**CHAPTER 3**

**SECURITY CONCERNS IN SMART GRID CYBER-PHYSICAL SYSTEM**

**Dr.S.Brindha\***

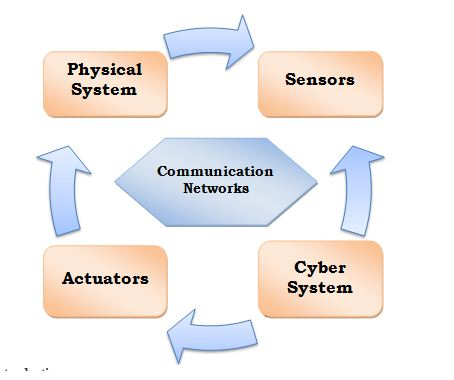
**Abstract:** A smart grid cyber physical system (SG-CPS) is an optimal fusion of power network infrastructure and cyber system through a communicating network. The SG-CPS employs advanced technologies to deliver energy supply and provide flexible choices for prosumers. The SG-CPS are using multiple components in different units and this has given rise to more complexity in managing them. The reliable operation of any smart grid is necessary to enjoy uninterrupted services. As many smart devices are being used, more cyber attacks are also targeted on smart grid cyber physical systems. The different types of attacks necessitate a broad security perspective to ensure safe services in the smart grid. The countermeasures for securing the smart grid have to be designed in all layers encompassing the cyber physical power system. If the power system is targeted then all the dependent devices will be at risk. A blackout scenario will cause more damage to industrial and household applications. Emerging technologies like Blockchain, AI , ML and IoT present a promising trend in the smart grid cyber physical system. By predicting the power demand, supply can be adjusted automatically. Many such power system related issues have smart solutions. In this chapter, we will first review the security challenges and attacks in the context of smart grid cyber-physical systems. Then the potential vulnerabilities to cyber-attack threats and risks in smart grid cyber-physical systems have been outlined. Finally, countermeasures for the security attack scenarios in SG-CPS are outlined.

**Keywords:** Smart Grid, Cyber Physical Power System, Cyber attacks

**INTRODUCTION**

In the past few years, advancements in Information and Communications technology (ICT) systems have showed the strategy for the adoption of the Cyber-Physical System (CPS) for various applications. The cyber physical system is made up of three components namely the physical parts of the system, the data and information related cyber system and the communication network for the network between the two systems. CPS is an embedded system controlled and managed by computer algorithms with communicative network components.

**\*Corresponding author Brindha S:** HoD, Department of Computer Networking, PSG Polytechnic College, Coimbatore. E-Mail: hod.dcn@psgpolytech.ac.in



**Fig.1.** Cyber physical system

The various components of CPS are providing the foundation for the emerging innovations and automated services in building tools and technologies. The world changed a lot due to the advent of the internet. As a result of the internet, the communication methodologies through which people communicate among themselves changed.  As shown in Fig.1 [Cyber physical systems](https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286) combine sensors, computing devices, actuators and communicating networks for connecting them to the Internet and to each other. CPS has the capability to reinvent things with more smart components and redesign the world with more responsive, sustainable and reliable systems.

One of the most application oriented CPS is the smart grid CPS (SG-CPS) aiming to provide power supply to modern age consumers in a better way. The smart grid is an upcoming technology which has immense potential to cater to the changing demands of the industry with respect to power consumption.. Smart Grid enables monitoring, controlling, and managing the power grid in real-time. Cyber-Physical Systems (CPS) is an upcoming technology that can tackle many challenges in smart grid systems. Smart grids are electric grid networks using monitoring tools and controlling components to deliver uninterrupted and reliable power supply. The conventional electrical machines like generators, transformers and distribution devices have been made smart by attaching the cyber components with them, Thereby managing the large physical systems have been made automatic and easier.

Smart grids (SGs) are such a boon for smart energy supply and they open the door for a modern and automated use of the electric power supply system. The stakeholders involved in the electric energy supply chain have to collaborate and establish new standards for smart grid energy supply. The main criteria for the deployment of SGs is the flawless combination and interoperability obtained from physical components belonging to conventional power grid and the latest cyber field components involving computing capabilities. This cyber physical system integrated with the power system is called as cyber physical power system (CPPS).Smart systems integration will provide accurate estimation, power demand forecasting, fault diagnosis and self-healing power to the smart grid environment. The new age producer and consumer called the prosumer will be benefited largely by adopting this cyber physical system. A sustainable and economically feasible power system would be available for the prosumers. The application of SG-CPs will be diverse in nature and based on the feedback many corrections can be initiated in the system. The security aspects of smart grid are to be carefully examined as it is very important.

