Concordia Institute for Information System Engineering (CIISE)

INSE 6680 System Physical Security

Project Final Report

A Survey on Cyber Physical System

Security Challenges and Threats on SmartGrid

Submitted to:

Professor Dr. Mohsen Ghaffouri

Submitted By:

Student Name	Student ID
Parveen Parveen	40120909
Chandrima Chakraborty	40127853

Table of Contents

List of Figures

1. ABSTRACT

This report will give insights to some of the challenges faced by the cyberspace when deploying a smart grid. As more and more smart grid technologies are developed and deployed, the operational features, of these frameworks is building out to be more predominant and progressively complex in many ways, and the cyber space for the smart grid is expanding and it's significance continues to grow with each passing day.

The safety and security of a smart grid is of utmost value to keep up the smooth operation of power systems, even during adverse situations when the grid's security is breached, and power is cut off for unforeseen circumstances. In order to provide a safe and secure smart grid one must make sure the chances of hardware glitch or software malfunction is kept at is minimum. If the security protocols are compromised for any reasons, bad actors can infiltrate the system and cause blackouts which can have a run-off and result in lot of financial stress. Thus, ensuring that the grid is secure and is free of incursions should be the highest priority.

The smart grid infrastructure is different from traditional grid in many ways, one key difference is that smart grids access the internet space and can be controlled remotely. The power generation is way more advanced, and it considers the trends going to the future and also provides a lot of unique functionalities to its consumers who never got to use these features with traditional grids. In order to ensure a smooth power generation using smart grids the hardware that makes the grid is modernized and is able to communicate to the control center using specialized software. This creates a cyber space domain where infiltrators can hack and compromise the system. Though this seems dangerous, one cannot neglect the insights and advantages a smart grid can offer to the consumer and the utility company. Thus, ensuring the secure operation of a smart grid is the key going forwards. Any breach/violation can lead to monetary losses, lack of customer loyalty and can also have national security issues for any affected nation. We have discussed some of the attacks that took place and how they were rectified and what were their consequences in detail in the upcoming sections. [1]

With cyber terrorists becoming more and more proficient with their techniques ensuring the safety of a grid is a race against time. In most cases with the current technology an attack can only be realized once it happens, and the utility companies are always looking for mitigation and not prevention. If we as a society keep growing the energy needs will only increase and mitigation is not the way forward. With increasing cyber attacks, the potential consequences include power gird collapse and result in huge blackouts and financial losses that cannot be easily comprehended. Hence the key principles of cyber security such as availability, authenticity, non-repudiation, integrity, confidentiality and most importantly accountability must be upheld at all levels without leaving any room for compromise. This paper discusses all the properties in detail and how a smart grid can be compromised if we fail to uphold these values in detail.

2. INTRODUCTION:

Cyber physical systems or CSP's are the leading cutting-edge technology in terms of their computation, efficiency, procedures and frameworks. They facilitate heterogeneous components

with attention to increasing interactive, intelligent and distributive operations in a system. The CPS have made their mark for their high-end design and innovation.

In today's modern world an effective, reliable and scalable power framework is critical and impending. The electric force framework ought to be designed in a way that can withstand major cyber events and dynamically recuperate from physical and cyber events to prevent any disturbances that may arise due to these unforeseen circumstances. The current grid in use is extremely complex and includes interdependent parameters. The varying layers of progressive control must be taken into consideration, which include numerous examples of complex and interdependent cyber resources controlling the physical hardware related with the power grid. It is important to note that the power grid id the lifeline for the masses and any disruptions to its functioning can be catastrophic.

The current electric grid has four major components, and all the players are of paramount importance. The four components include:

1. **Power Generation**: The starting or the initial phase where electricity is generated through renewable and non-renewable sources ranging from oil and natural gas, nuclear plants, solar grids, hydro electric power plants, wind farms etc.,
2. **Transmission:** Once the power is generated it should be transmitted over long distances through power lines.
3. **Distribution:** The high voltage must be downsized for appropriate consumption at the client's end.
4. **Consumption:** The different consumers have varying needs. It is important to take into the consideration of businesses, industries, transportation, utilities, education facilities, healthcare and many more players.

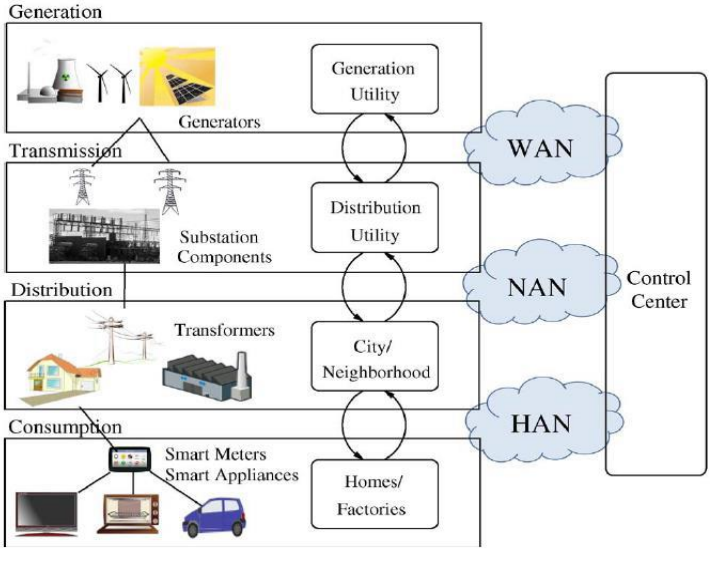

Figure1: Cyber Security view of Smart Grid

The traditional power distribution systems were used to transport electrical energy produced at a central power plant by varying the voltage levels and then distributing it to the consumers by dropping voltage levels significantly. Although, this method has several impending

shortcomings, which include the properties such as unable to include various power generation sources, high cost and expensive resources, time-consuming processes which led to increasing downtime, high carbon emission, and frequent blackouts.

For example, a study conducted by researchers at the Berkeley National Laboratory in 2004 showed that power interruptions have cost the American economy approximately $80 billion per year; other estimates indicate a higher cost of $150 billion per year. It is clear evidence that these problems cannot be fixed with the existing electricity grid which seems quaint. Hence a much more modern and technologically advanced and efficient grid is the need of the hour. But such grids have their own pitfalls as well. It all comes down to the tradeoffs that can maximize the efficiency and minimize risks.

