Prevent another "Operation Olympic Games"
&
Save the world from "Son of Stuxnet"

- Deepto Ghanti

National Institute of Technology Durgapur, West Bengal, India

***Abstract*:** Increasing volatilities within power transmission and distribution force power grid operators to amplify their use of communication infrastructure to monitor and control their grid. The resulting increase in communication creates a larger attack surface for malicious actors. Indeed, cyber-attacks on power grids have already succeeded in causing temporary, large-scale blackouts in the recent past. In this paper, we analyze the communication infrastructure of power grids to derive resulting fundamental challenges of power grids with respect to cybersecurity. Based on these challenges, we identify a broad set of resulting attack vectors and attack scenarios that threaten the security of power grids. This paper reviews research that demonstrates cyber security risks and constructs solutions to enhance the security of a power grid. To achieve this goal, this paper covers: (1)Methodology and Assumptions, (2) Cyber Deterrence Challenges (3) Legal and Treaty Assumptions (4) Solution Architecture, (5) Prototypes and (6) Benchmark for Success.

Keywords: critical infrastructure; cyber-physical security; cybersecurity; power grid; power system communication; ICT; WANs; SCADA

Recommended Citations:-

i) Rajendra Kumar Pandey, Mohit Misra, "Cyber Security Threats - Smart Grid Infrastructure" , https://www.iitk.ac.in/npsc/Papers/NPSC2016/1570293178.pdf

ii) Chih-Che Sun, Adam Hahn , Chen-Ching Liu, "Cyber Security of a Power Grid: State-of-the-Art" https://www.sciencedirect.com/science/article/abs/pii/S0142061517328946

• Introduction: *What is Stuxnet?*

In 2010, computer programmers around the world noticed a strange kind of cyber attack—although it had global reach, it was highly targeted and very sophisticated. A German team, led by Ralph Langner, figured out that the worm, now known as Stuxnet, specifically targeted certain operations related to the Natanz nuclear facility in Iran, causing the enrichment centrifuges to break down without any notice or apparent reason. Like other computer worms, Stuxnet spread indiscriminately from one vulnerable computer to the next. [1]

What set Stuxnet apart from the thousands of other worms that went before it is that it was designed to unleash its payload only when it entered an industrial control system (ICS) matching the characteristics of Iran's nuclear enrichment facility at Natanz. And when it did, it tampered with the code of the programmable logic controller (PLC) used to control the centrifuges at Natanz, ultimately destroying about a thousand centrifuges and disrupting Iran's nuclear program. No previously reported worm had done anything like that before, either in terms of precision targeting or causing physical damage through ICS manipulation. Is Stuxnet a forefather of future cyber-weapons? [2]

Specifically, multiple pieces of malware can be built from the same coding framework and be used for very different purposes. This allows the attack team to quickly update their malware, adapt it for unique targets, and use different pieces of malware together in either direct or indirect support of each other. By using different modules of code the malware creators could modify, remove, or add modules to make entirely different pieces of malware. In the following years, the cyber world saw the rise of many other malwares like Duqu, Flame and Conficker whose origins were traced back to Stuxnet as they shared the same coding frameworks. [3]

Inevitably we will soon see a rash of attacks against ICS components and devices, which include Supervisory Control and Data Acquisition (SCADA) systems, as well as PLCs. These crtitical systems are used, for instance, to operate electric power grids, distribute oil and gas, and control water treatment systems and dams. Are they adequately protected against cyber-attacks? Will we witness cyber-attacks that go beyond the usual data theft and service disruption in order to cause serious physical damage against specific targets? Will cyber-terrorists use Stuxnet-like tools to cause nuclear explosions, shut down power grids, blow up gas lines, cause floods, or otherwise wreak havoc?