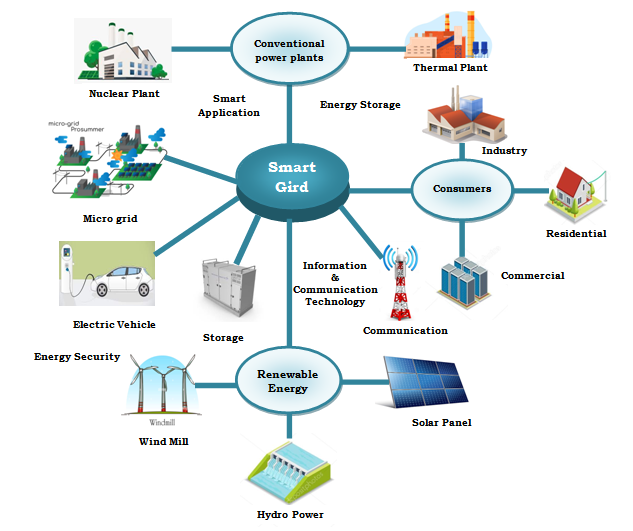
**1.SMART GRIDS**

The smart grids are more intelligent when compared to conventional power grids. Smart grids [1] are the one which use computing devices along with the power system components for better monitoring and management of the electric power supply system.It employs the sensors, actuators and control equipments in all stages of power supply like generation, transmission and distribution. By this way the prosumers are more aware of the happenings of power system network and can interact in real time.

As prescribed by the National Institute of Standards and Technology [2] the smart grid model can have seven functional units: generation, transmission, distribution, customers, service provider, operations and markets. Having mentioned the above developments, this new age can witness the transformation of a centralized power industry into a consumer interactive smart grid network. In a Smart grid [3] the activities can be monitored and feedback actions can be initiated for better performance.

In every home and industry in future we can expect a producer and a consumer i.e., prosumer [4] and the power system setup must be geared up to meet the growing demands of the people. In order to achieve this the power network must coordinate with the computing components in a flawless way.

The structure of SGs is depicted in Fig. 2, where it can be seen that there are many units interconnected to make such a large scale power system [5].Conventional power plants like nuclear and thermal power plant are on the power generation unit, renewable energy sources like wind mill, solar panels and hydro power also contribute to production of power, transmission and distribution systems are in place and consumers from industrial, residential and electric vehicles all together with the communication infrastructure form the smart grid.



**Fig.2.**Smart grid.

The smart metering infrastructure, sensors, actuators and protocols for communication are to be in synchronization to achieve sustainable and reliable power supply. The security aspects [7] of smart grid have to be viewed from the cyber security perspective as it is having new attack patterns. The cyber attacks [6] have the potential to disrupt the normal functioning of the grid. Hence countermeasures and security policies must be laid out stringently. The smart grid model must be approached holistically by computing professionals, electric engineers and security analysts to achieve a common mission of power supply in an intelligent manner.

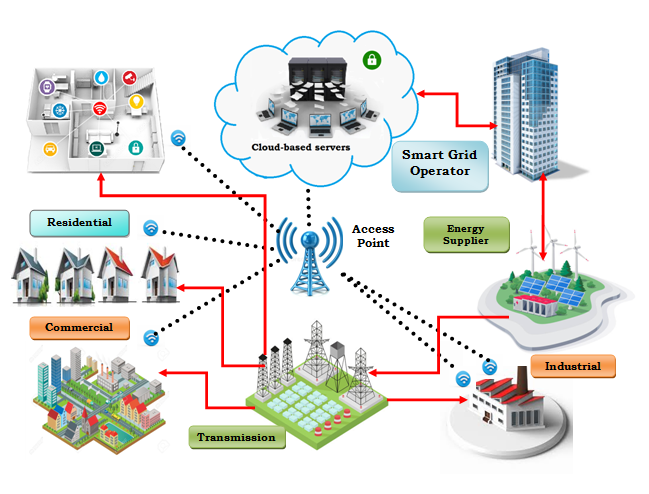
**Model for smart grid**

A huge system like the smart grid must be envisioned in a proper model so that the researchers and engineers can understand the functioning of the grid.There are two models proposed for understanding the working of smart grid.[8] One is the centralized model in which all the units of the grid are connected to a centralized cloud server. The other model is the layered model where the various units of smart grid are approached in a layered manner.

As it is seen in Fig. 3, in the centralized model the grid control is a separate unit along with the other units of the smart grid. All the units communicate to the server and corresponding actions are initiated by the server. The database server based on cloud computing and the applications in all the subunits integrate to provide a single central unit, the smart grid. Though this model [9] is easier to visualize, it is not a practical approach to have all communications from all subunits through the centralized server.

The architecture of smart grid given by NIST is shown in Fig.4.In the layered model of smart grid as shown in Fig.5, the various functions of the grid are subdivided into different layers and this enables the units to interact among themselves at various levels with varying capabilities.

Using the layered architecture, the entire power grid is visualized into several smaller layers [10]. The model starts from the components layer which involves the physical parts of the grid. The communication layer houses the protocols for transmission. The information layer places the data. The function layer [11] takes care of the functions of the grid. The business layer deals with the regulations of smart grid.



