sunlight onto a thermal receiver, which absorbs and gathers heat before transferring it to an engine generator. The Stirling engine is the most frequent form of heat engine utilized in dish/engine systems. The fluid heated by the receiver is used to move pistons and generate mechanical power in this system. To generate energy, mechanical power drives a generator or alternator [17].

Given that solar thermal energy systems are also dependent on the sun's energy, the main limitations and challenges are shared with solar PV systems. The main difference would be that in solar thermal power plants, a large amount of thermal energy storage material such as salt is required in order to facilitate the heat transfer and ensure maximum capturing of the sun's heat energy. Nevertheless, the challenges of PV systems remain the same including, weather dependency, large land use requirements, limited efficiency and regular maintenance needs.

2.4 Hydroelectric Energy

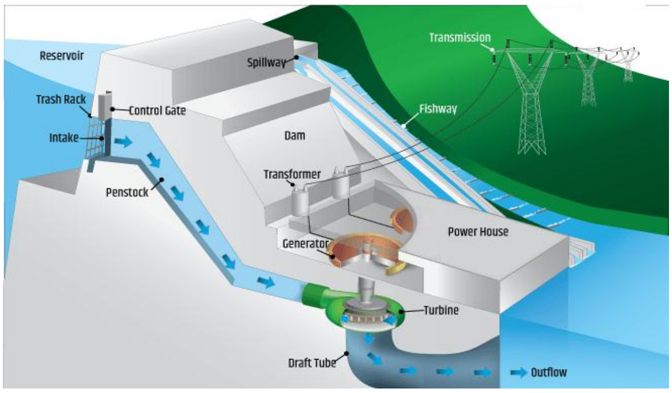

Fig. 2.4 Hydroelectric Power Plant [18].

Hydropower, often known as hydroelectric power, is one of the oldest and greatest forms of renewable energy, generating electricity from the natural flow of flowing water. Hydroelectric technologies produce electricity by utilizing the elevation difference generated by a dam or diversion structure between water flowing in on one side and out on the other [18]. Most hydroelectric power plants contain a water reservoir, a gate or valve that controls how much water comes out of the reservoir, and an outlet or location where the water ends up after flowing downstream, as shown in Fig. 2.4. Just before it overflows over the top of a dam or runs down a slope, water accumulates potential energy. When water travels downhill, potential energy is transferred to kinetic energy. The water may be utilized to turn the turbine blades, generating energy that is then supplied to the power plant's consumers.

There are three types of hydroelectric generating plants. A dam is used in an impoundment facility to regulate the flow of water held in a pool or reservoir. Water is discharged from the dam when extra electricity is required. Gravity takes control after the water is freed, and the water flows downward via a turbine. The turbine's blades rotate, which powers a generator.

A diversion facility is another form of hydroelectric generating plant. This plant is remarkable in that it does not use a dam. Instead, it employs a network of canals to direct river water into the generator-powered turbines.

The third type of plant is called a pumped-storage facility. This plant collects the energy produced from solar, wind, and nuclear power and stores it for future use. The plant stores energy by pumping water uphill from a pool at a lower elevation to a reservoir located at a higher elevation. When there is high demand for electricity, water located in the higher pool is released. As this water flows back down to the lower reservoir, it turns a turbine to generate more electricity [19].

Hydropower can be superior to wind and solar PV in many aspects such as, continuity and reliability, however, it still consists of many challenges as a system that need to be addressed. Hydroelectric generation is reliant on a consistent supply of water, which can be influenced by weather patterns such as droughts or floods. This can have an impact on the availability and dependability of hydroelectric electricity. Also, constructing hydroelectric dams may have a substantial influence on surrounding ecosystems and wildlife habitats. This can involve river flow disturbance, the extinction of fish and other aquatic species, and the damage of natural ecosystems. Furthermore, the topography of a certain location limits hydroelectric power. substantial quantities of power require a substantial elevation decrease or a high volume of water flow. Unlike wind and solar PV, it is also difficult to change or adjust the output of a hydroelectric power plant once it has been built to accommodate changing energy demands. This may restrict its use in locations with changing energy demands.

2.5 Geothermal Energy

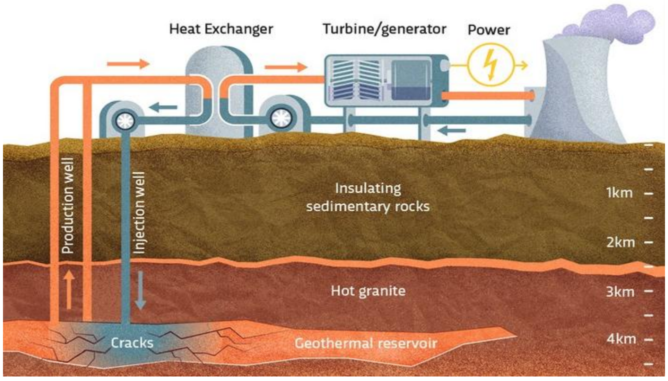

Fig. 2.5 Geothermal energy power plant [20].

Geothermal energy is a renewable energy source derived from the Earth's core. It is caused by heat created during the planet's creation and radioactive decay of elements. This thermal energy is stored in the earth's core in the form of rocks and fluids. The temperature differential between the earth's core and the surface promotes a continual transmission of thermal energy from the core to the planet's surface.

High temperatures of more than 4000°C allow part of the rock in the Earth's core to melt and produce hot molten rocks known as magma. Since the mantle is lighter than the underlying rock, these temperatures force it to act plastically and sections of it to convect upwards. The Earth's crust's rock and water may reach temperatures of roughly 370°C. Thermal energy may be found in rocks and fluids from modest depths to many miles below the Earth's surface as shown in the diagram in Fig. 2.5 [20].

Geothermal Energy has been used for thousands of years in various cultures for cooking and heating systems. Underground geothermal reservoirs of steam and hot water can be utilized to generate power as well as for heating and cooling.

A geothermal heat pump built roughly 10 feet underground is one type of heating and cooling. These pipes are filled with either water or antifreeze. Water is pushed via a closed loop of pipes. These ground source heat pump systems aid in the cooling and heating of buildings throughout the summer. This is accomplished by absorbing the earth's heat when the water cycles back into the structure [21].

To access geothermal resources, wells up to a mile deep or more are sunk into subsurface reservoirs. These resources can be derived from naturally occurring heat, rock, and water permeability, or via improved geothermal systems, which improve or develop geothermal resources via a process known as hydraulic stimulation. These geothermal resources, whether natural or modified, provide to power turbines that are linked to power generators.

Geothermal power facilities are classified into three types: dry steam, flash, and binary [20].

- Dry Steam: the earliest method, drawing steam straight from ground fissures to power a turbine.
- Flash Plants: extract high-pressure hot water from the ground and mix it with cooler, lower-pressure water. This produces steam, which is then used to power a turbine.
- Binary Plants: Hot water is transported through a secondary fluid with a lower boiling point than water in binary plants. The secondary fluid is converted to vapour, which powers a turbine. The majority of future geothermal power facilities are likely to be binary.

Similar to hydroelectric energy plants, geothermal energy plants are highly dependent on the geography of the site, where it is only available in specific locations of the world where geological conditions are favorable, such as hot springs or active volcanic zones. As a result, its potential as a worldwide energy source is limited. Contrary to the rest of RES energy sources, geothermal resources can diminish with time, limiting the lifespan of a geothermal power plant and making geothermal energy at risk of disappearing in the future. Despite the extensive research that has been done on this type of energy source for the past 30 years, in terms of efficiency, current geothermal technologies has several limits, since it can be difficult to extract enough heat to create substantial amounts of energy. This is especially true for geothermal systems that operate at low temperatures. A unique limitation that is also accompanied with geothermal power plants is that it requires significant volumes of water for cooling and other activities, which might be difficult in water-stressed locations.

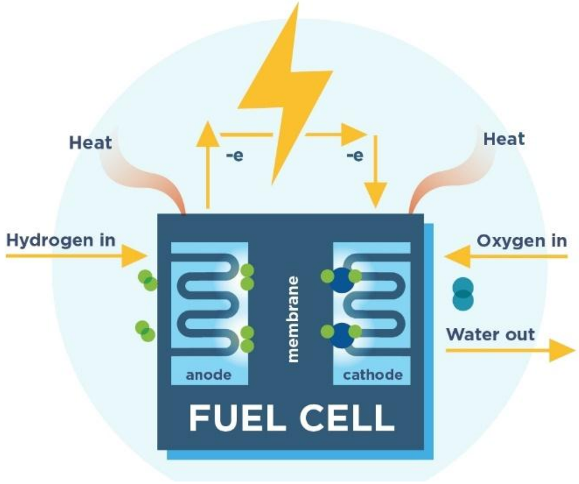

Fig. 2.6 Hydrogen fuel cell process [22].

