Cyber Security for Smart Grid System

P. KRISHNA SAI ANUDEEP[1], N. SAI SURYA[2]
[1, 2] *Department of Electrical and Electronics Engineering, Sasi Institute of Technology and Engineering, Tadepalligudem*

Abstract- ***The conversion of conventional energy networks to smart grid transforms the enery industry as to accuracy, performance and willing by providing two-way communications to control, detector and controlling power-flow calculations. Hence communication networks in smart grids leads to growth and associates with increased severe security, vulnerabilities and protests. Smart grids are the major aim for cyber terrorism because of it's critical nature. Accordingly, smart grid security is previously getting many attentions from government, energy industries and utilizers. Till date, many research efforts for developing a smart grid system. This article gives an information about challenges and perspectives regarding smart grid security system, where we mostly focus on difficulties and proposed solutions. Then we contour current state of analysis and future perspectives with this term-paper, readers can get more through understanding of smart grid security system.***

Indexed Terms- ***Cyber security, smart grids, networks in smart grid, smart grid securities.***

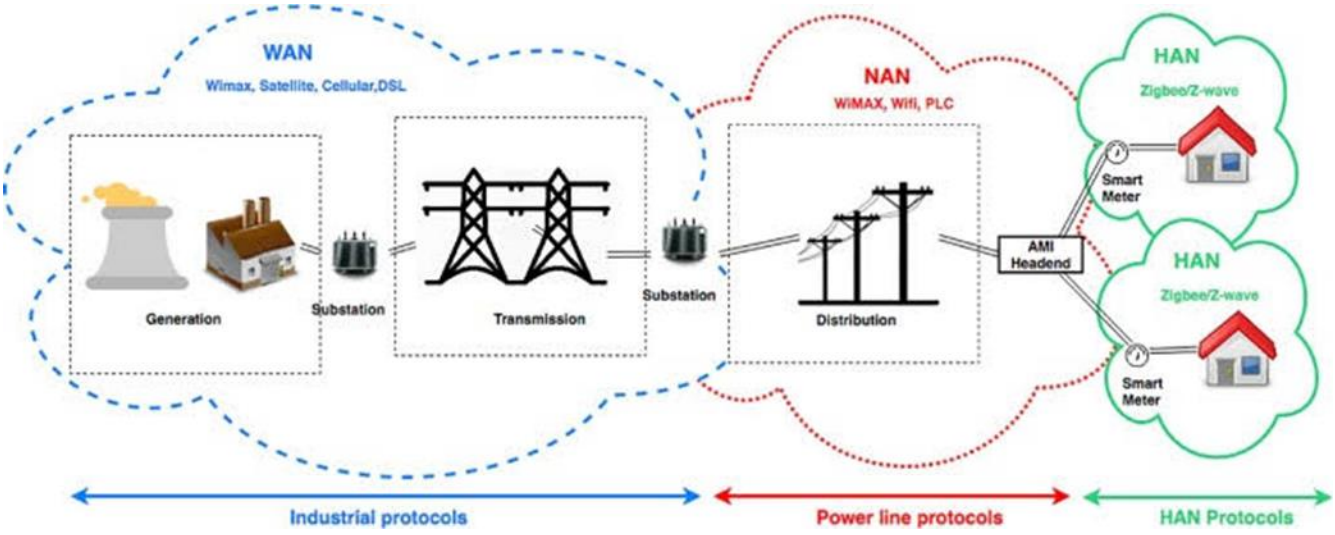
I. INTRODUCTION

The combination of electrical distribution system with communication networks configures smart grid where power and information of transmission is in two-ways.

In past years, power systems has faced so many cyber-attacks, they have created a lot of questions about the security vulnerabilities and impact on the power systems.

Mainly the smart grids contain 7 domains:

Markets, Service providers, Operations, Huge generation, Transmission, Attributions and Utilizers. Where first three domains deal by collection of data and managing of power whereas, the last four domains are related to power and continuity information in smart grids. Hence these are all links together to secure communication lines in power systems.



- Some Major Cyber Attacks on The Power Grid Are Discussed Below:

I. Southern Brazil Blackout (11th March, 1999):

Nearly 97 million people got affected, it is recorded as the world's largest power failure. "A lightning hits the tripped 440KV circuit under substation in SI O PAUL O State.