**Fig.3.** Centralized Model

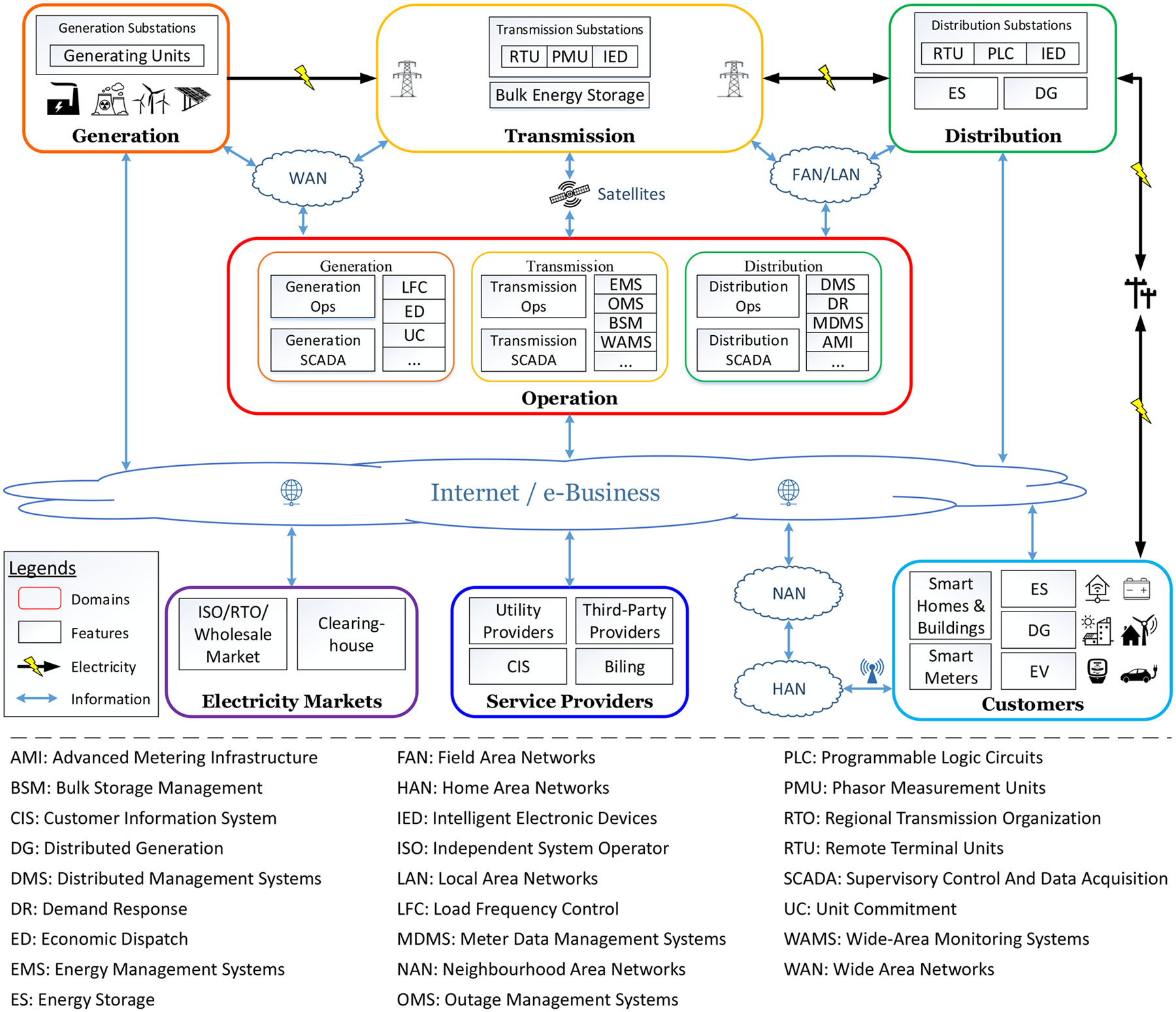
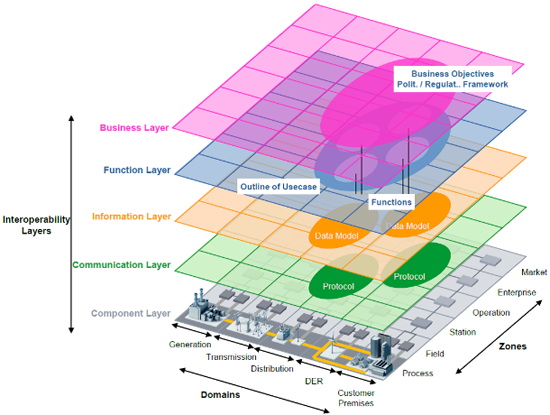


Fig.4 Architecture of smart grid



**Fig.5**  Layered model

**Characteristics of CPS with Smart Grid**

The smart grid houses both bulk generation from power plants and renewable energy generation from prosumers and hence the functionality of the grid must be characterized to meet the expectations of prosumers.Roles as many smart devices [11]are coexisting with the power system components in the smart grid

To facilitate the varying requirements of the industry, it has become mandatory to tie up Information and communication Technology with all physical systems. The smart grid interoperates with cyber physical system to satisfy the needs of prosumer. The core requirements [12] of CPS with Smart grid are listed below:

**Connectivity:**

Connectivity [13]is aimed at providing a communication channel and transmission protocols for data transfer between the power system and digital components. Connectivity comes in two perspectives: (1) Edge connectivity where the devices like sensors and actuators are connected to the computing devices through edge interface. (2) Communication channels and protocols in both wired and wireless forms for transferring data.