2.6 Hydrogen Fuel Cells

A chemical process is used to create power in hydrogen fuel cells. A negative anode, as demonstrated in Fig. 2.6, and a positive cathode are found in each fuel cell. The process that generates electricity takes place at these electrodes, with an electrolyte conveying electrically charged particles between them and a catalyst to accelerate the reactions. Other types of fuel cell systems employ hydrocarbon fuels such as natural gas, biogas, or methanol. Fuel cells can reach better efficiency than traditional energy generation systems because they employ an electrochemical process rather than burning. This may be increased further by using combined heat and power generators, which utilize waste heat from the cell for heating or cooling.

The operation of a fuel cell may be summarized as follows:

- The anode receives hydrogen atoms, whereas the cathode receives oxygen.
- At the anode, hydrogen atoms are split into protons and electrons.
- The newly positively charged protons go to the cathode via the membrane (or electrolyte), while the negatively charged electrons travel in an opposite direction as they are driven through a circuit to create energy.
- Electrons and protons meet at the cathode after travelling through the circuit and the membrane, where they react with oxygen to form heat and water as byproducts.

Because single fuel cells do not produce a great quantity of electricity, they are stacked to provide enough power for their intended function, which might be powering a small digital gadget or a power plant.

Fuel cells function similarly to batteries, but unlike batteries, they do not need to be recharged and may continue to create energy as the fuel source (in this case, hydrogen) is available. A fuel cell has no moving components and is composed of an anode, a cathode, and an electrolyte membrane, making it quiet and very dependable [22].

The following are some of the limitations related with fuel cells:

1. Cost: Fuel cells may be expensive due to the usage of platinum as one of the most expensive component elements. Work is being done to develop non-platinum catalyst techniques [23].

2. Extraction of Hydrogen: The extraction of hydrogen for use in fuel cells can use a significant amount of energy, undercutting the environmental benefits of fuel cell use.

3. Establishment of infrastructure: There is a need to build infrastructure to support the increased usage of fuel cells, including retrofitting automobiles.

4. Security: The flammability of hydrogen raises obvious safety issues for its extensive use.

Because hydrogen is abundant in the cosmos, hydrogen fuel cells are a renewable source of energy. They are also a clean source of energy, while there are still some worries about the usage of fossil fuels for hydrogen extraction, as well as the possible carbon footprint connected with hydrogen transportation. However, hydrogen fuel cell technology has the potential to be a totally green and sustainable source of energy, with only heat (which may be utilized elsewhere) and water as byproducts. Furthermore, unlike batteries, fuel cells do not need to be recharged as long as there is a continual supply of fuel and oxygen.

The actual lifetime of a fuel cell is determined by its application, much to how batteries drain at varied rates depending on application. However, hydrogen fuel cell automobiles, for example, can currently go between 312 and 380 miles before needing to be refueled. The fuel cell stacks in automobiles are meant to last the vehicle's lifespan, which is around 150,000 to 200,000 kilometers. Fuel cells may be disassembled, and the materials recycled once they have served their purpose.

2.7 Comparison between above mentioned RES

Each of the renewable energy sources described above has its own distinct qualities and benefits, and each may play an essential part in the transition to a low-carbon energy system. Wind energy and solar PV are two of the most popular and cost-effective renewable energy sources, with wind energy best suited to locations with strong and constant winds and solar PV most suited to areas with plenty of sunlight. Hydroelectric power is another well-established and dependable renewable energy source that can supply a consistent source of electricity.

Geothermal and solar thermal energy are less common but have future development potential, with geothermal energy being especially suited to areas with hot springs or volcanic activity, and solar thermal energy being useful for applications such as heating water or powering industrial processes. Although the infrastructure for hydrogen generation and delivery is still in its early stages, hydrogen fuel cells are gaining popularity as a clean and efficient means to power automobiles and other uses. To establish a sustainable and low-carbon energy system, a mix of these renewable energy sources, as well as energy efficiency measures and energy storage technologies, will be required.

2.8 Challenges and limitations of RES

While RES provide several benefits such as reduced carbon emissions, less reliance on fossil fuels, and increased energy security, they also provide their own set of obstacles. One of the most significant issues is intermittency, which impacts the majority of renewable energy sources. Grid-scale batteries offer a solution to this challenge. The battery stores electric energy, which is subsequently released when needed. Batteries can readily solve the intermittent problem for wind and solar while also taking advantage of market prospects. For example, although solar resources generate during the day and are inactive at night, if a battery is installed alongside the solar array, a portion of the output from the solar array may be utilized to charge the battery. After the sun sets, the battery's energy may be drained. In the case of wind, which normally provides more energy at night, a part of the energy may be redirected to charging the battery and then released during the day [24]. On the other hand, when energy storage systems are introduced in an RES, the economics of the system's infrastructure drops making the system less attractive to developers with respect to the conventional power plants. This issue is being researched with respect to developing more efficient batteries from materials that are less costly than Lithium based batteries [25].

Wind and solar power generation are impacted by meteorological conditions, whereas hydroelectric power is affected by variations in water levels. This makes integrating these sources into the system and ensuring a consistent supply of power problematic. Energy storage technologies like batteries and pumped hydro can assist address this issue, but they also have drawbacks including cost and environmental effect. Another problem is the need for supporting laws and incentives to encourage the adoption of renewable energy technologies, which frequently compete with established fossil fuel companies with entrenched interests. The unpredictability of renewable energy sources can also pose issues in grid management, necessitating the development of new technologies and tactics to balance supply and demand. Finally, certain renewable energy technologies raise environmental and social problems, such as the effects of large-scale wind and solar farms on wildlife habitats and local residents, or the potential for geothermal energy to trigger earthquakes. Overall, while renewable energy sources offer considerable potential to contribute to a low-carbon energy system, overcoming these problems will need a mix of technological innovation, supporting policies, and public education. Furthermore, just like desalination plants and any power plant, RES plants are also subject to physical and cyber threats and attacks which need to be addressed and mitigated.

3.RES in Water Desalination Plants

Over the years, research on sustainability was driven to focus on finding alternative energy sources to all the mankind's operations. As mentioned in the previous chapters, desalination is a heavily powered process and is one of the essentials of living on earth for mankind as it provides clean water for all life purposes.

3.1 Solar Energy integrated in Desalination Applications

The integration of renewable energy sources in desalination plants is not a modern concept. In 1983, the authors in [27] have proposed the utilization of solar-powered brackish water distillation in inland settings that has the potential to reduce brine discharge to a less proportion of the feed. This would be by increasing the temperature of the steam from the solar boiler which lowers the product costs while increasing productivity per unit area of the solar collector.

However, there are many different hybrid systems that apply the energy produced from renewable sources in order to run the desalination plants. In 1998, authors in [28] proposed a Stand-Alone PV system that can run in a remote place and operate an RO desalination plant since the RO unit requires consistent power supply, a battery storage system is required. The results of the work shows that small-scale PV-RO desalination plants constitute a viable alternative for potable water delivery in locations without access to the energy grid. Due to the high cost of PVs, their usage is appropriate for small-scale facilities and rural places where power from traditional sources is unavailable or the cost of producing electricity is high.

Furthermore, in [29] a batteryless photovoltaic-powered saltwater reverse-osmosis desalination system that is efficient and cost-effective is described as demonstrated in Fig. 3.1. Existing photovoltaic-powered desalination demonstrations often use lead-acid batteries, which allow the system to operate at constant flow. In practice, however, batteries are notoriously difficult to maintain, particularly in hot areas. The method used is variable flow, which allows it to make optimum use of the naturally fluctuating solar supply without the usage of batteries. The system makes use of typical industrial inverters, motors, and pumps that are both energy and cost efficient. The relatively simple control algorithm proposed provides MPPT for solar arrays.