II. Central American Blackout (1st July, 2017):

Countries were stick-ed to a 6-hour power shortage, millions of people got affected.

Immediately Panama supplied the power that mid-night itself.

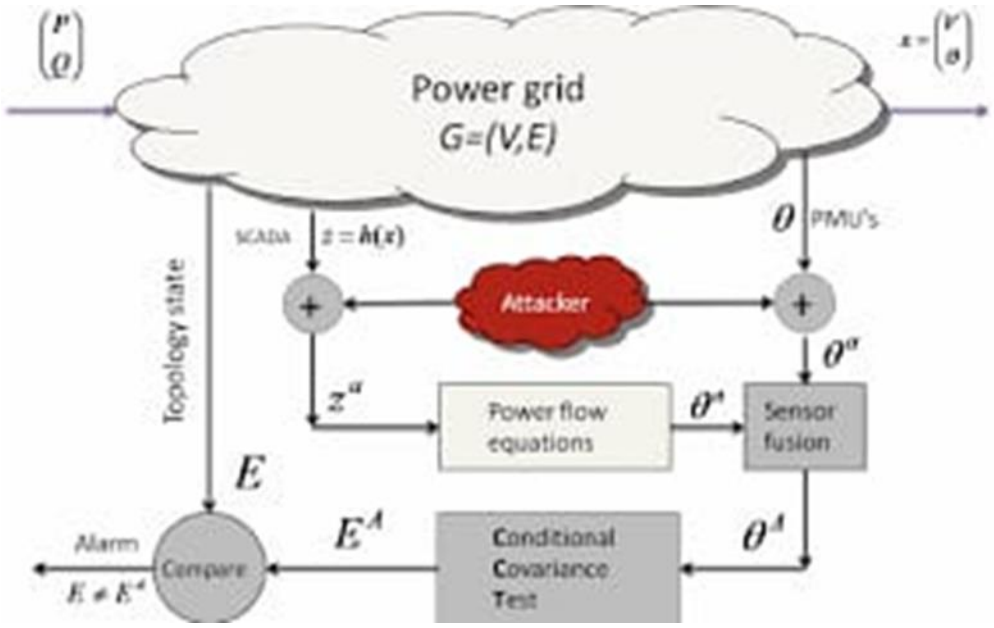
III. Pakistan Blackout (9th January,2021):

The power shortage struck almost 200 million people who were affected in Pakistan.

This fault occurred due to the frequency drop in GUDDU around 11.40 p.m.

IV. Eastern Texas blackout (10th January, 2021):

This dim-out relates to the snowfall experienced in Eastern Texas, migrated nearly 1,00,000 consumers due to no-electrical power. Hence, by observing all above attacks the cyber security got weakened in interior of the total power grid. So, we can focus on the smart grid securities by researching on cyber(software) techniques to prevent from cyber-attacks.



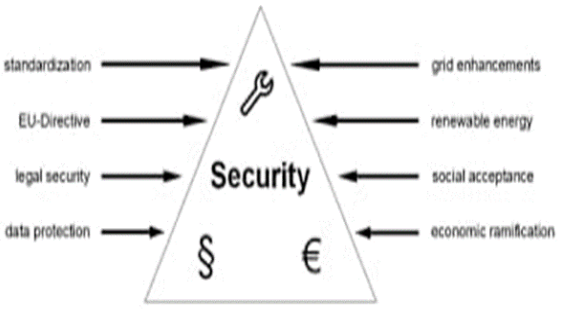
1. Cyber Security in Smart Grids:

Smart grids are the digital support which sits on top of already existing electrical grid. This mainly serves to monitor the grid conditions like consumption of energy, generations and auto manual of it's operations. And smart grid systems are made possible by bi-directional(two-way) communication technology.

Earlier there is a presence of power grids only to generate power and distributes to the end-users, flow and working occurs in uni-directional(one-way). For getting more benefits smart grids came into picture in 21st century where it is bi-directional communications as discussed earlier, by the vulnerabilities of smart grid, infrastructure etc.