**Mobility:**

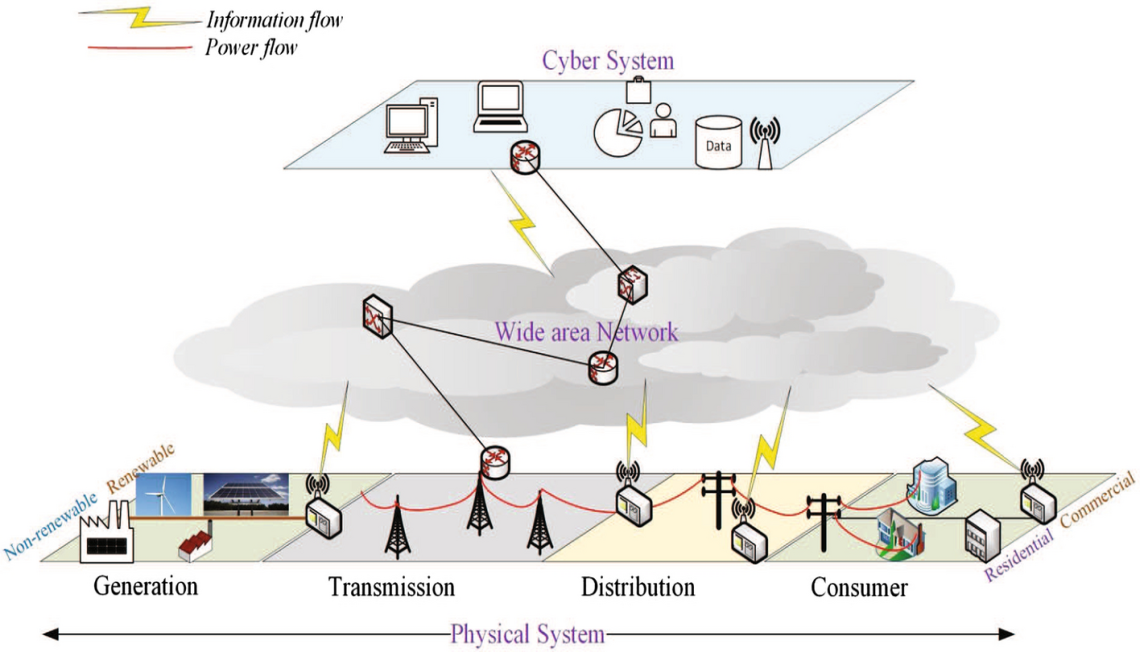
Mobility [14] is a new characteristic of the Smart Grids. Only large physical systems which are difficult to move will be stationed in a place. New devices are smaller in size and moving them is not an issue. The prosumers will definitely require the smart grid to support in terms of mobility as it has become the order of the day. The mobility of the devices will reflect changes in all layers of the smart grid and all sub units must reflect them.

**Security & Privacy:**

Security and Privacy [20] are most important in the smart grid cyber physical system.If the smart meter is compromised then the billing system is compromised and data privacy goes off. Security issues like data theft, malware injection are now directly linked with the physical power components and pose a serious threat to the security system.

**Flexibility:**

Flexibility [22] is required in the smart grid so that it is adaptable to dynamic load fluctuations together with monitoring and control of renewable energy sources in the prosumer side. The grid is no longer located within a small substation. The grid is geographically distributed and networking protocols [15] must also be flexible to support the needs of different devices. Such, characteristic cyber-physical system based SG is illustrated in Fig. [6](https://link.springer.com/article/10.1007/s11276-021-02579-1#Fig4).



**Fig. 6.**CPS based SG

**Dynamics**

* Dynamics [16] in the smart grid ensures the auto update and live connection of all the components in the grid.
* In traditional grid all the machines were mostly sciatic and any change would be predetermined. But in current scenario the various components of smart grid are updated in real time. Hence the smart grid has become dynamic in nature.
* The communication protocols and all supporting hardware and software must support this dynamic nature.

**Interoperability**

Interoperability [17] [18] focuses on providing a wide coverage with all the sub units and components of the smart grid. The information technology (IT) systems must work in synchronism with operational technology (OT) systems. The success primarily relies on maintaining the greatest synergy between IT/OT networks, building, and micro-grid/neighborhood’s necessities, flexibility, dynamics, safety, privacy, and security. The capacity of all the varied sub units to work together as a common system with transparency is the fundamental attribute of Interoperability. In order to attain this, the cyber physical components, irrespective of their heterogeneous nature, are provided standard communication protocols and interface support.