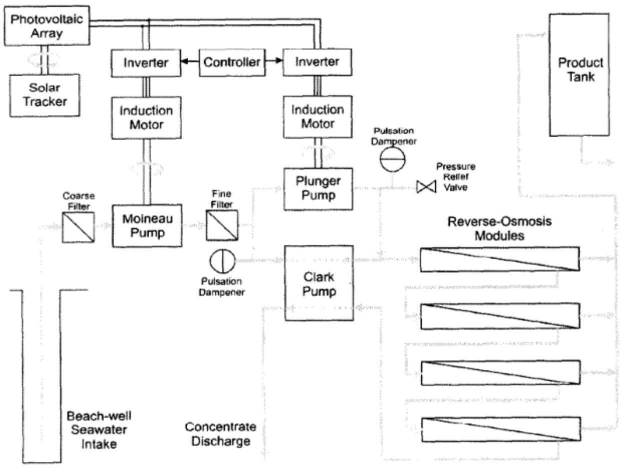

Fig. 3.1 Diagram demonstrating the batteryless photovoltaic-powered desalination system [29].

In [30], the authors examine the mechanics of interfacial solar desalination using a sophisticated heat and mass transport model. The model is used to demonstrate the advantages of interfacial evaporation over classical evaporation. Furthermore, the authors elucidate the impact of solar flux and surface area adjustment on evaporation efficiency. It is also demonstrated numerically that the impact of environmental factors on evaporation efficiency cannot be abolished by subtracting the dark evaporation rate from the evaporation rate under sunlight conditions. It is also discovered that interfacial evaporation in a solar still does not achieve the predicted high total solar desalination efficiency, but that additional improvement is conceivable through system design. This research provides insights into the thermal mechanisms involved in interfacial solar evaporation and provides vital perspectives to the field.

3.2 Wind Energy integrated in Desalination Applications

In 2002, authors explain the utilization of renewable energy sources as a need on Croatian islands, and it is a necessary prerequisite for their long-term growth [31]. The study describes the key characteristics of the County's existing, developed, and projected water delivery infrastructure. A hybrid plant based on reverse osmosis desalination has been suggested, with wind-powered electric power as the source of energy.

In 2006, the author in [32] demonstrated the technical feasibility of physics-based system models of wind-powered desalination using both reverse osmosis and mechanical vapour compression, and the technical viability of utilizing wind as a power source for desalination has been proven. The resulting costs of the demonstrated system, shown in Fig. 3.2, are in line with what is predicted for a conventional desalination plant, demonstrating that it is especially cost-competitive in places with excellent wind resources and high energy costs. It is possible to infer that wind-powered desalination may compete with conventional desalination technologies in terms of producing safe and clean drinking water in an ecologically friendly manner.

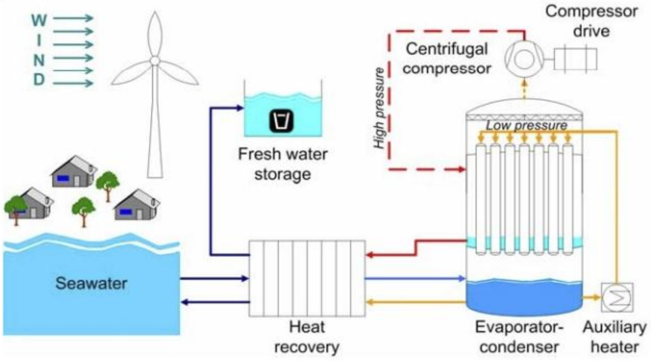

Fig. 3.2 Conventional wind-powered MVC process [32].

To add on to the above advances in the research field on RES in desalination, the other RES mentioned in chapter 2 such as geothermal and hydroelectric can also be utilized as an energy source for desalination plants, however, research focuses more on Solar PV, Solar Thermal and Wind energy integrated systems as they are more common in and are not geographically limited due to their nature.

3.3 Challenges of using RES to power desalination plants

The variable and intermittent nature of most renewable energy sources is the main obstacle in integrating RES in desalination plants. Desalination requires a continuous and consistent source of energy to function, and changes in wind or solar power generation can impair the desalination process. This may be solved by employing energy storage technology such as batteries or pumped hydro to store extra energy during periods of strong renewable energy generation and release it when required.

Another issue is the high energy demand of desalination operations, which can be energy-intensive and necessitate large quantities of power. This can be especially difficult in off-grid or isolated areas where access to reliable energy is restricted. Using renewable energy sources can assist lower desalination's carbon footprint, but the cost and practicality of adopting RES at scale must be addressed.

Furthermore, some desalination systems, such as reverse osmosis, need high pressure and temperature, making integration with renewable energy sources more difficult. Other processes, such as thermal desalination, may be more suitable for usage with renewable energy sources, although they also have environmental consequences, such as the release of heated brine back into the ocean.

Finally, the environmental consequences of large-scale desalination operations must be properly studied. These include the possibility for increasing energy consumption and accompanying greenhouse gas emissions, as well as the effects on marine ecosystems and habitats.

4.Introduction to Cyber Attacks

A cyber attack stands for any an attempt by hackers to damage or destroy a computer network or system. This chapter will cover the basic introduction to several types of cyber attacks to be familiarized with the terminologies for the upcoming chapters.

There are several types of cyber-attacks, some of which are [33]:

4.1 Malware attacks: Malware attacks are typical types of cyberattacks in which malware (usually malicious software) performs illegal operations on the victim's system. Malicious software (sometimes known as viruses) comprises a wide range of assaults, including ransomware, spyware, command and control, and others.

- There are several types of malware attacks:

1 Trojan Horse: This is a software that looks to be one thing (e.g., a game, a beneficial application, etc.) but is actually a virus delivery mechanism. A trojan horse requires the user to download it (often through the internet or as an email attachment) and execute it on the target.

2 Virus: A virus is a sort of self-propagating malware that uses code injection to infect other programs/files (or even sections of a target's operating system and/or hard drive). This nature of malware propagation via injection into existing software/data distinguishes between a virus and a trojan horse (which has purposely built malware into one specific application and does not make attempts to infect others).

3 Worm: A worm is malware that is meant to spread to other computers. Whereas viruses and trojan horse malware are restricted to one infected target system, worms aggressively seek for new systems to infect (often without any human intervention).

4.2 Phishing attacks: Phishing is a sort of social engineering attack that is frequently used to acquire user information such as login passwords and credit card details. It happens when an attacker poses as a trustworthy entity and tricks the victim into opening an email, instant message, or text message. The receiver is subsequently duped into clicking a malicious link, which can result in malware installation, system freeze as part of a ransomware assault, or the disclosure of sensitive information [34].

4.3 Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks: A distributed denial-of-service (DDoS) attack is a malicious attempt to interrupt regular traffic to a specific server, service, or network by flooding the target or its surrounding infrastructure with Internet traffic. DDoS assaults are effective because they use several hacked computer systems as attack traffic sources. Computers and other networked resources, like as IoT devices, can be exploited machines.

DDoS assaults are done by using networks of machines linked to the Internet. These networks are made up of computers and other devices (such as IoT devices) that have been infected with malware, allowing an attacker to manage them remotely. Individual devices are known as bots (or zombies), while a network of bots is known as a botnet. After establishing a botnet, the attacker may conduct an attack by sending remote commands to each bot. When the botnet targets a victim's server or network, each bot sends requests to the target's IP address, possibly overloading the server or network and triggering a denial of service to regular traffic. Because each bot is a genuine Internet device, it is possible to separate the attack traffic from the legitimate traffic [35].

4.4 **SQL injection attacks:** SQL injection (SQLi) is a web security flaw that allows an attacker to tamper with database queries made by an application. It typically enables an attacker to examine data that they would not otherwise be able to get. This might include data belonging to other users or any other data that the program has access to. An attacker can often edit or destroy this data, resulting in lasting changes to the application's content or behavior. An attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure, or launch a denial-of-service attack in specific circumstances. There are several SQL injection vulnerabilities, attacks, and strategies that can occur in a number of settings[36]:

- Retrieving hidden data, where you may change a SQL query to produce additional results, is a popular SQL injection example.
- Subverting application logic, which involves changing a query in order to interfere with the program's logic.
- UNION attacks, which allow you to retrieve data from many database tables.
- Analyzing the database, where you may extract information about the database's version and structure.
- Blind SQL injection, which occurs when the results of a query controlled by you are not returned in the application's answers.

4.5 **Man-in-the-middle attacks:** A man in the middle (MITM) attack occurs when a perpetrator inserts himself into a dialogue between a user and an application, either to eavesdrop or to mimic one of the parties, giving the impression that a regular flow of information is taking place. An attack's purpose is to steal personal information such as login passwords, account information, and credit card numbers. Users of banking apps, SaaS enterprises, e-commerce sites, and other websites that require signing in are typical targets. Information collected during an attack might be utilized for a variety of objectives, such as identity theft, unauthorized financial transfers, or unauthorized password changes. It may also be used to obtain entry into a secure perimeter during the infiltration stage of an advanced persistent threat (APT) attack. A MITM attack is roughly analogous to a mailman reading your bank statement, writing down your account information, resealing the package, and delivering it to your door [37].