So many communications networks (Ex: SCADA systems and advanced metering infrastructure) provides more stability, reliability, flexibility and efficiency to the operation of power grid systems. Even though, the huge vulnerabilities of the interior power grid cyber-attacks on smart grids. Therefore,

there is a need to identify the smart grid security issues relates to cyber security.



2. Requirements for Smart Grid Security Issues Related to Cyber Security:

- Self- healing
- Confidentiality
- Integrity
- Availability
- Accountability

The above-mentioned points preserve authorized restrictions on information access and disclosures. It also refers as ensuring timely and reliable access and use of information to the users.

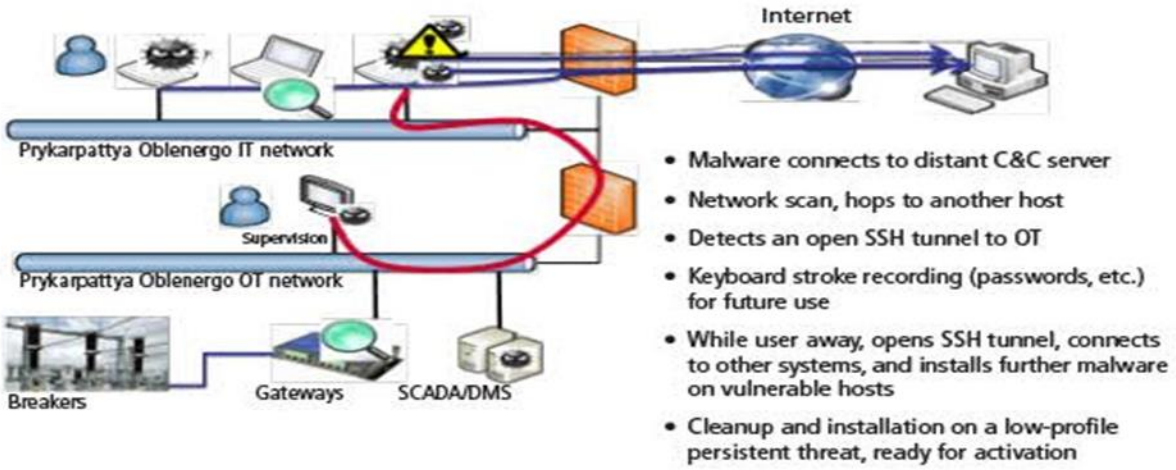
Risk=Assets*Vulnerabilities*Threats*Space.