**Components of Smart Grid**

Smart Grids have two main type of networks: IT (Information Technology) and OT (Operational Technology). The OT overlay is often called the CPS network, which has a variety of CPS domains, noted below. The CPS network layers are levels 0-3[23]

* Level 0: Sensors, thermostats, meters, actuators and more.
* Level 1: Basic Controls such as HMI and PLCs
* Level 2: Supervisory-Controls like SCADA, Engineering Stations, and Operators’ interfaces
* Level 3: Operational-Controls needed for site production and operations

The devices in the OT network mostly uses IP, UDP, and Industrial Protocols for communications. The industrial protocols and field-bus used are *BACnet, LON, Zigbee, Modbus DALI, Dynet, M-Bus, Profibus, IEBus, ANSI, IEC, DLMS…*[24] [25].Some of these protocols are insecure with known vulnerabilities, and they are prone to various attacks.

Although the synchronized interoperability of the CPS/OT and IT networks make the utility smart and responsive, on the flipside, it also increases the cyber security risks and attack surfaces (including protocol attacks, routing attacks, intrusions, malware/spyware/worms, DoS, and insider threats). The North American power grid, Ukraine power grid (Black Energy), Stuxnet Malware, Irongate, Ukrenergo, Mirai, Smart-Meter hacks and US electric utility attacks are a few examples of vulnerabilities in the CPS and the interconnected network[28] [30].

**Applications of SG-CPS**

With the advent of modern technologies like IoT [31]and Artificial Intelligence [33]the world is undergoing a drastic change in which everything from homes to entire world is becoming increasingly smart. A cyber-physical system (CPS) is an intelligent system that integrates physical processes and computers employing information communication technologies (ICT). The purpose of CPSs is not simply automation or remote operation but rather an intelligent operation in real-time with sufficient autonomy so that human operators can focus on other matters.

Smart Grid applications improve grid reliability through advanced sensing capabilities, power storage devices, and distributed generation systems; they also have advanced algorithms for load management and new technologies such as power electronics devices (e.g., variable speed drives) and advanced technologies low-voltage switchgear equipment. The Smart Grid is a broad term that describes the connection of an energy system’s consumers, producers, and storage devices to an information network. The goal is to use futuristic technologies like Blockchain, Artificial Intelligence, Machine Learning, and Big data analytics to improve efficiency and reliability while reducing energy costs.

The Cyber-Physical Systems (CPS) concept provides an excellent example of how these concepts can be combined in one system. It describes how physical entities such as machines or vehicles are connected to the Internet and can interact with other commodities through this connection; however, it also includes their ability for autonomous action based on sensory input from sensors. For applications in this domain, such as smart grids, CPS can be considered a foundational technology that enables interaction between actors within a specific environment like communities or households using communication networks such as [wireless local area networks (WLANs)](https://www.ehacking.net/2017/04/netattack-tool-for-wireless-network.html).[35] This type of interaction allows them to access better services provided by cloud services from private providers but also opens up new opportunities for facilitating innovation through new business models based on open standards. In addition, CPS allows organizations operating within those environments better control over critical infrastructure components, including power plants or heating systems which could lead to improved safety measures against cyber attacks.

**Applications of Smart Grid Cyber Physical System (SG-CPS)**

The SG-CPS can be used to make the functioning of smart grid in a better way. The sole purpose of integrating the cyber system into a smart grid is to enhance its functionality. Various trending technologies are making their presence in the smart grid using the cyber system as their gateway.The applications of SG-CPS are given below:

**1. Advanced Metering Infrastructure (AMI)**

Smart meter primarily aims at bidirectional flow of information between the prosumer and the grid. Using the smart meter[36] the consumption at the customer side can be measured dynamically and intimated to them. If power generation also takes place at the customer side using solar panels or wind farms, then, it can also be measured and indicated. The various working domains of a smart meter are as below:

* Pricing based on usage time.
* Forecasting the consumption of electricity
* Outage detection
* Calculating the power pumped into the grid from consumer by solar or wind farms

By providing all the above functions the grid performs its operations better. The smart meter enables the monitoring of power consumption and helps in better usage.

**2. Demand Management**

The main idea of demand management programs is to progress the consistency of smart grid by managing the demand based on the supply demand scenario. In the purview of smart grid demand management system [39] more flexibility and adaptability has been provided. The power system management team can announce various methods to adjust the demand. If the consumers are given price benefits for utilizing power during less demand times then we can balance the demand. The pricing schemes should be based on the load fluctuations and demand needs. The price should be forecasted and informed to the customers on a preliminary basis so that they can tune their requirements.

**3. Electric Vehicles (EVs)**

The recent surge in usage of electric vehicles [42] has opened up new demand areas like charging stations all over the country. Here also the customers can save cost by charging during non peak hours and thereby the load on the smart grid can be reduced.

**4. Wide-Area Situational Awareness**

In this geographically distributed world, there is a need for tools and technologies to understand the powers system components distributed across the world. The Wide-Area Situational Awareness (WASA) [41] aims at providing the same. The entire topology of the grid would be useful for the operators to understand the overall functioning of the grid.

**5. Distributed Energy Resources and Storage**

The new generation prosumers are also producing energy at their end and hence the energy resources are distributed i.e. they are part of Distributed generation. Some examples of generation at customer side are hotels having rooftop solar system and wind generating farms [40].