4.6 **Cross-site scripting (XSS) attacks:** XSS attacks are a sort of injection in which malicious scripts are injected into otherwise innocuous and trustworthy websites. XSS attacks occur when an attacker utilizes a web application to transmit malicious code to a separate end user, typically in the form of a browser side script. The flaws that allow these attacks to succeed are extremely common, and they occur whenever a web application includes user input inside the output it creates without verifying or encoding it.

An attacker can use XSS to deliver a malicious script to an unwary user. The browser of the end user has no means of knowing that the script should not be trusted and will run it anyhow. Because the malicious script believes the script came from a trustworthy source, it has access to any cookies, session tokens, or other sensitive information stored by the browser and utilized with that site. These programs can even rewrite the HTML page's content [38].

4.7 **Advanced Persistent Threat (APT) attacks:** An advanced persistent threat (APT) is a generic term for an attack campaign in which an intruder, or a group of invaders, maintains an unlawful, long-term presence on a network in order to harvest extremely sensitive data. The targets of these meticulously selected and studied attacks are often huge companies or governmental networks. The ramifications of such invasions are numerous, and they include [39]:

- Theft of intellectual property (e.g., trade secrets or patents)
- Sensitive information has been compromised (e.g., employee and user private data)
- Critical organizational infrastructure sabotage (e.g., database deletion)
- Whole site takeovers

5.Vulnerabilities and Solutions Towards Cyber Attacks in RES-Desalination Plants

Renewable Energy Source (RES) desalination plants are crucial infrastructure structures that are required to provide safe drinking water to people all over the world as discussed in the previous chapters. These facilities, like any vital infrastructure, are vulnerable to cyber assaults that might impair their operations and jeopardize the safety of the drinking water supply. Cyber attackers may exploit the following vulnerabilities in RES desalination plants:

- Unsecured Networks: RES desalination facilities frequently use computer networks to regulate processes such as water input and outflow, water treatment, and power production. If these networks are not effectively protected, cyber attackers might possibly get access to sensitive information or even seize control of important systems, causing operations to be disrupted or causing harm to the public.
- Weak Passwords: Many cyber assaults use automated software to guess passwords and gain access to systems. Cyber attackers might undermine RES desalination facilities if the passwords used are weak or easily guessable.
- Outdated Software: Like any computer system, the software used in RES desalination facilities might have weaknesses that cyber attackers can exploit. It is critical to maintain software up to date in order to guarantee that any known vulnerabilities are addressed.
- Social engineering tactics, such as phishing emails, can be used by cyber attackers to acquire access to sensitive information or corrupt systems. Workers at renewable energy desalination facilities should be educated to identify and avoid such assaults.

Therefore, it is critical that RES desalination plants take cybersecurity seriously and employ precautions to prevent cyber intrusions. This includes routine software updates, the use of strong passwords, teaching personnel on how to spot and prevent social engineering attacks, and the implementation of physical security measures to secure vital systems.

This chapter discussed the research field in the past 20 years on the vulnerabilities and solutions that were proposed over time to decrease cyber attacks in RES desalination plants.

5.1 Cyber Attacks on Desalination Plants

The vulnerability on modern power infrastructures is getting worse, an attacker who lacks complete power grid topology and parameter information can still carry out a fake data injection assault without being recognized by the state estimator. This study [40] presents an efficient technique for selecting the best assaulting zone with minimal network knowledge. Extensive simulations are used to validate the suggested algorithm's efficacy. This report opens a new chapter in the study of smart grid cyber security by determining a possible assault zone with less network information. This work is particularly important for developing effective defense techniques against false data injection attacks based on a thorough understanding of the assaults' processes and strategies.

In this research [41], the authors demonstrate how typical power network activities may be statistically separated from the situation of stealthy assaults. The authors present two machine-learning-based strategies for detecting stealthy attacks. The first technique trains a distributed support vector machine using supervised learning on labeled data support vector machine (SVM). The distributed SVM is designed using the alternating direction approach of multipliers, which provides proved optimality and convergence rate. The second approach requires no training data and identifies measurement variance. Principal component analysis is utilized in both approaches to minimize the dimensionality of the data to be analyzed, resulting in lower computing complexity.

In [42] the authors state that data analysis approaches are now being used to combat fake data injection attacks (FDIAs), particularly when large scale smart grids generate massive volumes of data. In this research, a novel data analysis approach based on the data-centric paradigm and utilizing the margin setting algorithm (MSA) is suggested to detect FDIAs. The suggested method's performance is proved using simulation using a six-bus power network in a large area measurement system setting, as well as experimental data sets. Two FDIA situations are investigated: playback attack and time attack. The experimental findings are contrasted with those of the SVM and the artificial neural network (ANN). When used to FDIA detection, the findings show that MSA outperforms both SVM and ANN in terms of detection accuracy.

In [43] the authors use deep learning algorithms to recognize the behavior aspects of FDI assaults using historical measurement data, and then use the acquired features to detect FDI attacks in real-time. As a result, the suggested detection system efficiently relaxes the assumptions on various attack scenarios while maintaining high accuracy. In addition, the paper presents an optimization model to explain the behavior of one sort of FDI assault that compromises the power system's restricted number of state measurements for electricity theft. The performance of the suggested technique is demonstrated through simulation using an IEEE 118-bus test system. The research also uses an IEEE 300-bus test system to assess the scalability of the suggested detection technique.

Furthermore, the impact of fake data injection (FDI) assaults on automated generation control (AGC), a fundamental control mechanism utilized in all power grids to keep the grid frequency at a nominal value, is investigated in [44]. Attacks on AGC sensor readings can result in frequency excursions that need corrective measures like as removing customer loads or generators, resulting in blackouts and potentially costly equipment damage. The authors develop an attack impact model and assess an ideal assault, which consists of a sequence of FDIs that minimize the remaining time before the commencement of disruptive corrective activities, giving the grid the least time to respond. It is demonstrated that the attacker may learn the attack impact model and perform the ideal attack in reality using eavesdropped sensor data and a few easily obtained system constants. This research offers critical understanding of the physical constraints of FDIs on power grids, as well as an analytical approach to assist the safety of sensor data lines. The authors build efficient methods to identify the assault, estimate which sensor data lines are under attack, and limit the consequences of the attack.

Modern Water Distribution Systems (WDSs) are frequently regulated by Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs), which govern their operation and ensure a steady supply of water. As a result, and with the cyber layer becoming a critical component of WDS operations, these systems are more vulnerable to intrusions. This study [45] presents a model-based technique for identifying sophisticated cyberattacks that cannot be fully detected by hydraulically based criteria alone, based on a deep hydraulic knowledge of WDSs paired with an anomaly detection algorithm. When evaluated on data from the BATtle of the Attack Detection ALgorithms (BATADAL) competition, the findings suggest that the proposed algorithm is capable of obtaining the best-known performance. The method employs a three-phase approach in which: 1) the demand is estimated based on a portion of the SCADA readings; 2) a hydraulic model is used to check whether the hydraulic data from the SCADA corresponds to the estimated demand; and 3) a multilevel classification approach is then implemented to classify the obtained errors into outlier and normal errors. The results reveal that the suggested technique was successful in raising an early warning for all of the labeled simulated cyberattack occurrences.

Another approach, shown in [46] tries to comprehend and develop techniques for using fault detection and isolation (FDI) methodologies to improve the cyber-security of cyber-physical systems (CPS). In this paper, the authors employed state estimation to check relationships between process variables, known as invariants, and thereby identify the commencement of assaults. Multiple attack scenarios were investigated, and the suggested state estimation approach was proven to be very effective in detecting assaults on sensors inside the system, given that not all sensors are compromised during the attack. However, due to delays or a lack of information to locate the attacked component, the recommended approaches for later isolation and rectification were limited. The authors tested the suggested method on a well-equipped pilot scale water treatment unit with controllers.

Detecting a different type of cyber-attack, [47] discussed the use of machine learning-based methodology for detecting distributed Denial of Service (DDoS) assaults in smart cities as shown in Fig 5.1. The proposed approach use limited Boltzmann machines to learn high-level characteristics from raw data, and a feed forward neural network model is trained on top of these learnt features for attack detection. The proposed framework's performance is validated using a smart city dataset acquired from a smart water plant. The findings demonstrate the suggested framework's usefulness in identifying DDoS assaults. The experimental results show the ability of the proposed framework to detect DDoS attacks with high accuracy, where adding the deep learning step outperforms the classification algorithm applied alone.