One of the major problems that needs paramount importance is blackouts. Blackouts are regularly perceived simply after customers report of it happening. Keeping up with power generation to demand is challenging since utilities managements company do not have techniques to anticipate request and to demand request decrease (load shedding). We were given a clear example in March 2021, when the Texas power generation systems crippled under the harsh winter conditions. Though the cause has been greatly attributed to lack of winterization of the system, a major reason was demand went up sharply and the producers could not produce adequate power to meet the demand. As a result, they have to over produce power for top requesting which is costly what's more problematic is, it adds to overall Green-house Gas (GHG) outflows. For obvious reasons it is also hard to join variable power generation sources, for example, such as wind and solar power, into the grid. Combining all the sources is challenging and needs a lot of resources and capital.

Hence, we now ask ourselves, how can we solve all the potential drawbacks of the system? The concept of smart grids has now evolved. The smart grid is an embodiment of data and the infrastructure of the power generating resources which gives the users the access to power without any major disruptions. The goal of the smart grid revolves around adaptability, improved quality, effective energy distribution. These parameters are in turn governed by the combination of various key advances in technology, two-way communication, advanced components and control methods, improved metrics and decision support systems.

It is to be noted that, it is completely normal that the heterogeneous, diverse and complex segments that make up the grid will create a plethora of vulnerabilities. Additionally, the power grid is the foundation of any society which assists in keeping up every imperative area that are pivotal to financial stability and social prosperity. Thus, when we introduce modern information systems into the smart grid, we will have to encounter the potential for cyber and physical attacks with the aim of getting to critical data or even cause major disruptions which hurt the economy badly.

This report addresses various issues that pose dangers to such modern Smart Grid Systems and provides insights on how to possibly mitigate and prevent such adverse effects if they were to happen on a regular basis.

3. PRELIMINARY STUDY:

In order to understand the changing dynamics of the Smart grid networks we need to look at the existing smart grids that are in use and the data that are generated from them can be better used to rationalize decisions going forward. Smart grids have been in use at varying levels in different parts of the world and in the upcoming section we have discussed a few systems that were compromised to varying levels.

The first instance happened on August 14, 2003, when huge segments of the Midwest and Northeast United States and Canada, encountered a power outage which stayed for as long as 96 hours in some parts by posing difficulties to around 50 million citizens and 61,800 megawatts (MW) of burden in some parts of the United States of America. After investigation it was found that this huge scope power outage was not related to any malicious activity of the cyber terrorists but rather caused by a failure in the software program of the cyber system. This gives an example of what to expect when such crisis happens in real time.

The second potential disruption happened in Italy in the same year. In September of 2003 a major disruption caused massive blackout in the Italian peninsula and some parts of Switzerland. This outage affected more than 56 million people and the outage which lasted close to 20 hours in Italy put a lot of strain on the country's finances. The cause of the mistake was found to be human made but what made it worse was the lack of communication between the systems for mitigation.

The next recorded and studied case of malfunction happened in 2006 near the South Western Europe. This black out which happened to affect several countries was also attributed to human made errors and lack of communication which could have saved the system from ballooning under stress.

In 2010 a dangerous worm named Stuxnet which spreads through vulnerabilities in Windows was found to be targeting Siemens equipment and it led to significant damages to the grid that used Siemens hardware and also caused the company in monetary losses. This is a clear cut example of an intrusion into the system to cause havoc and result in losses for the producers and consumers.

In the 2011 report of RISI, Repository for Industrial Security Incidents found that 35% of the incidents were a direct result of remote intrusions. Between 2004 and 2008 there were close to 12 incidents of such scope which is a 20% increase compared to the previous four years. So it is clear that with more modern and sophisticated technology the dangers of such attacks is trivial and they tend to keep outpacing the market.

From the above-mentioned case studies, it is without doubt that major cyber and physical vulnerabilities of the smart grid framework are identified to be cyber issues. Trojans, bugs and worms keep crawling the systems unnoticed and later unleash their potential causing disruptions. Taking this into account , the Smart Grid Infrastructure Security (SGIS)which is a governing body must address the intentional attacks by cyber terrorists or hacktivists and other industrial espionage players, disgruntled employees, user errors, equipment failures, and natural disasters. The recent incidents related to cyber-attacks in a smart grid were discussed in this

section which motivates the power system design, effective communication strategies and writing better software which happens to be a big scope in these systems.

4. FEATURES OF A SMART GRID:

The primary advantage of using a smart grid in the first places is the option to expand the grid versatility and reduce greenhouse emissions. Resilience is the ability of a given entity to resist unexpected events and recover quickly thereafter. This is also called as fault tolerance. In today's world, the versatility of a grid has become non-debatable and is of paramount need, particularly when power interference can potentially affect the economy and cause losses in billions within a matter of hours. [2]

The smart grid promises to give potential adaptability to such scenario if they were to happen and unquestionable quality by empowering power supply, allowing the integration of new assets into the grid, and empowering restorative abilities when such failures happen do happen. The goal is to prevent failures in the first place but if they were to happen the goal will be to turn around quickly with less damage. Another byproduct of smart frameworks is to power electric vehicles as trades for regular vehicles keep increasing year over year, and decreasing energy utilized by clients and reducing energy losses within the grid which tend to be costly in the long run.

CONCEPTUAL MODEL FOR A SMART GRID:

According to NIST (National Institute for Standards and Technology) a smart is made up of seven building blocks. They include generation, transmission, distribution, customer, markets, service provider, and operations. Each block has its set of actors and applications. Thus each block has its own vulnerability and putting one over the top of other will add to complexity of the systems. And each layer is tasked with a set of functions which are trivial to it's existence.

Given below is an example for a smart grid with seven layers.