**6. Distributed Grid Management**

The various components of the grid are distributed and there is need for a distributed grid management system to maintain it. This system is responsible for increasing the efficiency of the grid and manages supply demand issues in the smart grid.

**7. Energy management**

Energy can be efficiently used by allowing customers to use energy according to supply. Based on knowledge about peak usage hours and supply demand gaps, the customers can use energy in a proper manner.

**8. Smart home**

The power delivered to a home is used for various appliances. Using the SG-CPS the quality of power supplied will be enhanced and thereby smart appliances can be seamlessly developed at home. If there are unusual load fluctuations then the devices will not work properly.

**9. Self healing grid**

The self healing grid uses its cyber physical components like the sensors and communication protocols to enable real time automatic correction in the grid for any unprecedented damages that may arise in the smart grid. The unwanted events could be predicted and appropriate corrective actions would be triggered in the grid. This is possible because of the smart components involved in the smart grid.

**10. Power demand forecasting**

The operation of the grid varies due to variation in supply and demand. If Artificial Intelligence Techniques are employed in the smart grid, then the demand could be predicted. The prediction could be done for various scenarios like for an hour or a day or month. This will then enable the operators to employ suitable techniques to increase the supply.

**11. Power generation forecast of renewable energy**

As many consumers have also turned into producers by using renewable energy sources it is equally essential to forecast the power generation forecast like the power demand forecast. The accurate prediction of energy demand in cases like wind, photovoltaic energy is more desirable to make the power system efficient.

**12. Fault diagnosis and protection**

The occurrence of faults in power systems is unavoidable. But it can be diagnosed properly and re occurrence could be avoided. The isolation of a fault is the first step in taking defense mechanisms against a fault.

**14. Smart Grid Security**

The smart grid is a major point of attack for terrorists in order to disrupt the functionality of a nation. Having a vast number of components the SG-CPS is also prone to cyber attacks. Hence various applications for protecting the smart grids have to be developed and used. Intrusion detection, Malware analysis, User behaviour analysis and Information security are all needed to protect the SG-CPS.

**Security objectives in SG-CPS**

The security objectives [41]of any system is defined by the conceptual CIA triad, indicating the criteria defined by National Institute of Standards and Technology (NIST). In SG-CPS system also in order to attain the security goals of the system the following network security criteria are required.

* Confidentiality
* Integrity
* Availability
* Accountability

**Confidentiality**

Confidentiality is entitled to maintain secrecy of data. The data should be understood only the intended receiver. In order to achieve this Cryptography mechanisms are suggested. The information is disclosed only to authorized receiver. It prevents data leakage to unauthorized entities or processes. Confidentiality also ensures the privacy of data.

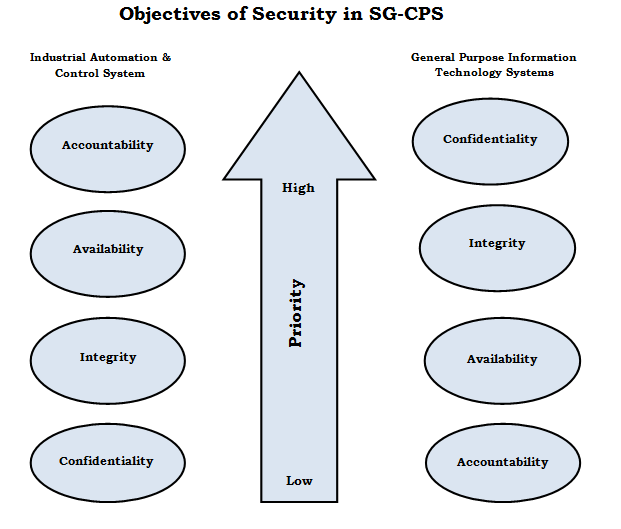
In SG-CPS system confidentiality is required in all the associated cyber and physical systems. If confidentiality could not be achieved then say for example the billing data in smart meter would be leaked and privacy of information is not preserved. The billing information could be altered and used for financial gains.

**Integrity**

Integrity focuses on ensuring that data is not modified and the data is same at both sender and receiver side. In SG-CPS system, false data injection attack (FDIA) where wrong data is fed into the system with an objective of destabilizing the state variables in the system. This could lead to malfunction of smart grid. Nonrepudiation and Authenticity of information are important network objectives to provide data integrity. Nonrepudiation aims at ensuring that an action is performed by the user and not having an opportunity to deny it later. Authentication ensures the identity of the entity and proof of authentication is obtained using knowledge, possession or biometric factors.

**Availability**

Availability is ensuring access and use of data whenever required. In SG-CPS system it is particularly important to ensure reliable access to data as otherwise loss of data will cause disruption to use data in smart grid. It can be cited for example that loss of information can block the flow of and interfere in the smooth operation of control system.



**Fig.7.**Security objectives in SG-CPS.

**Accountability**

Accountability is pivotal to ensure traceability of people, events, processes and entities in a system. It is required to deal with corrective actions in the event of attack. This cannot be denied by the entities later. In SG-CPS the accountability is required in all sub components. For example in case of an attack to a generator, the trigger would have come from the connected computing system by an unsolicited email response, It is therefore essential to maintain accountability to find out who logged on the system, at what time and what action triggered the attack.