3. Security Challenges in Smart Grid System:

- Connectivity
- Trust
- Customer's Policy
- Software vulnerabilities

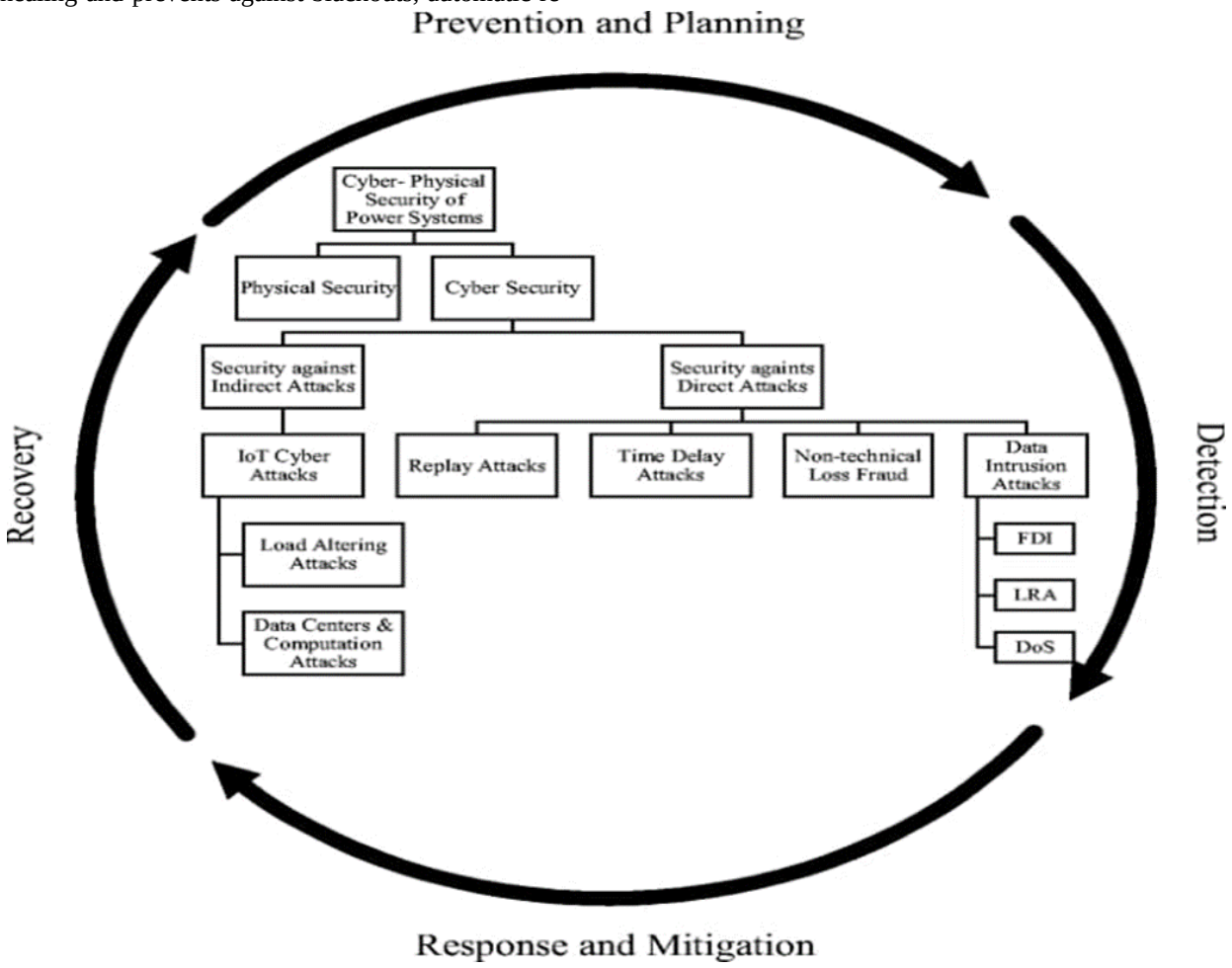
The above-mentioned points deal with the consequences of the attacks i.e., physical damage caused due to the black-outs and lack of efficiency. Some customers will not adhere to the terms and conditions, agreements. Ensuring consumers privacy and electrical needs is important aspect in any system including smart grid.

Software suffers by a wide variety of vulnerabilities that includes malwares. Most frequently, all the cyber-attacks are occuring due to the vulnerabilities of physical securities of smart grids. Power systems cyber-physical resilience centers around the system's ability to recognize, adapt and to absorb disturbances in timely manner. Resilient system operation focuses on monitoring the system limitations to detect disturbances and adjusting control actions respectively.



4. Prevention of Blackouts in Power Grid Systems:

Modern power systems should be capable for self-healing and prevents against blackouts, automatic re-closing of transmission lines and component reintegration. After power system blackout, the power system should be restored automatically and quickly.

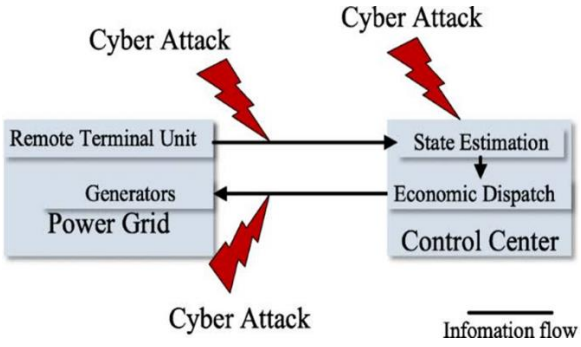


5. Perspectives of Cyber-Attacks in A Smart Grid:

- Cyber-attacks target a resource (physical or logical) has one or more vulnerabilities that can exploit by cyber criminals that results in an attack. Confidentiality, integrity and availability of the resource maybe compromised.
- In some cyber-attacks, the damage, data exposure or control of resources extend beyond the one initially identifies as vulnerable including gaining access to an organization's Wi-Fi networks, social media, operating systems (OS) or sensitive information like credit card numbers, hacking cyber-security of a smart grid etc.
- Passive cyber-attacks lead to confidentiality.
- Active cyber-attacks lead to integrity and availability.