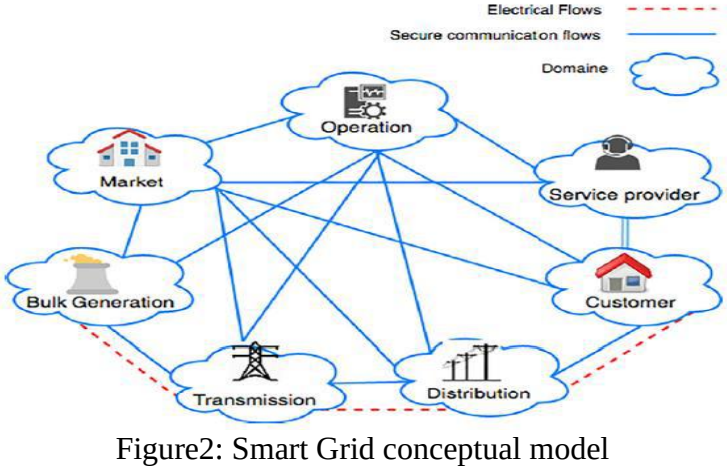

Figure2: Smart Grid conceptual model

The main actor is the end user in the client domain. The clients are a trivial part of this whole architecture as it is easy to compromise things at the client's end. It is also important to note that

without the existence of customers there is no business model. Generally speaking, there are three types of clients: home, commercial, and industrial. In addition to consuming electricity, these actors can also generate, store, and manage the use of energy on their own. We have seen customers increasingly opting to renewable sources like solar and installing power walls. This domain is connected to the distribution domain and communicates with the different players in the distribution, operation, market and service provider. In the market domain, actors are the operators of such grids and the different participants in the electricity markets. This domain is responsible for maintain the tradeoffs between supply and demand. In order to keep up the production with demand, the market domain communicates frequently with the supply domains which encompass the bulk generation domain and distributed energy resources (DER) respectively. [3]

The service provider domain includes the organizations that provide services to both electrical customers and utilities. They act as a bridge between the different players. These organizations are responsible for providing services such as billing, customer account, track energy usage. Naturally this domain has a lot of information and can use these data to gain valuable insights to improve their business models. The service provider communicates with the operation domain for situational awareness, system control operations and also communicates with customer and market domain to develop smart services such as enabling customer interaction with market applications to meet their standards and needs and also energy generation at home. The operations domain's actors are the managers for the movement of electricity from source to destination. This domain maintains efficient and optimal operations in transmission and distribution of electricity and is a trivial cog in this seven-layer architecture. In transmission, it uses energy management systems (EMS), whereas in distribution it uses distribution management systems (DMS). These two systems help in managing and distributing power evenly and efficiently.

The bulk generators tend to produce electricity in very large quantities. The energy generation is the first step in the process of delivering electricity to the client. The energy is generated using resources like oil, natural gas, coal, nuclear, wind and solar etc., The bulk generation domain is connected to the transmission domain and communicates through an interface with the other important domains like market domain, transmission domain, and operations domain.

In the transmission domain, the produced electrical power is carried over long distances from generation domain to distribution domain through various substations. It is to be noted that this can lead to losses in the power produced but is generally managed by the large quantities produced. This domain may also store and generate electricity using battery technology and other renewable sources. The transmission network is monitored and controlled via supervisory control and data acquisition (SCADA) system, which is an embodiment of a communication network, control devices, and monitoring devices. These components help in transmission and distribution of power. The distribution domain includes the distributors of electricity to the end user. This is mostly the local municipality.

The electrical distribution systems have different methodologies such as radial, looped, or meshed. Each architecture has its own advantages and disadvantages. The decision to go for a particular architecture depends on the market and the current need. They also look at trends that may arise in the future. In addition to distribution, this domain may also support energy

generation and storage. This distribution domain is in turn connected to the transmission domain and the customer domain. It also has an interface with the billing and accounting domain.

In order to make a smart grid that is efficient we need to have several heterogeneous components that work together and can act independently without any adverse influence on one another. There are two main such systems which are discussed in the upcoming sections.

The supervisory control and data acquisition also called as SCADA is a framework that is used to monitor and control an electric power grid. It is regularly used in large installations. It comprises of three important features: the human-machine interface (HMI), the remote terminal unit (RTU), Master terminal unit (MTU). The HMI provides the user interface that the administrators use to interact with the system. The RTU has three CPU like component and each have a very specific role, the initial one used for information retrieval, the second one is responsible for implementing the standards coming from the MTU which is a third component that is used for the communication. MTU acts as the brain of the entire SCADA system and controls the flow of information between RTU and HMI.

The advanced metering infrastructure (AMI) is a vital component for the client and the distribution domain. This AMI it is acquitted with the task of resourcing, estimating and analyzing energy needs. The AMI has a duplex communication mechanism between the client and the utility company. The AMI is made out of three essential segments namely: a smart meter, an AMI headend, and the communication network. The smart meter is an automated device that mainly focusses on tracking the energy utilization at a client facility, it records the power consumption and sends this data to the AMI headend which in turn will forward the data to the utility company. The utility company will use this data for billing and customer service and also gain insights that can better serve the clients. The AMI headend is typically a server that consists of a meter data management system also called as MDMS. The duplex communication that takes place between the smart meters, the home machines, and the AMI headend is typically via Z-waves.

5. SMART GRID ARCHITECTURE:

The architecture of a smart grid metering system is as given in the figure below.

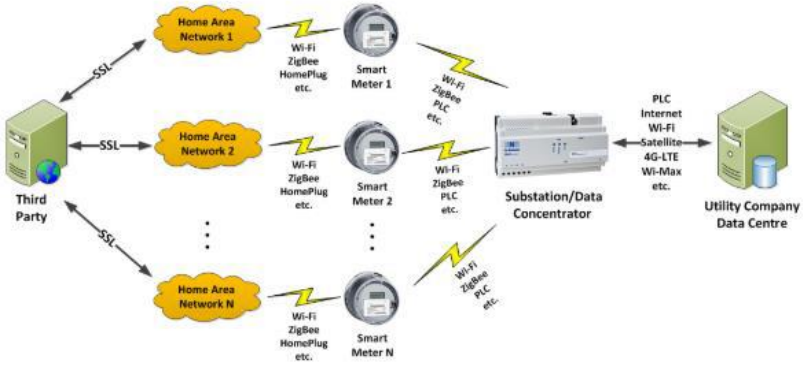

Figure 3: Smart Grid Architecture

From figure 1 we can identify the different components. The following section briefly describes the roles each component plays in a smart grid architecture.

Home Area Network (HAN):

The HAN is responsible for giving the client access, control and monitor the real-time power utilization. The HAN consists of a gateway that pulls theutilization information from the smart meter and displays it on a PC/tablet/cell phone. In addition, the gateway may share the data about the power utilization to any third parties for other value-added services. These services may include recommendations from the service provider, providing advice and so on. The HAN integrates the controller digitally that allows the client to remotely control the status of their home appliances and make changes to them if needed.[3]

The Utility Company and it's role:

The utility company communicates with various substation networks through a WAN interface and the communication station may use the services of Wi-Fi, satellite, 4G and so on. The utility company is liable for preparing cautions and alarms, record and validate the meter data, and manage accounting and billing. The Utility Company provides an application that can be web or mobile based and this application will allow the stakeholders to access their user account digitally. The account will be useful to provide billing information, power consumption and so on. This removes the need for traditional paper-based invoices.