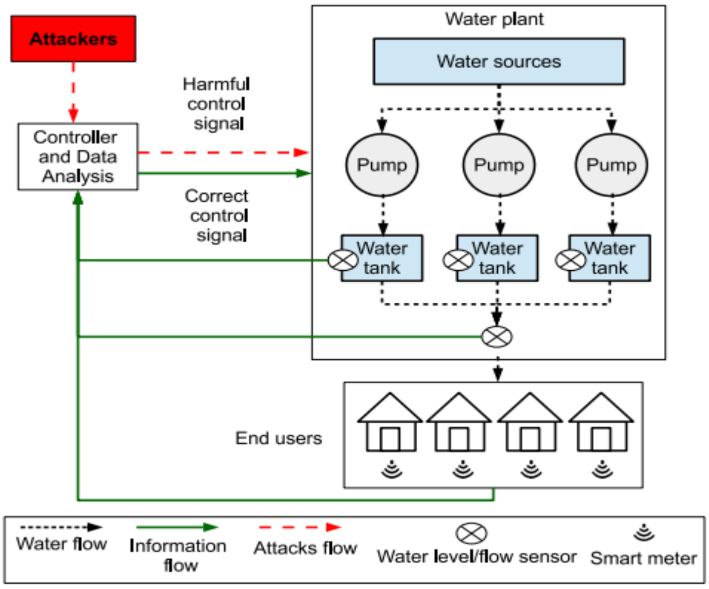

Fig 5.1 Example of DDoS attack in smart water plant [47].

Worthwhile extensions to the proposed work in this paper could be by generating a dataset from different smart applications, such as smart grids with more rich features and types of attacks to test more complicated cases and scenarios.

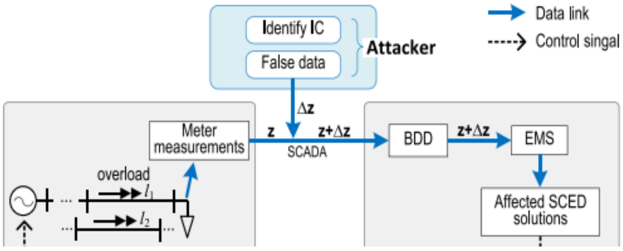

Fig 5.2 Data flows and control signals under the attack [48].

Furthermore, in [48], the authors examine a potential relationship between data attacks and physical effects, as well as how an attacker may launch a malicious data assault to cause successive outages as shown in Fig. 5.2, and thereby cause significant grid damage. The attacker builds an optimum fake data injection attack to purposefully induce a targeted branch outage sequence that trips many branches and leads to consecutive failures in this attack technique. The investigated attack technique combines building an optimum data attack and detecting vital lines, imposing a significant security effect with a high probability of occurrence. Simulations on the IEEE 118-bus system confirm the attack technique and emphasize the vulnerability of similar assaults in today's smart grids.

The vulnerability of a consensus-based distributed energy scheduling method to data integrity attacks is addressed in [49]. To identify fraudulent information and get optimal results, a reputation-based neighborhood-watch technique is created. When there are misbehaving controllers, the operational point changes. The reputation-based neighborhood watch algorithm performs three major functions: 1) verifying the accuracy of neighbors' information based on two-hop shared information; 2) identifying the compromised controller based on reputation indexes; and 3) maintaining the accuracy of local information estimation in the presence of false information.

Simulation evaluations in the future renewable electric energy distribution and management system demonstrate the usefulness of the suggested strategy as shown in Fig. 5.3 below.

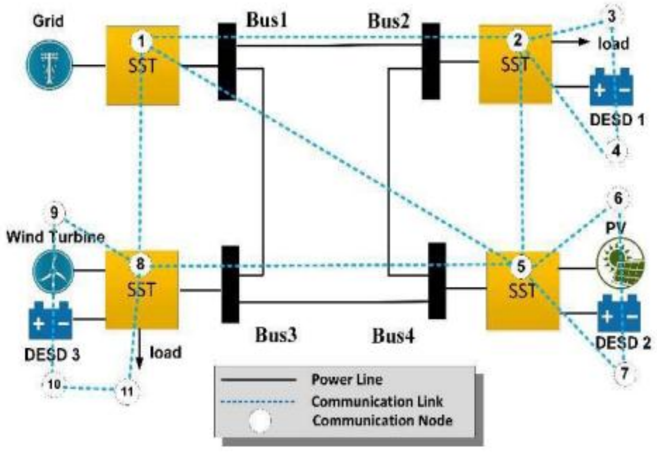

Fig 5.3 Microgrid conFiguration with communication links [49].

The work in [50] proposes Open Source Exploitation (OSEXP), a methodology that uses information from public infrastructure to identify an advanced attack vector on power systems. The assault is aimed against Phasor Measurement Units (PMUs), which rely on GPS signals to deliver time-stamped circuit values of power lines. The authors offer a GPS time spoofing attack that makes use of low-cost commercial hardware and open source software. By building a testcase model of the power system in a digital real-time simulator (DRTS), the essential information for the implementation of the OSEXP attack is retrieved. DRTS is also used to assess the efficacy and impact of the established OSEXP attack approach. The given targeted attack indicates that a low-budget actor may cause major damage to a nation.

On another note, and from the perspective of economics and mechanical engineering, the authors in [51] conduct an interdisciplinary cyber threat analysis on a desalination plant model, presenting cyberattacks and assessing their impact on plant performance and equipment. The study reveals that cyber criminals can cause significant financial harm by interfering with plant operation. It also conducts control volume and finite element analysis studies to look into the possibilities of Stuxnet-like assaults that might cause mechanical damage and equipment failure. Performance attacks on a Matlab desalination plant model were investigated, as were mechanical assaults on an ANSYS model we constructed. The findings indicate that the attacker has a number of alternatives for initiating assaults that optimize impact while maintaining within operational constraints. Furthermore, the mechanical engineering analysis reveals that there is a risk of cyberspace equipment damage. This effort intends to raise awareness of the need of cybersecurity research for desalination plants while also serving as a platform for the development of mitigations against process-aware assaults.

Islanded microgrids, which include renewables, are highly unpredictable systems that require extra communications and information sharing for Load Frequency Control (LFC), which leads to Cyber Physical Systems (CPS). The secondary frequency control (SFC) of a microgrid refers to this extra communication-based coordination of generators. Furthermore, electric vehicle (EV) batteries engage in the SFC by adjusting frequency deviation via a cyber interface. The SFC is extremely vulnerable to several sorts of cyber disruptions, including as False Data Injection (FDI), which can corrupt sensor and actuator data to influence decision-making processes or initiate disruptive reconstructing actions, perhaps resulting in blackouts. All uncertainties, including renewable energy and measurement noises, should be modeled and handled to imitate actual circumstances for FDI detection and control. This study [52] proposes a robust control strategy for actuators in the presence of uncertainty expressed as Unknown Inputs (UIs). The proposed controller has two layers: the first layer uses a Stochastic Unknown Input Observer (SUIO) to identify microgrid states and UIs, and the second layer uses optimum control to limit frequency excursions. The suggested resilient control framework is compared to classic LQR using simulations to demonstrate performance advantages.

The previous papers discussed offer an insight on the cyber-attacks after occurring and how to resolve them, however this study [53] delivers the first instance of active protection against cyber assaults on renewable-rich microgrids. Cyber risks in such a microgrid environment have been found. A protection system based on dynamic watermarking for identifying cyber abnormalities in microgrids, is proposed. The suggested approach is demonstrated to be easily implementable and to have theoretically demonstrable performance in identifying cyber threats. The suggested mechanism's efficacy is evaluated and confirmed in a Texas A&M 4-bus microgrid testbed with 100% sun penetration.

Similar to [52], the authors in [54], offer a novel anomaly detection method based on a Luenberger observer and an artificial neural network (ANN). To increase dependability, sustainability, and efficiency, smart power grids are being supplemented with a communication infrastructure. Despite these considerable benefits, their open communication design and connection make power systems vulnerable to a variety of threats. This paper offers a new resilient control method for load frequency control (LFC) systems that are vulnerable to fake data injection (FDI) attacks. Encryption in data transfer lines is commonly used as the first layer of security; it is suggested a second defensive layer that may concurrently identify and reduce FDI assaults on power systems.