6. Challenges for Security Smart Grids from Cyber-Attacks:

- Lots of care to be maintained while designing a sub-station and power grid systems.
- Must be needed to design all the sub-stations or smart grids in different methods and integrating them.
- Activation of GRPS, sensor connectivity to the smart grids.
- Hence these are all about how well you play with the data from all the smart devices makes the grid smarter.
- Mainly, electrical infrastructure at distribution level doesn't support for complete automation of the grid. We focus on introducing RMVs (Ring main unit) modern technologies.



7. Security Issues of Cyber-Physical Smart Grid:

In smart grids, the infrastructure power system and cyber system of information and communication technologies are highly attached with cyber-securities. Smart grid security issues need to address a reliable, safe, efficient and a stable working grid.

A smart grid handles as the combination of power system apparatus and cyber system infrastructure includes software, hardware and communication requirements. Smart grids help to generate bulk amounts of power flow from plant to the end-users (Consumers). Where information flow occurs in both directions i.e., among the operators and service provider level and device level for coordination to accomplish more efficient and advanced operations.

Therefore, in a smart grid both cyber infrastructure system securities are more essential.

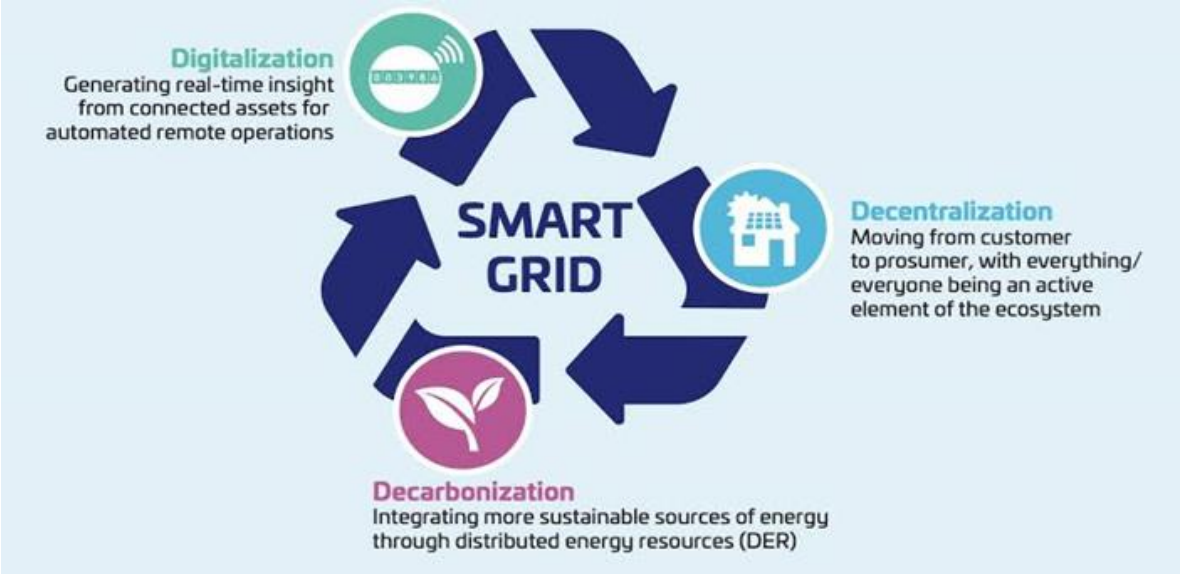
Benefits of FACT Solutions:

- Parallel Compensation:

1. Hybrid SVC (Addition of both SVC And STATCOM)
2. SVC (Static Var Compensation)
3. MSC/MSR (Mechanically Switched Capacitor/Reactor)
4. Synchronous Condenser

- Series Compensation:

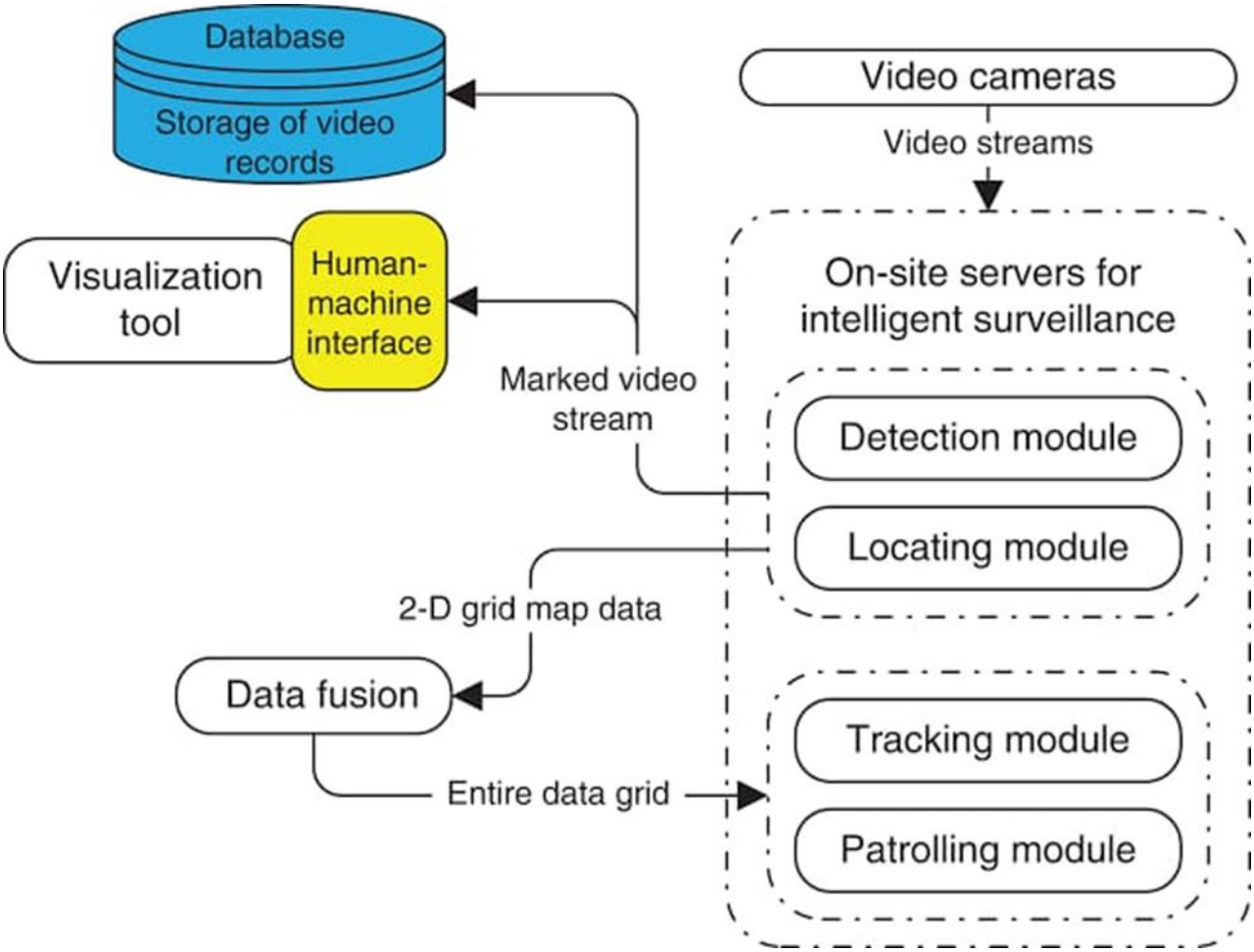
1. FSC (Fixed series Capacitors)
2. TCSC
3. TPSC



Risks Associated with Cyber-Physical Smart Grid:

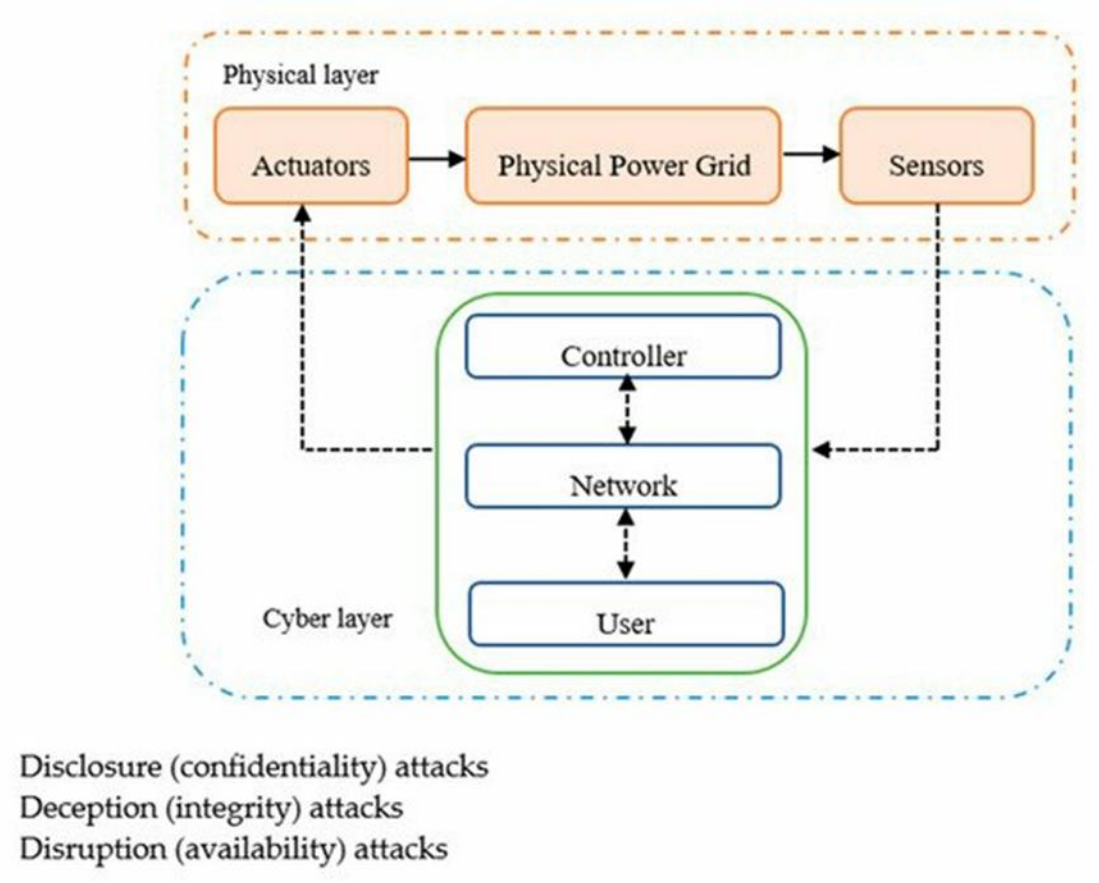
1. Complexity: Implementation of new techniques in the smart grids increasing of complexities.
2. Cascade Failures: In a smart grid, the cyber systems and physical grid systems are coupled together. Therefore, failure due to random attacks, cyber-attacks or any targeting attacks leads risks.
3. Security and Privacy Issues: Securing the information and power is little difficult and increasing of electronic devices leads to gathering of data in two-way information flow that extensively introduces the problems related to data confidentiality and intrusions of customer's privacy.

In the way of making power grid more effective, automatic, controls lead the risk of increasing cyber-attacks. Specially controlling domain is major target for cyber terrorists. Thus, by introducing new technologies like PLC SCADA systems, advanced metering infrastructure, FACTS devices.



We can secure smart grids and power grids from cyber-attacks mainly the power providers (at generation station) are also adopting different risks and technologies against cyber-attacks. Securing smart grids is more essential because they provide lots of benefits like:

1. Better demand supply.
2. Reduce carbon emissions.
3. Good power quality.
4. Shortage of power occurs (i.e., in emergency situations) smart grids helps for continuity.
5. Smart grids reduce cost more effectively.



Therefore, by transforming a power grid into a smart grid by using the combination of information technology, communication technology and electrical systems one can achieve a reliable, efficient and continuous power supply to the end-users (consumers).

REFERENCES

[1] proceeding of the IEEE southeastCon 2015, April 9 - 12, 2015-Fort Lauderdale, Florida

[2] A. Anwar, A. Mahmood, "cyber security of smart grid infrastructure", The state of the Art in intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, January 2014, pp. 449-472

[3] Times of India