Role of Substations:

The substation is responsible for disbursing the generated power to the clients. The managing team at the substation will monitor a specific region of the grid. They are responsible for collection, storage and management of locally generated data. They install smart meter at every client facility and this meter will record all the activities on the grid. The smart meter will relay the information to the substation's data collector via cables or wireless modes of transmission. The data collector will in turn transmit this information this information to the utility company who handle user accounts and customer service.

Smart Meter:

As discussed above the smart meter is a vital cog in this complex chain of communication. The meter has a microcontroller controlling all the activities, and the communication is handles by the communication bus which is another set of boards and cables that relay the meter information to the substation. The metrology board is where the actual computation takes place. The meter integrates itself with all the household devices via a Wifi router or a wired cable. The smart meter also has a control switch that enables the substation/utility company to cut down power supply to the client temporarily, should the need arise.

Third Party Services:
The third party service provider gets the information from the utility company and they provide value added services to the client. The purpose of these services should be to better assist the client to manage his power consumption and cut down on costs that are unnecessary.

6. SECURITY PARAMETERS DESIRED FOR A SMART GRID:

According to the NIST, there are three main desirable properties for any smart grid or any digital service in general. They are confidentiality, availability and integrity. The following section discusses the importance of each and every property and states the reasons why it is necessary to uphold these principles to the fullest of the potential.

Confidentiality:

The term confidentiality refers to limited access to the data generated. If a party has no scope with a particular piece of information then they must be restricted access to such information though it seems unnecessary. Confidentiality ensures the client the privilege that his/her data will not be released to unnecessary actors for unknown reasons. If any unapproved access happens then the confidentiality is lost and the client may become skeptic to use the services provided by the provider. This is very important as sensitive user information is shared by the meters installed at the user's facility.

Integrity:

The term integrity refers to the unauthorized access to sensitive data/ destruction of data that may prove to be financially stringent to any parties involved. In layman terms the user data should not be corrupted/changed/destroyed without his/her action. When the smart meter receives any communication from the substation it should verify the correctness of such received information. This refers to the authenticity of such information. There should be a handshake mechanism that validates that the information received is true and can be implemented.

Availability:

The term availability means uninterrupted access to the power supply. It is the most important parameter to be kept track of. Denial of Service (DOS) attacks tend to be more common and can potentially cost the economy in billions. When the smart meter is compromised and is unable to contact the substation then the duplex communication is technically cut off. This may be costly and dangerous as sometimes adjustments to the grid which can be life saving may be sent out by the substation, and when the substation can't open a connection, it is violating the availability principle and can be deadly.

There are three other properties that are desirable for any safe operating of a smart grid. The following section discusses the prospects of those properties in detail.

Non-repudiation:

There should be checks and balances in place so that any actions/tasks performed by either the client or the service provider cannot be denied later in the future. This can be become a serious issue when sensitive information is being transmitted and no one wants to claim ownership of their actions.

Authentication:

The term authentication involves verifying the identity of any stakeholder. The users must be verified and the machines must also be subjected to various firewalls and communication protocols so that any undesired bad actors don't get access to sensitive information.

Authorization:

The term authorization refers to granting access rights to users/administrators/other services. This check is of paramount importance as bad actors can be filtered out from getting access to critical data.

7. FUNCTIONS OF A SMART GRID:

The smart grid is basically an upgrade to the traditional grid and so there are no big differences to its functionalities. The basic functions include:

- Managing power quality.
- Improve power utilization efficiency.
- Provide uninterrupted access to the users.
- Manage assets efficiently.
- Fault tolerant.
- Prevent attacks.
- Quick turnaround.
- Self-repairing.

8. REQUIREMENTS FOR A SECURE SMART GRID:

There are several components/heterogeneous components that are trivial for the safe operation for a smart grid. The following are some of the most important in the hierarchy.

Power market: There should be sufficient demand in order to establish a smart grid. The capital involved in establishing a smart grid is comparatively higher than the traditional grid. Hence if there is not adequate demand for power then it is not a cost effective solution.
Energy Management Systems: The EMS is responsible for the integration of the bulk generators and the transmitters.

Distribution Management Systems: The DMS is responsible for controlling the voltage across the transmission channels. As the bulk producers transmit in high voltages, the regular households need to subsequently downsize the power to appropriate levels. The DMS also makes sure that the wastage is kept at minimum.

Advanced Metering Infrastructure (AMI): The single piece of equipment that handles all the communication between the client and the service provider. It handles sensitive data such as billing, account management, consumption profile etc.

Wide Areas Measurement, Protection and Control (WAMPAC): It is a set of processes that provide monitoring, control and protection of the power grid.

The principles that govern all the components include authenticity, availability, confidentiality, integrity, non-repudiation.

9. CYBER PHYSICAL SECURITY CHALLENGES AND THREATS IN SMART GRID

Threats in Smart Grid Environment

Threats are described as "possible acts that could be taken against a framework." These acts may be intended to cause harm, such as death, injury, damage, the exposure of private information, interference with operations, or denial of service. It's not unusual to come across just a few sentences identifying challenges to fundamental structures. They are typically based on detailed characteristics, for example, the threat agent behind it, the level of intentionality, the manner by which the threat agent is organized, and so on. In this section, we will accumulate an overview of the present threats that could affect the smart grid from a set of various documents where this topic is addressed.

Accidental/Inadvertent threats:
Unintentional incidents can result in security threats to resources. Indeed, safety failures, infrastructure failures, carelessness, and natural disasters may sometimes cause more actual harm than intentional attacks. However, someone who is unfamiliar with proper procedure and policy can inadvertently trigger a danger.