Because of the reduction in overall inertia of the power system, time delay attacks are a type of cyber attack that can have a significant impact on the frequency stability of power systems with large penetration of renewable energy sources. In [55], a new virtual inertia control approach is developed, that augments the standard virtual inertia technique with a virtual damper to lessen the consequences of time delay assaults on the isolated microgrid's load frequency control loop. During a time delay assault, in which an adversary delays the frequency measurement from the phase measurement unit, the suggested technique offers superior frequency control response with fewer oscillations and frequency deviation nadirs, increasing the security and stability of the microgrid.

As opposing to the cyberattack causes and solutions discussed in the studies above, the authors in [56] offer an iterative optimization-based strategy to recover the preattack values of the attacked grid variables while making as minimal changes as feasible to the non-attacked ones. Suggested framework. Furthermore, a methodology for calculating an indicator called the Recovery Quality Index (RQI) is given to evaluate the recovery algorithm's performance. The simulation results demonstrate that the suggested technique performs well in terms of computed RQI for a large number of simulated attack samples on various IEEE test bus systems.

Moreover, in [57], the "End-User Privacy Protection Scheme (EPPS)" is suggested to safeguard business and non-commercial users by allowing smart meters to report correct readings during FDIA/intrusion. In this proposed technique, a statistical machine learning method based on Gaussian Mixture Model Clustering (GMMC) and Mean Square Error (MSE) is evaluated for true measurement against false data injection using two performance indices, the Data Protection Capability (DPC) and the confidential interval. A passive distributed network is investigated to evaluate the performance of the suggested technique. The customer pattern is recreated using EPPS by removing. FDIA-caused cyber intrusion on a smart metering system. This study confirms the suggested strategy using MATLAB software and data from the National Renewable Energy Laboratory's smart meters (NREL).

To maintain load-generation balance, power grids are outfitted with Rate-of-Change-of-Frequency (ROCOF) and Load Shedding (L5) relays. As renewables become more prevalent, power grid inertia decreases, resulting in a quicker drop in system frequency in the event of a load-generation imbalance. In [58], the authors investigate the viability of initiating a False Data Injection (FDI) attack in order to generate False Relay Operations (FRO), also known as a FRO attack, in power systems with substantial renewables. The authors simulate the frequency dynamics of power systems and the accompanying FDI assaults, including the effect of factors such as synchronous generator inertia and governor time constant and droop on FRO attack success. The FRO assault is formalized as a Constraint Satisfaction Problem (CSP) and solved using Satisfiability Modulo Theories (SMT). The case studies reveal that power networks containing renewables are more vulnerable to FRO assaults, and synchronous generator inertia plays an important role in lowering the success of FRO attacks in power grids.

Accurate state estimate (SE) in the face of increased uncertainty caused by the high penetration of RESs is becoming more critical for improving the optimum and resilient functioning of renewable-rich power grids. However, attackers planning to control the target power grid are expected to produce assaults that inject false data to the SE via device and network weaknesses. FDIA is gaining prominence among possible attack types because it can circumvent bad data detection (BDD) measures provided in SE systems. Although various FDIA detection algorithms have recently been presented, the uncertainty of system design caused by the continually rising penetration of RESs has received less attention in the literature. This research [59] presents a unique FDIA detection technique for renewable energy-rich power networks to overcome this issue. A deep learning framework is created specifically by establishing a Bidirectional Long Bi-LSTM (Bi-LSTM) combines current smart grid features. The created framework is tested on an IEEE 14-bus system that integrates different RESs utilizing various attack scenarios. In a renewable energy-rich grid setting, a comparison of numerical data demonstrates that the proposed FDIA detection method outperforms existing deep learning-based systems.

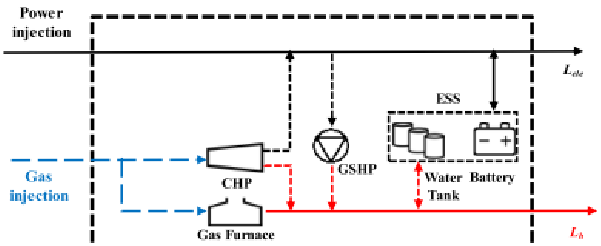

Fig. 5.4 Proposed model [60].

FDIA constructed wisely by attackers can have serious implications such as uneconomic operation and blackouts, especially in multivector energy distribution systems (MEDS), which are intimately coupled and interdependent. In [60] the authors examine the cyber resilience challenges of a MEDS created by FDI as shown in Fig. 5.4, taking into account the unpredictability of renewable resources. To increase day-ahead and real-time resilience, a unique two-stage distributionally robust optimization (DRO) is developed. The Wasserstein distance and moment information are used to generate the ambiguity set. In comparison to robust optimization, which analyzes the worst-case scenario, DRO produces less conservative solutions and hence delivers more cost-effective operating schemes.

Software-Defined Networking (SDN) is a resilient networking solution that is used to more effectively solve security problems. The most crucial component in the SDN architecture is the controller, which oversees the flows of each suitable forwarding unit. The flow statistics of the controller are expected to give useful information for developing an Intrusion Detection System (IDS). As a consequence, the authors in [61] propose a five-level classification technique based on SDN flow data for developing a Smart Attacks Learning Machine Advisor (SALMA) system for detecting intrusions and defending smart cities against smart attacks. At all stages, they employ the Extreme Learning Machine (ELM) approach. On the NSL-KDD and KDDCUP99 benchmark datasets, the suggested system obtained 95% and 99.2%, respectively.

5.2 Suggested solution model security against cyber-attacks in RES powered desalination plants

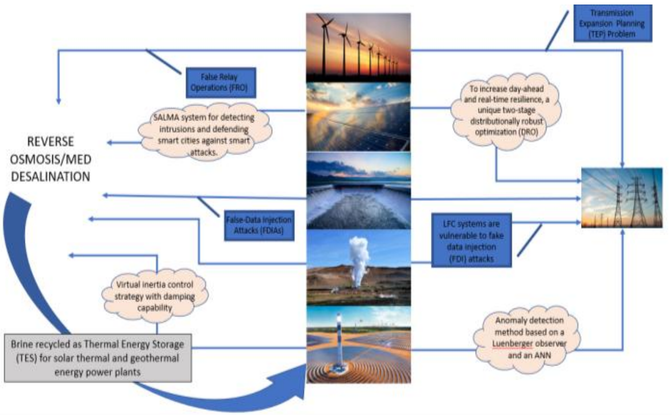
Transmission Expansion Planning (TEP) Problem
False Relay Operations (FRO)
SALMA system for detecting intrusions and defending smart cities against smart attacks.
To increase day-ahead and real-time resilience, a unique two-stage distributionally robust optimization (DRO)
REVERSE OSMOSIS/MED DESALINATION
False-Data Injection Attacks (FDIAs)
LFC systems are vulnerable to fake data injection (FDI) attacks
Virtual inertia control strategy with damping capability
Anomaly detection method based on a Luenberger observer and an ANN
Brine recycled as Thermal Energy Storage (TES) for solar thermal and geothermal energy power plants

Fig 5.5 Suggested solution model of security against cyber-attacks in RES powered desalination plants.

Micro grids are the future of sustainable cities and the review done above on the research done so far supports the transition that will be taking place soon to net zero sustainable and renewable cities. Fig 5.5 above suggests a model of integration of renewable and clean energies for the operation of desalination plants. It can be seen that different RES such as , Wind, Solar PV, Hydro, Geothermal and Solar Thermal can be the main sources of energy to run desalination plant, whether be it Reverse Osmosis or MED plants as they require high power sources in order to be run as discussed in chapter 3, therefore, a hybrid energy source of all the renewable energy plants would be sufficient to run the desalination plants [62]. The balance energy from the renewable power plants can be utilized to generate electricity and be distributed through the AC grid for residential and commercial consumers.

A suggested solution that was inspired by the authors in [63], is to use the brine produced from the desalination plants in order to be recycled as the Thermal Energy Storage (TES) substance in the solar thermal and geothermal plants. This will be an efficient way for brine management as well as a cost-efficient and renewable way to provide a TES medium for the RES plants.

The blue boxes intercepting the route diagrams between the power plants and desalination plants and AC grid are the examples of cyberattacks that were shown to be a vulnerability to power plants in this review paper. False Relay Operations [58], False-Data Injection Attacks (FDIAs) [64] and Transmission Expansion Planning (TEP) Problem [65]. The clouds present are suggested solutions to these cyberattacks based on the research papers reviewed such as, SALMA system for detecting intrusions and defending smart cities against smart attacks [61], to increase day-ahead and real-time resilience, a unique two-stage distributionally robust optimization (DRO) [60], Anomaly detection method based on a Luenberger observer and an ANN [59] and Virtual inertia control strategy with damping capability [55].