The above four security objectives as to be used in SG-CPS are illustrated in Fig 7.The priority of the objectives change according to needs of customer and network policy decisions.

**Cyber attacks in SG-CPS**

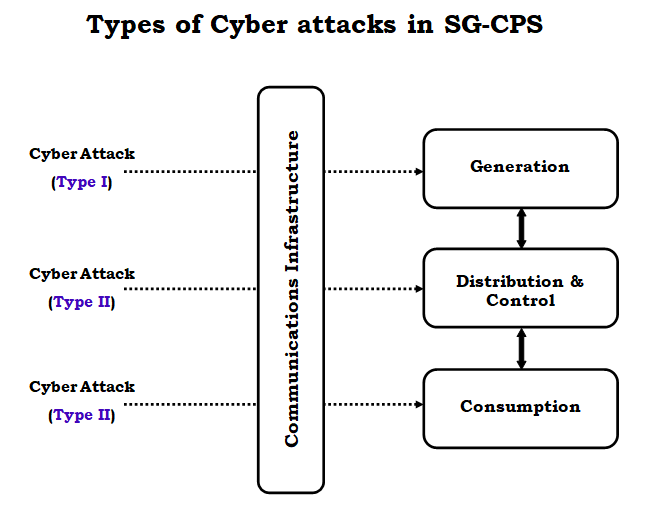
Cyber attacks are targeted on all types of systems. Hence the smart grid is no exception to cyber attacks.If the smart grid is attacked then it would affect all the stakeholders involved and power supply to entire nation could be severely affected.

As shown in Fig. 8 the cyber attacks in a smart grid can be grouped by referring the sub units in it like generation, distribution and consumption.

As many cyber threats and attacks are prevailing in the internet, the smart grid cyber physical system is also no exception to the attacks. The SG-CPs system is susceptible to both physical and cyber attacks. Although various mitigation strategies are followed, the SG-CP system is still prone to attacks. The most prominent task lying ahead is to keep up with latest developments in the field and also to develop defense mechanisms.

#### Transmission system attacks

In the smart grid the power generated is sent over long distances through transmission lines and substations. Many types of attacks are aimed at the transmission system. The various attacks and their counter measures are to be analysed.



**Fig.8** Cyber attack types

**Interdiction attacks**

It is one of the major attacks that can happen to power system. The interdiction attack mainly aims at tripping of lines or other devices like transformers, substation components in the grid. If multiples such components are disturbed then it will lead to a black out. The attack can be initiated by software commands or false measurements.

#### Complex network (CN)-based attacks

The complex network attack is based on the knowledge of topology of the network. By knowing the critical components in the network the attacker can target the attack on specific components simultaneously. The attack can be enormous based on the knowledge of the topology by the attacker. This type of attack can be reduced by changing the position of some critical components randomly.

**Substation attacks**

The substation could be damaged or compromised in the event of an attack. A well protected sub station will have necessary firewalls and routers. If an attacker could bypass them and disrupt the operation of a substation then it could lead to short term power loss or blackout. A frequent security analysis and auditing of the substation could predict the possibility of an attack and avoid major disruptions.

#### Switching attacks

The switching attack is targeted on the circuit breakers available in the transmission system. By making the circuit breakers malfunction, the operation of connected transformers or generators could be interrupted and damage to be caused. The attacker bas\*ed on his knowledge can wrongly configure the switching system and make the system enter into unstable states.

#### PMU attacks

The Phasor measurement units (PMU) [29] are connected with satellites to obtain timestamps for synchronising their data. This is a vulnerable point since spoofing type of attack can be made on PMUs since they are interacting with GPS satellites. If the time stamp data is wrong, then there can be errors induced in the system. By spoofing it means that the trusted device can be duplicated and wrong data could be fed inside the PMU.

### Smart meter attacks

The smart meters are installed on the customer end. Due to the size and other restrictions they have limited security. Hence if they are compromised it may lead to false billing, wrong data feed and thereby false alarms in a power system. If a group of smart meters are affected then the attack could be larger. This also leads to data privacy theft.

The various CP attack schemes and defense strategies in the smart grid are to be investigated carefully to have an efficient SG-CPS.

The security attack may happen due to lack of awareness of operator about malware, password attack and social engineering. Having high profile security devices like firewall, unified threat management device and security software for providing encryption are of no use if the first line of defense is properly guided.

Some of the attacks that have happened are Aurora attack, Stuxnet attack, Wanna Cry ransomware attack, etc., In the Aurora attack a test cyber attack was conducted to estimate the possibility of a software attack to penetrate and disturb the generator. The test was conducted in Idaho National Lab by altering the commands for the circuit breaker and making it fast open and close thereby causing a malfunction and a short term power outage. The impact of cyber attack was demonstrated to the world. The defense mechanisms must be developed in many layers to avoid attacks in various levels. The different security layers are shown in Fig.9.