Deliberate threats:
It's important to note that the legal, social, and financial consequences of effective targeted attacks can be enormous, far outweighing the physical harm.
Accidental/inadvertent threats may be further divided into various failures:

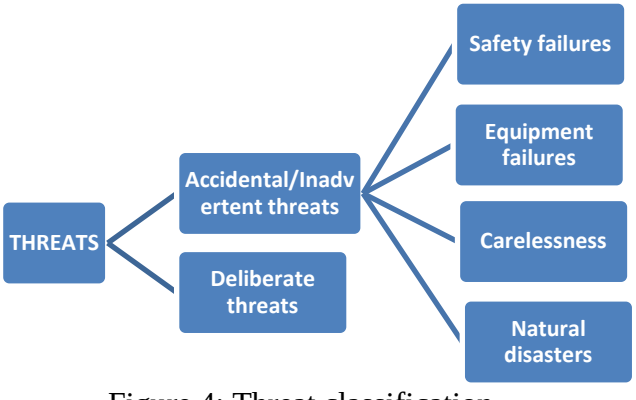

Figure 4: Threat classification

Safety failures:
Security has always been a primary concern. To improve this protection, cautious techniques have been developed and perfected over and over again. These methods are the most critical

component of a safety program; electronic methods for monitoring the status of key equipment and recording compliance with safety protocols can greatly increase safety and serve a number of purposes. For example, electronic monitoring of safety measures inside electric power substations can also help to prevent some deliberate attacks, such as vandalism and robbery.

Equipment failures:
These are the most commonly known and expected risks to the power system's reliability. Over the years, notable work has been completed, including redundant components and networks, hardware status tracking, and so on.

Carelessness:
Complacency ("no one has ever harmed any equipment in a substation yet"), laziness ("why bother to lock this door for the few moments I am moving into the other area"), or frustration ("these security measures are interfering with my ability to do my job") are all common reasons for carelessness. Examples of carelessness threats include: permitting tailgating into a substation; not locking doors; inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards; applying updates, corrections and other changes to operating systems and control applications without a previous test in a controlled environment; etc.

Natural disasters:
Storms, hurricanes, and earthquakes can cause widespread power outages, security breaches, as well as opportunities for robbery, vandalism, and terrorism.

10. SMART GRID SECURITY CHALLENGES

Clearly, smart grid can significantly enhance control over power use, use, and distribution to the benefit of customers, energy producers, and grid operators. But improved operations and administrations would come at the cost of exposing the entire power structure to new challenges, especially in the area of communication system and information framework security.
A description of the most important smart grid protection issues is given below. Some of them have only recently been presented in previous fields, while others are equally important.

Data and information security requirements:
ICT will become the latest smart grids' central nervous system. Streams of data and information will inundate all regions. Data integrity and availability will be crucial in the grid's operational sections (for example, generation, transmission, and distribution automation). Similarly, when handling end-buyer-related information, such as usage data or even personal data at billing systems, confidentiality must be ensured during transit and storage. Furthermore, the smart grid framework application will sometimes determine which security measurement is increasingly important for an equivalent bit of data.

Data protection specifications for each smart grid network domain and application should be clearly defined, with the goal of allowing manufacturers, operators, and other actors involved in smart grid creation and execution to set up the necessary security controls and technologies to protect smart grid data Encryption of data flows, tunneling, authentication and no repudiation,

digital certificates, and other topics including supply chain protection, firmware validation, and patch management should all be discussed.

Large numbers of "smart" devices:
The smart grid network would result in the installation of a large number of electronic and data-handling devices, forming a large mesh. When all is said and done, smart meters and gadgets, as well as the AMI communication system, are likely the most important model. However, substation robotization in the conveyance space, as well as the smartening of transformer focuses, will generate a slew of IED and related ICT advancements. Deploying, structuring, and maintaining a flexible and solid arrangement will be a huge test for grid administrators who aren't used to it and don't have the necessary mechanisms or even internal procedures in place. When all is said and done, smart meters and gadgets, as well as the AMI communication system, are likely the most important model. However, substation robotization in the transmission space, as well as the smartening of transformer focuses, will produce a slew of IED and related ICT advancements. Deploying, structuring, and maintaining a flexible and solid arrangement will be a huge test for grid administrators who aren't used to it and don't have the necessary mechanisms or even internal procedures in place. This will greatly complicate the situation. Frameworks or software as a service, cloud storage, and security in depth strategies should all be considered, especially for small and medium-sized businesses.

Physical security and grid perimeter:
A Smart Grid is a DSO's (Distribution System Operator) most significant investment and a national asset that relies on mission-critical and life-saving services. Every second of every day, the government, businesses, and people depend on the service it provides. It provides revenue to the energy provider, and it gives the DSO access to highly privileged and confidential customer information. At considerable cost, the information and communications technology (ICT) industry has discovered that perimeter security against cyber criminals is insufficient. A perimeter is made up of a mix of technology, procedures, and people. Even if the ICT component provides high theoretical security, the mechanism and people will build "loopholes," which cyber-criminals are expert at exploiting.[4]

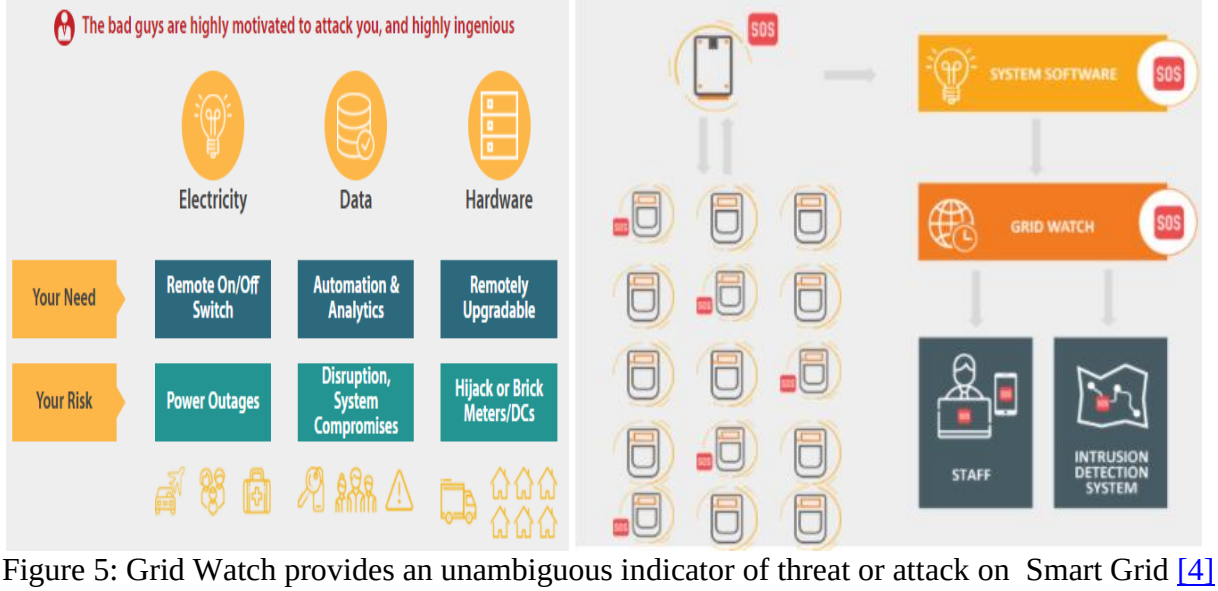

Figure 5: Grid Watch provides an unambiguous indicator of threat or attack on Smart Grid [4]