- **Methodology and Assumptions: Smart Power Grid**

  - *Why are Smart Power Grids considered as critical infrastructure?*

    Smart grids are an evolving new power system framework with ICT driven power equipment massively layered structure. With the support of information and communications technology (ICT), power system operators can perform operation and control tasks based on data acquired from remote facilities. [4] For example, the advanced automation system isolates a faulted segment by opening switching devices (e.g., circuit breakers and automated reclosers), and sends the fault information back to the control center. However, the upcoming deployment of smart devices at different layers followed by their integration with communication networks may introduce cyber threats. The interdependencies of various subsystems functioning in the smart grid, if affected by cyber-attack, may be vulnerable and greatly reduce efficiency and reliability due to any one of the device not responding in real time frame.[4]

    According to FERC analysis, the loss of 9 out of 55k+ US substations could lead to an extended (1+year) national blackout. [5] In India, on July 29,2012 circuit breakers on the 400 kV Bina-Gwalior line tripped, causing cascading power failures through the Agra-Bareilly transmission grid, resulting in two large-scale national blackouts affecting over 700 million people in 21 out of 28 Indian states and causing an estimated shortage of 32 GW. Officials described the failure as "*the worst in a decade*". Just due to the sheer amount of havoc that can be wrecked by the malfunction of a single substation and its cascading effects , *cyber security of smart grids has been recognized as a critical issue*.[6]

  - *Cyber Security Objectives and Requirements: -*

    This section deals with cyber security objectives and requirements in a smart grid cyber infrastructure. The National Institute of Standards and Technology (NIST) report explains three high-level cyber security objectives namely: availability, integrity and confidentiality. Apart from such high-level security objectives for the smart grid, the NIST report also addresses specific security requirements like identification, authentication, authorization, trust, access control and privacy. [7]

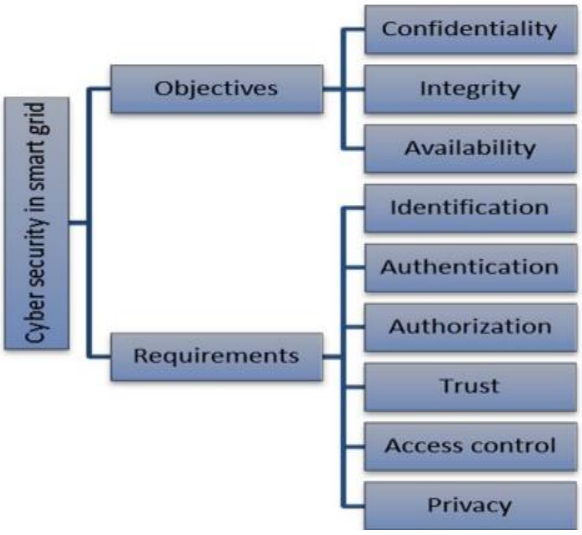

Fig:-1 Confidentiality, Integrity, and Availability (CIA) are the core principles of information security (CIA triad)
Image Source:- [8]

- *Cyber Security Threats in a Smart Grid:-*

A. Risk Inspection and Attenuation:-

Risk is the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences. Simply risk may be defined as the union of likelihood of an attack, possible actions that an adversary may pursue and its consequent outcomes. [9]

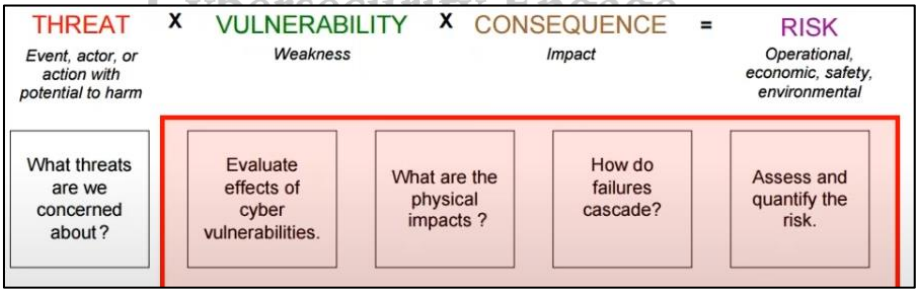

Fig.2. (Threat/Likelihood of Attack) × (Vulnerability/Possible Actions) ×(Consequent Outcomes/Impact)=Risk
Image Source: - https://youtu.be/PZFLVEoVf_4?t=406