8.Conclusions and Further Work

Cyber threats are a common and serious problem in the power industry. RES powered desalination plants were the main focus of this research and a comprehensive review of the research done in the past 20 years was performed.

This research offers a reference for future work that can provide structure and direction towards the gaps in the field and offers a proposed solution that captures the learnings of this survey paper and a future roadmap to smart cities and microgrids in general. It can be witnessed that the main threat that targets RES-D plants is FDIA and the solutions mentioned in the chapters above can be implemented in real life and have been a part of government and regional case studies. The topic discussed in this work is of national concern and a security threat to the whole region as desalination plants are a very essential part of a country's economy and the whole balance of the operations in a city.

Future work to this report can include the implementation and simulation of the suggested solution using an energy simulation software that offers a full decarbonization solution to future smart cities where hybrid RES power different types of desalination plants and the waste of theses plants are recycles in the RES itself. Excess energy from the RES can be used as a source of electricity for the city. Cyber threats discussed in the report can then be simulated and security framework can be created for RES-D plants. Access control, network security, system hardening, and incident response should all be covered by the framework. Furthermore, an automated system can be created that keeps an eye on the network and IT systems at the RES-D plants for potential security concerns. A threat intelligence module for this system that can deliver in-the-moment alerts and suggested mitigation measures is also essential. Moreover, an investigation of how artificial intelligence (AI) and machine learning (ML) may be used in RES-D plants to enhance the identification and mitigation of cyberattacks. By automating threat detection and response, these technologies can strengthen the plant's overall security posture.

To summarize, employing renewable energy sources in desalination has numerous advantages, but it also has certain drawbacks. To address these issues, a mix of technical innovation, supporting legislation, and careful consideration of environmental and social implications will be required.

References

[1] M. Shatat and S. B. Riffat, "Water desalination technologies utilizing conventional and renewable energy sources," *Int. J. Low-Carbon Technol.*, vol. 9, no. 1, pp. 1–19, Mar. 2014, doi: 10.1093/ijlct/cts025.

[2] "Electrodialysis." https://www.lenntech.com/electrodialysis.htm (accessed Nov. 30, 2018).

[3] "Membrane distillation | EMIS." https://emis.vito.be/en/techniekfiche/membrane-distillation (accessed Nov. 30, 2018).

[4] S. Alobaidani, E. Curcio, F. Macedonio, G. Diprofio, H. Alhinai, and E. Drioli, "Potential of membrane distillation in seawater desalination: Thermal efficiency, sensitivity study and cost estimation," *J. Membr. Sci.*, vol. 323, no. 1, pp. 85–98, Oct. 2008, doi: 10.1016/j.memsci.2008.06.006.

[5] O. A. Hamed, M. A. K. Al-Sofi, M. Imam, G. M. Mustafa, K. Ba Mardouf, and H. Al-Washmi, "Thermal performance of multi-stage flash distillation plants in Saudi Arabia," *Desalination*, vol. 128, pp. 281–292, May 2000, doi: 10.1016/s0011-9164(00)00043-6.

[6] "Thermal Desalination (MED & MVC) | IDE Technologies." https://www.ide-tech.com/en/solutions/desalination/thermal-desalination-med-mvc/ (accessed Nov. 30, 2018).

[7] R. Bahar, M. N. A. Hawlader, and L. S. Woei, "Performance evaluation of a mechanical vapor compression desalination system," *Desalination*, vol. 166, pp. 123–127, Aug. 2004, doi: 10.1016/j.desal.2004.06.066.

[8] "Mechanical Vapor Recompression Evaporation," Dec. 17, 2012. https://www.pfonline.com/articles/mechanical-vapor-recompression-evaporation(2) (accessed Apr. 27, 2023).

[9] Y. Ibrahim, R. A. Ismail, A. Ogungbenro, T. Pankratz, F. Banat, and H. A. Arafat, "The sociopolitical factors impacting the adoption and proliferation of desalination: A critical review," *Desalination*, vol. 498, p. 114798, Jan. 2021, doi: 10.1016/j.desal.2020.114798.

[10] S. Abolhosseini, A. Heshmati, and J. Altmann, "A Review of Renewable Energy Supply and Energy Efficiency Technologies," *SSRN Electron. J.*, 2014, doi: 10.2139/ssrn.2432429.

[11] "Wind energy." https://www.irena.org/Energy-Transition/Technology/Wind-energy (accessed Apr. 02, 2023).

[12] "How Do Wind Turbines Work?," *Energy.gov*. https://www.energy.gov/eere/wind/how-do-wind-turbines-work (accessed Apr. 02, 2023).

[13] "Wind Energy Basics," *Energy.gov*. https://www.energy.gov/eere/wind/wind-energy-basics (accessed Apr. 02, 2023).

[14] "How Wind Power Works | HowStuffWorks." https://science.howstuffworks.com/environmental/green-science/wind-power.htm (accessed Apr. 27, 2023).

[15] "Photovoltaics and electricity - U.S. Energy Information Administration (EIA)." https://www.eia.gov/energyexplained/solar/photovoltaics-and-electricity.php (accessed Apr. 02, 2023).

[16] A. O. M. Maka and J. M. Alabid, "Solar energy technology and its roles in sustainable development," *Clean Energy*, vol. 6, no. 3, pp. 476–483, Jun. 2022, doi: 10.1093/ce/zkac023.

[17] "Solar thermal power plants - U.S. Energy Information Administration (EIA)." https://www.eia.gov/energyexplained/solar/solar-thermal-power-plants.php (accessed Apr. 02, 2023).

[18] "Hydropower Basics," *Energy.gov*. https://www.energy.gov/eere/water/hydropower-basics (accessed Apr. 02, 2023).

[19] "Hydroelectric Energy." https://education.nationalgeographic.org/resource/hydroelectric-energy (accessed Apr. 02, 2023).

[20] "What is Geothermal Energy? How Does it Work?" https://www.twi-global.com/technical-knowledge/faqs/geothermal-energy/home.aspx (accessed Apr. 02, 2023).

[21] "How does geothermal energy work to produce electricity?," *BBC Science Focus Magazine*. https://www.sciencefocus.com/science/how-does-geothermal-energy-work-to-produce-electricity/ (accessed Apr. 02, 2023).

[22] "What is a Hydrogen Fuel Cell and How Does it Work?" https://www.twi-global.com/technical-knowledge/faqs/what-is-a-hydrogen-fuel-cell.aspx (accessed Apr. 23, 2023).

[23] "Platinum-free catalysts could make cheaper hydrogen fuel cells | Argonne National Laboratory," May 20, 2020. https://www.anl.gov/article/platinumfree-catalysts-could-make-cheaper-hydrogen-fuel-cells (accessed Apr. 23, 2023).

[24] B. Derasmo, "Solving the Intermittency Problem with Battery Storage," *POWER Magazine*, May 21, 2022. https://www.powermag.com/solving-the-intermittency-problem-with-battery-storage/ (accessed Apr. 27, 2023).

[25] "Researchers identify alternative to lithium-based battery technology," *ScienceDaily*. https://www.sciencedaily.com/releases/2022/05/220531161314.htm (accessed Apr. 27, 2023).

[26] A. A. and L. L. Kazmerski, "Renewable Energy Opportunities in Water Desalination," in *Desalination, Trends and Technologies*, M. Schorr, Ed., InTech, 2011. doi: 10.5772/14779.

[27] B. W. Tleimat, "Optimal water cost from solar-powered multieffect distillation," *Desalination*, vol. 44, no. 1–3, pp. 153–165, May 1983, doi: 10.1016/0011-9164(83)87115-X.

[28] E. Tzen, K. Perrakis, and P. Baltas, "Design of a stand alone PV - desalination system for rural areas," *Desalination*, vol. 119, no. 1–3, pp. 327–333, Sep. 1998, doi: 10.1016/S0011-9164(98)00177-5.

[29] M. Thomson and D. Infield, "A photovoltaic-powered seawater reverse-osmosis system without batteries," *Desalination*, vol. 153, no. 1–3, pp. 1–8, Feb. 2003, doi: 10.1016/S0011-9164(03)80004-8.

[30] X. Luo, J. Shi, C. Zhao, Z. Luo, X. Gu, and H. Bao, "The energy efficiency of interfacial solar desalination," *Appl. Energy*, vol. 302, p. 117581, Nov. 2021, doi: 10.1016/j.apenergy.2021.117581.

[31] R. Vujčić and M. Krneta, "Wind-driven seawater desalination plant for agricultural development on the islands of the County of Split and Dalmatia," *Renew. Energy*, vol. 19, no. 1–2, pp. 173–183, Jan. 2000, doi: 10.1016/S0960-1481(99)00029-4.