Legacy and (in)secure communication protocols:
Many of the communication protocols currently in use for power generation, transmission, and distribution control and robotization were never developed with protection in mind. Many of these protocols were originally envisioned as serial protocols with no built-in message authentication. Furthermore, since none of these protocols employ encryption or message integrity mechanisms, contact is vulnerable to eavesdropping, session hijacking, and manipulation. Despite the fact that these flaws have existed for a long time, new factors have increased the actual danger. To reduce costs and improve execution, organizations are switching from proprietary systems to generic networking protocols such as TCP/IP (i.e. Modbus/TCP, IEC 104, etc.) or new mainstream open protocols, such as OPC. Similarly, traditional legacy communication protocols, such as IEC 101, can now be found in their TCP/IP encapsulated form, with no protection mechanism in place. The capacity to control should be open to administrators.

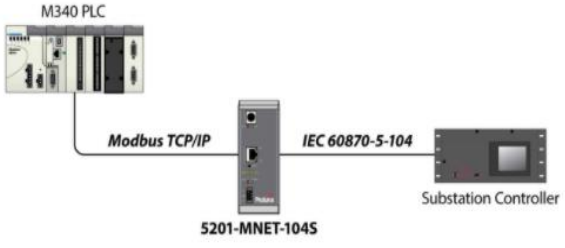

Figure 6: Modbus TCP/IP to IEC 60870-5-104 Server Gateway[5]

Connectivity:
The communication network in a smart grid is complicated since it connects a large number of interconnected devices. Given the decentralized design of the smart grid, the systems must have a high degree of security against attacks and vulnerabilities. Attacks may result in physical harm, power outages, and inefficiency. This is because, adversary gain control of the framework.

Trust:
Owing to the high connectivity of smart grid networks, clients are no longer considered to be trustworthy, which has impacted design decisions. Just a few consumers will stick to the agreements and understandings. Clients could, for example, intentionally damage the smart meter in order to disclose false data about power usage in order to save money.

Customer's Privacy:
The integration of smart meters into the smart grid raised various challenges in terms of protecting client data. Client information includes details on when they are available at home or on the road. It can also extract data about their everyday habits, such as sleeping, watching TV, or even what appliances they are using. The collected information is of interest to criminals planning a crime, businesses, advertisers looking to advertise, and even rivals. As a result, information should be protected during the transmission and capability procedures to prevent unauthorized access to data and ensure the client's privacy is protected.

Protocol attacks:
The protocols used in the power system, such as ICCP, IEC 61850, and DNP3, are not properly secured, they could be used to conduct cyber attacks. This necessitates stable versions of these

protocols that provide not only protection but also the latency and reliability guarantees needed by grid applications.

Routing attacks:
This is a cyber-attack on the routing infrastructure of the Internet. Despite the fact that this attack is not specifically related to grid operation, it may have an effect on some power system applications that depend on it, such as Realtime markets.

Software Vulnerabilities:
Malware-infected software suffers from a wide range of vulnerabilities. SCADA (supervisory control and data acquisition) systems are commonly useful innovations that are vulnerable to malware and malicious updates. A widely useful framework has a new significant weakness that must be solved in order for the framework to remain current. Patching, on the other hand, is regarded as a difficult process, especially in sensitive systems such as the smart grid, since it is costly and can result in downtime.

Intrusions:
This denotes to exploiting vulnerabilities in the software and communication infrastructure of the grid which then give access to critical frameworks elements. Example intrusion scenario is to gain access to substation HMI bypassing security controls (firewalls, system passwords).

Malware:
Malicious software that takes advantage of flaws in device software, programmable logic controllers, or protocols is referred to as this. The malware mainly searches the system for possible victim devices, exploits explicit vulnerabilities in those machines, distributes the malware payload to the victims, and then spreads itself. Malware attacks are developing in numbers and complexity, and this has been a source of significant worry for critical infrastructure systems including the power grid.

Denial of service attacks:
Denial of service is a term used to describe any attack that prevents actual clients from receiving basic administrations. In the sense of the power grid, this may also imply a loss of control. Major resource exhaustion attacks, which overwhelm the communication network or the server with massive amounts of traffic or fake workloads, refuse service to legitimate users, are typical of these attacks.

Insider threats:
An insider takes advantage of existing device privileges to commit a malicious act. Many federal documents, including the GAO CIP study, have described this type of threat as a source of concern in recent years.

Threat	Property Violated	Threat Definition
Spoofing identify	Authentication	Pretending to be something or someone other than yourself
Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Providing information to someone not authorized to access it
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Table 1: Attacks along with associated security property and definition [6]

Fake Topology:
In this type of attacks, a attacker attempts to create fake links, which resulting in changing the main server's view of the network. A compromised switch can also misguide the server by sending deceived packets.

Switch Black-hole:
A hacked or malicious router/switch can drop the packet immediately or abruptly terminate the flow path. It can also be set to drop packets of a specific form (for example, TCP or UDP) or from a specific source. In network jargon, this condition is referred to as a "black hole." As a result, traffic cannot be diverted to its destination, and the system's operation is badly harmed.

Interception of SCADA frames:
An intruder can intercept SCADA Distributed Network Protocol3.0 (DNP3) frames and decrypt plaintext frames that contain important data, such as source address and destination addresses, using a protocol analysis tool for sniffing network traffic. This collected data, which composed control and setting data, may be diverted to another SCADA system or intelligent equipment computer (IED) at a later date, potentially shutting down networks or causing service interference.