	Scope	Difficulty	Impact
Lateral Movement	Single Operator	High	High
Physical Access	Local	Medium	Medium
Remote Maintenance Access	Multiple Operators	High	High
Third-Party Exploit	Multiple Operators	High	Medium
Overcoming Air Gap	Local	High	Medium
Insider Attack	Single Operator	Low	High
Cascading Effects	Multiple Operators	High	High

Table 1. Classification of attack vectors specific for the energy sector.
Table Source: - https://www.researchgate.net/publication/236120151_Smart_grid_cyber_security_requirements

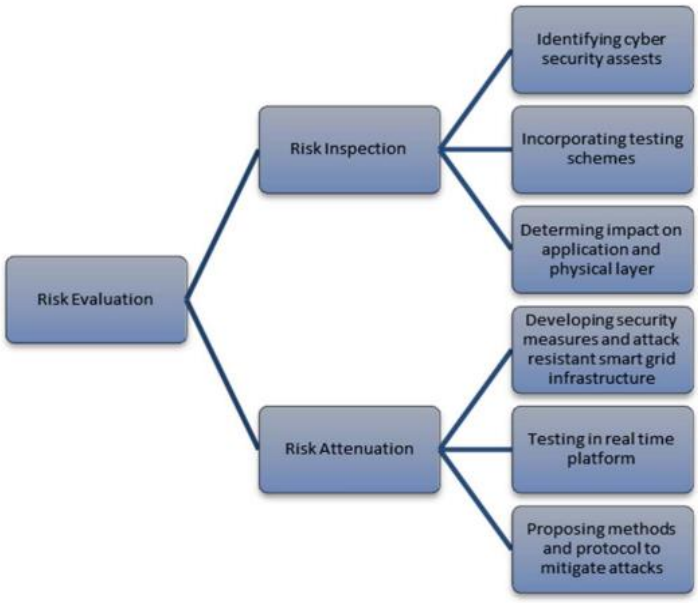

Fig. 3. Risk evaluation process
Image Source: - [8]

B. Probable Attack Points and Adversary Action:-

Attackers can leverage different attack vectors to compromise the network of a transmission or distribution system operator with the goal of causing a blackout or at least considerable disturbance in the power grid. To achieve this goal, an attacker will likely aim to compromise the PCN of the target system. From there, the attacker can compromise substations or field devices, potentially leading to a blackout. In the following, we discuss the most important attack vectors an attacker can exploit to access a PCN. We provide a summary of our classification of attack vectors in Table 1. [10]