#### Countermeasures

The cyber attacks against smart grid are increasing day by day and since multitude of components in both OT and IT systems are involved the types of attacks are also diverse. The attack scenarios in a cyber physical power system (CPPS) is due to the vulnerable entities in a CPPS. The vulnerable components are shown in Fig10.

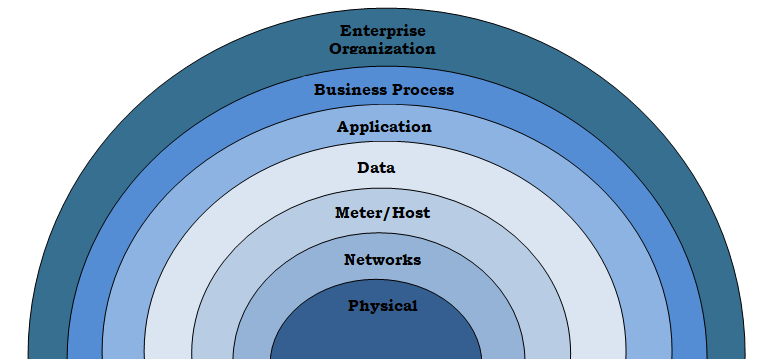
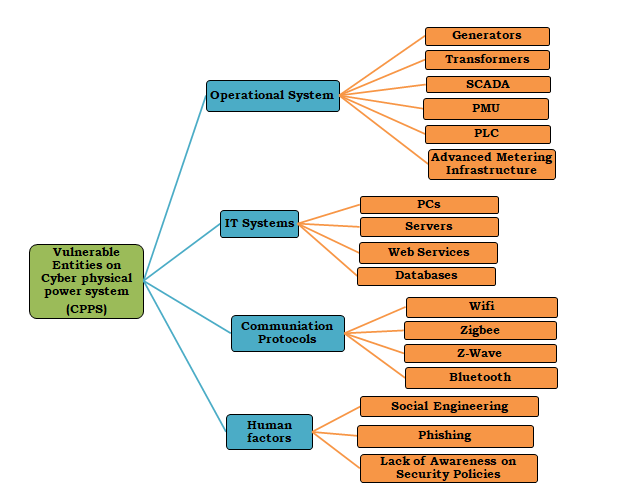


Fig.9. Layers of Security

**Fig.10.** Vulnerable entities in CPPS

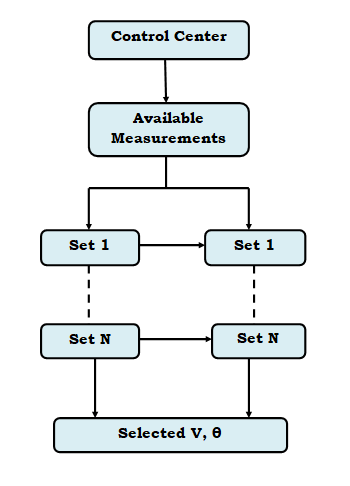
In order to keep all the above vulnerable entities protected an elaborate smart security infrastructure is required. Physical security must be the first level of defense in the smart grid. Since the number of physical components like generators, transformers, sensors, PLC, PMU are more in number; critical components must be identified and isolated to be protected. The communication protocols must be secured to add to the security layer. The users should be aware of network security oriented behavior so that they are protected against phishing, social engineering and other human factor attacks.

In the event of an attack, the operator must be trained such that he should immediately change the physical components under attack like the meters or sensors and estimate the length of the attack. If false alarms are initiated he should be able to use strategies to take alternative sets of data and initiate control actions from his side as soon as possible.

The mitigation steps taken by the operator will reduce the severity of the attack and forthcoming damages. As soon as attack is detected the counter actions must be initiated so the customers are not facing any problems. The backup devices for all critical components should be kept up to date and used immediately. In order to predict any attacks artificial intelligence based approaches can be used and necessary actions can be taken. White listing applications to be used, ensuring toned behaviour of operators, proper email and password related strategies are some of the easy to adopt proper security practices to ensure safe smart grid operation. A number of attacks could be prevented if the above said practices are ritually followed without any compromise.

##### **Counter acting attack using Moving Target Defense**

The moving target defense (MTD) is a method used to trick the attackers in real time. It involves dynamic change in the design of power system network without affecting the operation so that data integrity attacks are reduced. The control center can take any sets of data for calculation and it can be decided randomly and hence the attacker is fooled so that the attack cannot be launched as shown in Fig 11.



**Fig.11.** Simple MTD strategy.

#### Counter acting false data attack using anomaly detection

The false data injection can be identified by comparing the data feed with the normal data pattern. The pattern will be varying for an attack. The data obtained can be compared with already obtained data in a database and any attack patterns could be mitigated using anomaly detection approaches.

**Conclusion**

The smart grid is one of the prominent applications of Cyber physical systems. The specific characteristics, architecture and applications of SG-CPS were pointed out. The various types of cyber attacks and their countermeasures have been discussed. Enabling technologies like AI, ML and IoT will make the SG-CPS system more accurate and efficient.