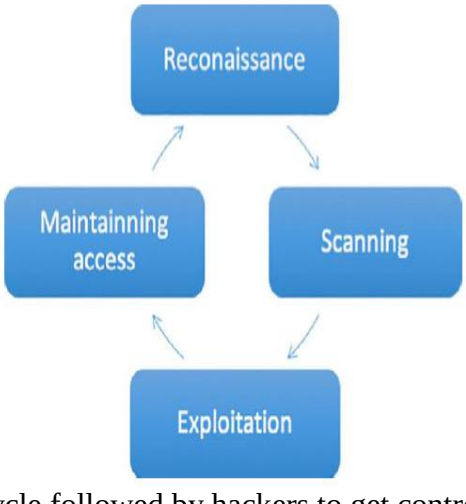

Figure 7:Attacking cycle followed by hackers to get control over a system [7]

Education and training

Furthermore, it is critical to emphasize that customers and utilities are under the benefits, costs, and risks associated with smart grid frameworks. Due to a lack of awareness, required investments, standardization actions, regulatory and policy initiatives, and so on may be overlooked. In this context, education and training, as well as public awareness campaigns, should be encouraged in order to generate the required momentum for the development and deployment of fully secure smart grids.

Information sharing

The electricity industry lacks practical systems for sharing and managing data related to cyber security incidents. The electricity industry lacks a reliable method for disseminating information about smart grid cyber security flaws, incidents, threats, lessons learned, and best practices. Furthermore, in some districts, such as the United States, the current administrative situation is contributing to the creation of a culture of consistency rather than a culture focused on achieving a far-reaching and effective cyber security. As a result of the industry's immaturity in terms of cyber security, vendors and operators are implementing security controls based on a variety of standards as well as their own proprietary mechanisms. As a result, there is a lack of interoperability, real security, and even hard security management.

Human factors

Include all of the human qualities and situations that a hacker would use to accomplish his or her malicious objectives. The security training that employees receive and the awareness-raising activities that groups engage in lawfully influence these human viewpoints and situations.

Social engineering attacks will test security awareness and training of the employees of smart grid operators, manufacturers, end consumers and so on. For example, an adversary may attempt to impersonate an employee from the utility's contractual worker to determine confidential data, for example as authentication credentials, or to get additional privileges in certain equipment. Regular instances of social engineering attacks also include the following

• Impersonating an employee in front of the IT Help Desk to change his or her password

• Pretending to be contractors in order to gain access to potentially confidential information or sabotage equipment

• Implanting a backdoor into the IT/smart grid infrastructure by leaving USB key drives containing malicious software in strategic locations.

• Phishing e-mails aimed at obtaining confidential information, such as consumer information.

Reconnaissance

The primary stage of reconnaissance,includes the attacks: social engineering and traffic analysis.

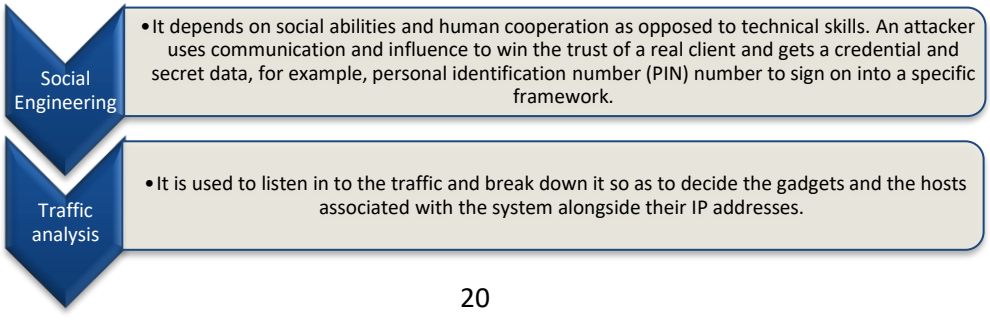

Figure 8: Social Engineering Attack Cycle[8]

Scanning Network:
The next step is to attack the network to find all of the gadgets and hosts that are still alive. IPs, ports, services, and vulnerabilities are the four kinds of scans. Typically, a hacker would begin with an IP scan to identify all of the hosts connected to the network as well as their IP addresses. Then he or she digs a little deeper by scanning the ports to see which ones are open.This scan is carried out on each networked host that has been uncovered. After that, the hacker performs a service scan to determine which service or system is running behind each opened port. If a system's port 102 is detected open, the attacker may deduce that the system is a substation automation control or messaging system. The target system is a phasor measuring unit if port 4713 is open (PMU). The final step, a vulnerability scan, aims to find flaws and vulnerabilities in each service on the target machine so that it can be exploited later. Industrial protocols Modbus and DNP3 are both vulnerable to scanning attacks. Since Modbus/TCP was designed for communication rather than security, it can be hacked using a technique known as Modbus network scanning. This attack includes sending a friendly message to all networked devices in order to gather information about them. Mod scan is a Modbus network scanner for SCADA systems that detects open Modbus/TCP connections and identifies device slave IDs along with their IP addresses. [9]

Exploitation
The third step, exploitation, involves malicious activities that attempt to exploit the smart grid component's vulnerabilities and get the control over it. These activities include viruses, worms, Trojan horses, denial of service (DoS) attacks, man-in-the-middle (MITM) attacks, replay attacks, channel jamming, popping the human-machine interface (HMI), integrity violations, and privacy violations are all examples of these operations.[10]

A **virus** is a program used to contaminate a particular device or a framework in smart grid. A worm is a self-reproducing program. It uses the network to spread, to duplicate itself, and to infect different gadgets and frameworks.[11]