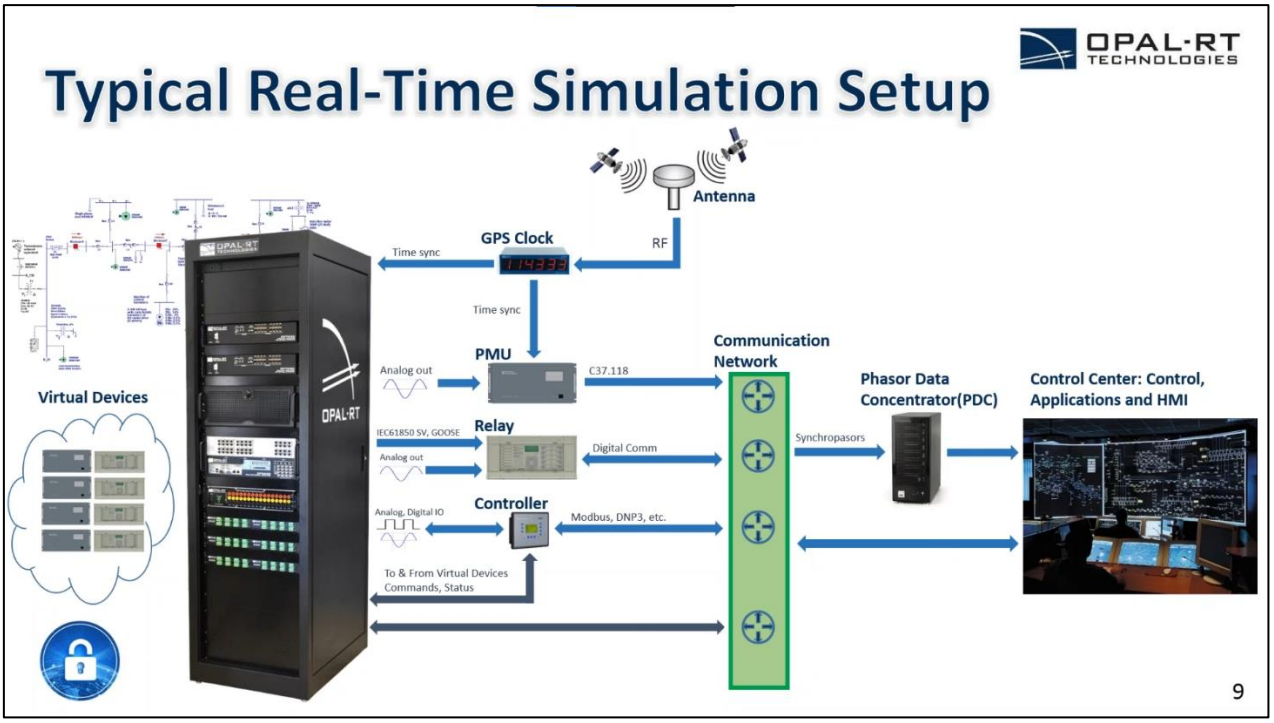

Fig. 3. Typical Real-Time Simulation Setup
Img Source:- https://youtu.be/PZFLVEoVf_4?t=721

The various attack points in power industry chain are listed below:

i) Generation System: An adversary may launch a DoS attack on the Ethernet based IEC 61850 infrastructure causing the relay to mal operate during the fault conditions. Various local control loops including that of speed control, valve control and AVR are linked with plant control center through Ethernet. If an adversary manages to find security holes then it can easily gain access inside the local area network (LAN) and plant a Trojan or get a backdoor entry hence enabling the adversary to compromise the digital control modules by disrupting the control logic. The generation plants are monitored and controlled by the SCADA system. An adversary may easily invade the SCADA system to change frequency measurements provided to the automatic governor control (AGC). RTUs and PLCs in power plants generally use MODBUS or DNP3 protocols for communication purpose. Neither does the MODBUS protocol provide security against unauthorized entry not does the DNP3 protocol employ encryption, authentication and authorization.

Jin *et al.* [10] have shown that "buffer flooding" attack can be easily done on a DNP3 based SCADA network. It is also possible to create "man-in-themiddle" attack [11] between the SCADA and the slave devices (RTUs or PLCs) to get information regarding the network topology and device functionality.

ii) Transmission System: RTUs (Remote Terminal Unit) and PLCs (Programmable Logic Controller) also have the same vulnerabilities in the transmission system as was in case of generation system. An adversary can specially craft an URL that can be sent to anyone at the control center. As the URL is opened from the HMI (Human Machine Interface) connected to the network, a malicious JavaScript snippet is executed in the web browser [12]. State estimation, optimal power flow computation, economic dispatch and unit commitment studies are done by algorithms embedded in software specifically designed to perform computations using thousands of measurements. If an adversary manages to penetrate inside the network and falsely inject "bad data" or "redistribute load" then the system will immediately shift towards unstable operating conditions and impact the smart grid economically as well. Furthermore adversary can send control signals to change the commutation angle of HVDC power lines or may even block the power flow causing severe loss of power at the targeted area. Modern FACTS devices uses high speed communication link to exchange information with each other during operation–hence increasing the vulnerabilities in the system. Manipulation of wind and solar forecast data sent to the control center can make the power system run haywire affecting system operations such as generation scheduling, dispatch, real time balancing and reserve requirements. Hackers might even go a step forward and reconfigure the entire energy gain and program the wind turbine to reverse its direction. Doing so, would not just harm the system operation, but also damage the wind farms.