[32] M. Forstmeier *et al.*, "Feasibility study on wind-powered desalination," *Desalination*, vol. 203, no. 1, pp. 463–470, Feb. 2007, doi: 10.1016/j.desal.2006.05.009.

[33] "What Is a Malware Attack? Definition & Best Practices," *Rapid7*. https://www.rapid7.com/fundamentals/malware-attacks/ (accessed Apr. 08, 2023).

[34] "What is phishing | Attack techniques & scam examples | Imperva," *Learning Center*. https://www.imperva.com/learn/application-security/phishing-attack-scam/ (accessed Apr. 08, 2023).

[35] "What is a distributed denial-of-service (DDoS) attack?," *Cloudflare*. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed Apr. 08, 2023).

[36] "What is SQL Injection? Tutorial & Examples | Web Security Academy." https://portswigger.net/web-security/sql-injection (accessed Apr. 09, 2023).

[37] "What is MITM (Man in the Middle) Attack | Imperva," *Learning Center*. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (accessed Apr. 09, 2023).

[38] "Cross Site Scripting (XSS) | OWASP Foundation." https://owasp.org/www-community/attacks/xss/ (accessed Apr. 09, 2023).

[39] "What is APT (Advanced Persistent Threat) | APT Security | Imperva." https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ (accessed Apr. 09, 2023).

[40] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of Local False Data Injection Attacks With Reduced Network Information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015, doi: 10.1109/TSG.2015.2394358.

[41] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017, doi: 10.1109/JSYST.2014.2341597.

[42] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017, doi: 10.1109/ACCESS.2017.2769099.

[43] Y. He, G. J. Mendis, and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[44] R. Tan *et al.*, "Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017, doi: 10.1109/TIFS.2017.2676721.

[45] M. Housh and Z. Ohar, "Model-based approach for cyber-physical attack detection in water distribution systems," *Water Res.*, vol. 139, pp. 132–143, Aug. 2018, doi: 10.1016/j.watres.2018.03.039.

[46] V. R. Palleti, Y. C. Tan, and L. Samavedham, "A mechanistic fault detection and isolation approach using Kalman filter to improve the security of cyber physical systems," *J. Process Control*, vol. 68, pp. 160–170, Aug. 2018, doi: 10.1016/j.jprocont.2018.05.005.

[47] A. Elsaeidy, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "A Machine Learning Approach for Intrusion Detection in Smart Cities," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Sep. 2019, pp. 1–5. doi: 10.1109/VTCFall.2019.8891281.

[48] L. Che, X. Liu, Z. Li, and Y. Wen, "False Data Injection Attacks Induced Sequential Outages in Power Systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019, doi: 10.1109/TPWRS.2018.2871345.

[49] J. Duan and M.-Y. Chow, "A Resilient Consensus-Based Distributed Energy Management Algorithm Against Data Integrity Attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729–4740, Sep. 2019, doi: 10.1109/TSG.2018.2867106.

[50] X. Liu, A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos, "Assessment of Low-Budget Targeted Cyberattacks Against Power Systems," in *VLSI-SoC: Design and Engineering of Electronics Systems Based on New Computing Paradigms*, N. Bombieri, G. Pravadelli, M. Fujita, T. Austin, and R. Reis, Eds., in IFIP Advances in Information and Communication Technology, vol. 561. Cham: Springer International Publishing, 2019, pp. 232–256. doi: 10.1007/978-3-030-23425-6_12.

[51] P. H. N. Rajput, P. Rajput, M. Sazos, and M. Maniatakos, "Process-Aware Cyberattacks for Thermal Desalination Plants," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, Auckland New Zealand: ACM, Jul. 2019, pp. 441–452. doi: 10.1145/3321705.3329805.

[52] M. R. Khalghani, J. Solanki, S. K. Solanki, and A. Sargolzaei, "Resilient and Stochastic Load Frequency Control of Microgrids," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*, Aug. 2019, pp. 1–5. doi: 10.1109/PESGM40551.2019.8974111.

[53] T. Huang, B. Wang, J. Ramos-Ruiz, P. Enjeti, P. R. Kumar, and L. Xie, "Detection of Cyber Attacks in Renewable-rich Microgrids Using Dynamic Watermarking," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, Aug. 2020, pp. 1–5. doi: 10.1109/PESGM41954.2020.9282071.

[54] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, Sep. 2020, doi: 10.1109/TIE.2019.2944091.

[55] A. O. Aluko, R. P. Carpanen, D. G. Dorrell, and E. E. Ojo, "Impact Assessment and Mitigation of Cyber Attacks on Frequency Stability of Isolated Microgrid Using Virtual Inertia Control," in *2020 IEEE PES/IAS PowerAfrica*, Aug. 2020, pp. 1–5. doi: 10.1109/PowerAfrica49420.2020.9219790.

[56] M. Jorjani, H. Seifi, A. Y. Varjani, and H. Delkhosh, "An Optimization-Based Approach to Recover the Detected Attacked Grid Variables After False Data Injection Attack," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5322–5334, Nov. 2021, doi: 10.1109/TSG.2021.3103556.

[57] N. K. Singh and V. Mahajan, "End-User Privacy Protection Scheme from cyber intrusion in smart grid advanced metering infrastructure," *Int. J. Crit. Infrastruct. Prot.*, vol. 34, p. 100410, Sep. 2021, doi: 10.1016/j.ijcip.2021.100410.

[58] M. Jafari, M. H. Shahriar, M. A. Rahman, and S. Paudyal, "False Relay Operation Attacks in Power Systems with High Renewables," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*, Jul. 2021, pp. 01–05. doi: 10.1109/PESGM46819.2021.9637969.

[59] M. Mohammadpourfard, Y. Weng, I. Genc, and T. Kim, "An Accurate False Data Injection Attack (FDIA) Detection in Renewable-Rich Power Grids," in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, May 2022, pp. 1–5. doi: 10.1109/MSCPES55116.2022.9770151.

[60] P. Zhao *et al.*, "Cyber-Resilient Multi-Energy Management for Complex Systems," *IEEE Trans. Ind. Inform.*, vol. 18, no. 3, pp. 2144–2159, Mar. 2022, doi: 10.1109/TII.2021.3097760.

[61] H. Ali, O. M. Elzeki, and S. Elmougy, "Smart Attacks Learning Machine Advisor System for Protecting Smart Cities from Smart Threats," *Appl. Sci.*, vol. 12, no. 13, Art. no. 13, Jan. 2022, doi: 10.3390/app12136473.

[62] D. Bogdanov, A. Gulagi, M. Fasihi, and C. Breyer, "Full energy sector transition towards 100% renewable energy supply: Integrating power, heat, transport and industry sectors including desalination," *Appl. Energy*, vol. 283, p. 116273, Feb. 2021, doi: 10.1016/j.apenergy.2020.116273.

[63] D. Xevgenos, K. Moustakas, D. Malamis, and M. Loizidou, "An overview on desalination & sustainability: renewable energy-driven desalination and brine management," *Desalination Water Treat.*, vol. 57, no. 5, pp. 2304–2314, Jan. 2016, doi: 10.1080/19443994.2014.984927.

[64] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017, doi: 10.1109/TII.2017.2656905.

[65] M. Sun, J. Cremer, and G. Strbac, "A novel data-driven scenario generation framework for transmission expansion planning with high renewable energy penetration," *Appl. Energy*, vol. 228, pp. 546–555, Oct. 2018, doi: 10.1016/j.apenergy.2018.06.095.

BIOGRAPHIES

Aya Elshinawy is a graduate of Sustainable and Renewable Energy Engineering from University of Sharjah, UAE. Currently pursuing her Master's degree in Electrical Engineering, specializing in Smart Energy at Rochester Institute of Technology (RIT), Dubai Campus.

Dr. Abdalla Ismail Alzarooni is a professor of Electrical Engineering at Rochester Institute of Technology, Dubai, UAE. He received his Ph.D. in Electrical Engineering from the University of Arizona, USA. He has over 35 years of experience in higher education, teaching, research and management. He was the Associate Dean of Faculty of Engineering and member of the President Technical Office at UAE University. His education and research interests are in intelligent control systems, smart energy and grids, and renewable energy. He published over one hundred and ten technical papers and two co- authored books. He has participated in several higher education quality assurance and accreditation programs boards and committees in the UAE and other GCC countries. He received several prizes and awards including the Emirates Energy Award, IEEE Millennium award, and Fulbright scholarship.