Attacks	Description
Trojan horse	It is a program that appears to perform a legitimate task on the target system. However, it generates a malicious code in the background. An intruder uses this type of malware to upload a virus or worm on the target system.
denial of service (DoS)	Few techniques are used, especially SYN attack, buffer overflow, teardrop attacks, and smurf attacks, puppet attack, and time synchronization attack (TSA). A SYN attack abuses the three-way handshake (SYN, SYN-ACK, ACK) used to set up a Transmission Control Protocol (TCP) session. The adversary floods a target framework with connection requests without responding to the replays, pressuring the framework to crash. The Modbus/TCP protocol is vulnerable against these attacks since it works over TCP
Buffer overflow	The intruder sends a huge amount of data to a specific system, thereby exhausting its resources. For example, ping-of-death is considered as a buffer overflow attack because it exploits the internet control message protocol (ICMP) by sending over 65 K octets of data. It then makes the system crash.
Teardrop attack	An attacker modifies the length and fragmentation offset fields in sequential IP packets. Once the target system accepts these packets, it crashes because the instructions on how the fragments are offset within these packets are contradictory.
Smurf attack	The attacker targets a particular framework, yet it can immerse and congest the traffic of a whole system. It comprises of three components: the source site, the bounce site, and the target site. For source site, the attacker sends a spoofed packet to the broadcast address of the bounce site. These packets stores the IP address of the target system. Once the bounce site gets the forged packets, it broadcasts them to all hosts associated with the system and afterward makes these hosts replay, saturating then the target system.
Time synchronization (TSA) attack	It targets mainly the timing information in the smart grid as power grid operations such as fault detection and event location estimation depend highly on precise time information. Most of the measurement devices in smart grid are equipped with a global positioning system (GPS), attack such as TSA, which spoof the GPS information
Puppet attack	It focuses on the advanced metering infrastructure (AMI) network by exploiting a vulnerability in dynamic source routing (DSR) protocol and afterward exhausting the communication network bandwidth. Because of this attack, the packet delivery drops between 10% and 20%

Intercept/alter attack	It is another sort MITM attack. It endeavors to capture, change, and alter information either transmitted over the system or stored in a specific device. For instance, so as to catch private communication in advanced metering infrastructure (AMI), an attack uses electromagnetic/radio-frequency block interception attack
Active eaves-dropping attack	It is another MITM attack type, where the adversary blocks private communications between two genuine devices. These MITM attacks attempt to compromise the confidentiality, integrity and accountability.
replay attack	As the industrial control traffic is transmitted in plain text, an attacker could maliciously capture packets, inject a specific packet, and replay them to the legitimate destinations, compromising then the communication's integrity. Intelligent electronic device (IED), which is a device designed for controlling and communicating with the SCADA system, could be targeted by replay attacks so that false measurements are injected in a specific register
jamming channel attack	An adversary exploits the shared nature of the wireless network and sends a random or continuous flow of packets so as to keep the channel occupied and afterward keeps authentic devices from conveying and exchanging information.
masquerade attack	It is a malicious individual may claim to be a real client so as to access a system or gain greater privileges to perform unauthorized actions. This attack could mess with tamper with the programmable communicating thermostat (PCT) which is uses to reduce electric power at a residential site. It compromises the availability, integrity, confidentiality, and accountability of the framework
Integrity violation attacks	It mean to damage the integrity and/or the accountability of the smart grid by modifying deliberately or accidentally the data stored in a given device in the network. For example, a client could play out this attack to change the smart meter data so as to decrease his electricity bill. This attack could likewise be used to target remote terminal unit (RTU), so wrong data will be reported to the control center, resulting in an increased blackout time
False data injection (FDI) attack	It is a type of integrity violation. It means to introduce arbitrary errors and corrupt some device's measurements, affecting the accuracy of the state estimate (SE). Since the SE is significant for framework monitoring to guarantee reliable operation in the power grid, and for the energy management system (EMS) to process an ongoing information gathered by the SCADA framework, FDI attack could compromise the SE's integrity leading to the instability of the smart grid system.[12]
backdoor attack	It is an undetectable program, stealthy installed on the target to get back later easily and quickly. If the attacker succeeds in embedding a backdoor into the servers of the control center of the SCADA, he or she can launch several attacks against the system which can cause a severe impact on the power system. In IT industry, security's parameters are classified on their

	importance in the following order: confidentiality, integrity, accountability, and availability. Whereas in smart grid, they are classified: availability, integrity, accountability, and confidentiality. Thus, we can say that attacks which compromise the availability of the smart grid systems have a high severity, while those targeting confidentiality have a low severity.

11. CONCLUSION

Cyber security in the smart grid is still in its early stages of growth. The number of cyber attacks has been rapidly rising recently. Intelligent cyber terrorists with advanced power system expertise may be able to launch an assault on the network's integrity, availability, or confidentiality. It is not only the duty of engineers, researchers, and utility operators to protect the smart grid from cyber attack; it is also the responsibility of the government to ensure the protection of this national critical infrastructure. The development of an attack-resistant electric grid is crucial in order to address growing concerns about the security of the country's critical infrastructure. As cyber attacks become more common, adversaries are turning their attention to industrial control systems, such as the electric grid. Furthermore, as smart grid advancements are implemented, the grid becomes increasingly reliant on ICT for control and monitoring functions, raising the risk of a cyber attack.

We addressed various Smart Grid protection threats and challenges in this survey. We hope that these problems and concerns provide sufficient impetus for future discussions and studies on security aspects of smart grid cyber physical device security.

12. REFERENCES

[1] J. E. Dagle, "Cyber-physical system security of smart grids," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, 2012, pp. 1-2

[2] Anwar, Adnan & Mahmood, Abdun. (2014). Cyber Security of Smart Grid Infrastructure. 10.1201/b16390-9

[3] https://electrical-engineering-portal.com/conceptual-model-of-smart-grid-framework-by-iec

[4] https://www.networkedenergy.com/en/products/smart-meter-applications/grid-watch

[5] https://www.prosoft-technology.com/Products/Gateways/PLX3x/PLX32/Modbus-TCP-IP-to-IEC-60870-5-104-Gateway

[6] https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

[7] Elmrabet, Zakaria &Kaabouch, Naima & el ghazi, Hassan &Elghazi, Hamid. (2018). Cyber-Security in Smart Grid: Survey and Challenges. Computers & Electrical Engineering. 67. 10.1016/j.compeleceng.2018.01.015.

[8] https://www.enisa.europa.eu/publications/metrics-tech-report

[9] https://link.springer.com/chapter/10.1007/978-3-030-31703-4_10

[10]J. E. Dagle, "Cyber-physical system security of smart grids," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, 2012, pp.1-2

[11] R. K. Pandey and M. Misra, "Cyber security threats — Smart grid infrastructure," 2016 National Power Systems Conference (NPSC), Bhubaneswar, 2016, pp. 1-6.

[12] Shapsough, Salsabeel&Qatan, Fatma &Aburukba, Raafat&Aloul, Fadi& Ali, A.. (2015). Smart grid cyber security: Challenges and solutions. 170-175. 10.1109/ICSGCE.2015.7454291.