iii) Distribution System: A conventional meter can be modified by reversing the internal usage counter or can be manipulated to control the calculation of electric flow. [13] Intelligent Electronic Devices (IED) like smart meters can be controlled to deploy various functionalities from remote location. This enables an adversary to remotely connect or disconnect the devices or tamper with data sent to the system operator or sneak into confidential data of the consumers. Also, if an adversary manages to send false data packets to inject negative pricing in the system then it will result in power shortages at the targeted area causing loss of revenue to the utility company. Networking and communication within the AMI infrastructure will rely on technologies like WLAN, ZigBee, RF mesh, WiMax, WiFi

and PLC. Wireless Local Area Networks (WLANs) follow IEEE 802.11 standards which by default do not provide authorization mechanisms. This protocol is also vulnerable to traffic analysis [14], eavesdropping and session hijacking attacks. ZigBee is based on IEEE 802.15.4 standards which are vulnerable to jamming attacks. [15] An adversary can hijack the Virtual Private Network (VPN) of distribution utilities. The effects of slammer worms migrating through a VPN connection to SCADA network are reported in [16]. The worm manages to infect the control center LAN and blocked the SCADA traffic. Due to lack of authentication and encryption at the Head End System (HES), an attacker can directly tamper the Meter Data Management System (MDMS) and send unauthorized trip signals to the smart meters. Also, an adversary can masquerade smart meters connected at consumers' end and send fake energy usage signals to the control center. Since the software installed at HES cannot spot the ambiguity, it executes the required control and sends command to turn off the smart meter. [17]

iv) Telemetry Infrastructure: Telemetry systems connect with control systems and SCADA architecture of various components in smart grid - generation systems, transmission systems, distribution systems and micro grids. Power system telemetry uses standard communication protocols like Modbus, IEC 870-5-10x, DNP3 and Profibus/Profinet. Irrespective of the type of protocol used, most ICS (Industrial Control System) protocols work on "master/slave" model having little or no security features and thus are susceptible to malicious network attacks. If an adversary gains access inside the "master" then the "slave devices" can then be forced to spuriously operate or even erase critical data.

However, there are certain ways in which system can be infiltrated by physical means. A disgruntled employee who has privilege to access the system components might alter the algorithms of software or may even change the settings of devices causing spurious operation (Insider risks). Devices such as laptops and USB memory sticks that are used both inside and outside the trusted perimeter can get infected with malware outside, and then invade the system when used inside. [18]

- **Cyber Deterrence Challenges**

The concept of deterrence was originally developed during the rise of nuclear technology. It relies on second-strike capabilities of opponents and complete certainty of who the opponent is, that it can survive the first strike and that it can strike back. This is known as mutually assured destruction (MAD).

Top Challenges to Cyber Deterrence:-

- *Inherent difficulty of assigning attribution*

i) Misattribution: Because of the inherent architecture of the internet and threat actors' ability to obfuscate the source of an attack, it is nearly impossible to attribute attacks with a high degree of certainty. This results in a cyber attribution dilemma whereby the need to impose the costs necessary for cyber deterrence is juxtaposed with the potential costs of misattribution. The current deterrence paradigm of mutually assured disruption — the equivalent of MAD in the cyber arena — has a high risk of escalating into a tit-for-tat exchange as a result of a false accusation.

ii) False flags: Adversaries have historically used false flag operations to make an operation appear as though it was perpetrated by someone else. Because of the cyber attribution dilemma, false flags are much easier to execute in cyberspace, where the challenge of attribution already exists.

False flags in cyberspace exploit this existing uncertainty and further compound doubt by casting suspicion on other actors.

iii) Plausible Deniability:- The attribution dilemma also gives threat actors the benefit of plausible deniability, further reducing the risks and costs associated with cyber actions. If we can't be certain who is responsible, once again, we can't impose costs without risking imposing the costs on the wrong actor.[19]

- *Unpredictability of the effects of cyber attacks*

With hindsight, many cyber incidents seem predictable, even preventable. Yet compared with risks like natural catastrophes or fire, which are well understood and can be modelled using historical loss data, cyber risk is particularly tricky to pin-down. When, where and how a cyber event will unfold is very difficult to predict. Even where likely scenarios can be identified, the likely impact and potential financial loss can be hard to anticipate and calculate. [20]

Zero-day vulnerabilities are one such kind of challenges. Because they were discovered before security researchers and software developers became aware of them—and before they can issue a patch—zero-day vulnerabilities pose a higher risk to users. Zero-day vulnerabilities are typically involved in targeted attack.

- *The potential for damage due to counter-retaliation*

If the potential aggressor is powerful, it could counter-retaliate, perhaps even in an escalatory manner. In evaluating the credibility of an Indian reprisal threat, the aggressor could ask itself whether India would still retaliate even in the face of a possible counter-retaliation. If confident that a counter-retaliation would make a difference, an aggressor is likely to present as daunting—that is, painful and credible—a counter-threat as possible.

Deterrence by punishment must satisfy at least two criteria. On the one hand, the threatened punishment must be sufficiently painful that potential attackers believe they will be worse off after punishment has been delivered even after factoring in the benefit from the bad act. On the other hand, the threat of punishment must be credible; having the requisite capability means nothing if the other side thinks it will not be used. [21]

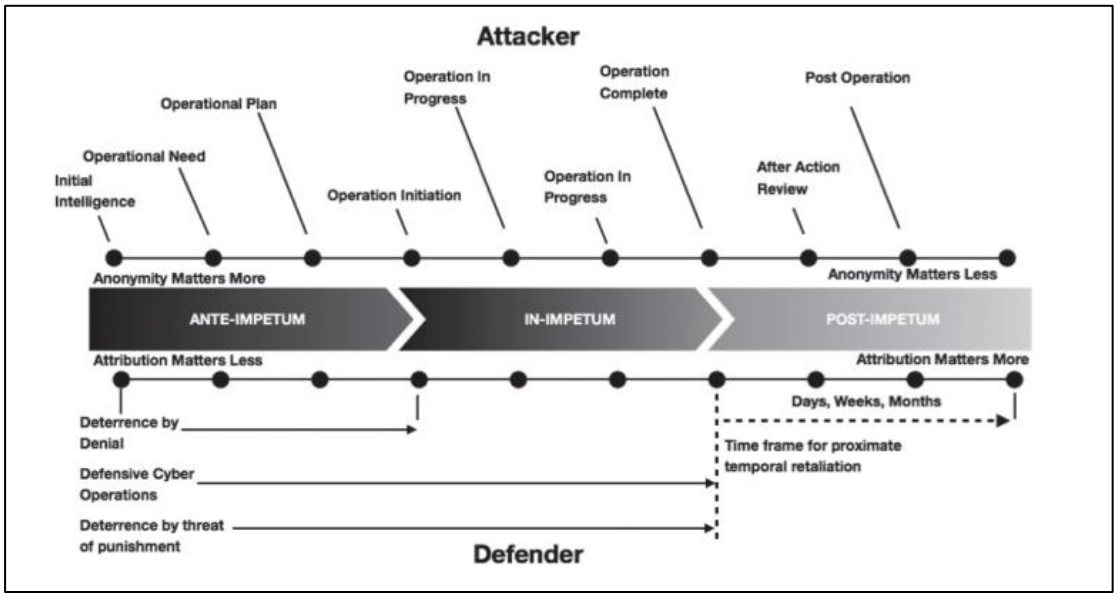

Fig. 4. Stages of Cyber Deterrence

- **Legal and Treaty Assumptions: -**

The Cybersecurity Legal Framework comprises of:-

i) Corporate duties of Loyalty and Care, to Disclose, to Monitor and Challenges to corporate governance.
ii) Statutes and Regulations, Common Law, Contractual Obligations, Self-Imposed Obligations and Constitutional Provisions. [22]
iii) Understanding the adversary and how it will react to a given deterrence strategy.
    a. Cyber-criminal activity is the largest group of cyber threats and one of the most difficult to effectively deter. Our ability to punish and deter this group is sometimes limited and largely dependent on law enforcement, extradition treaties signed and effective cooperation from foreign nations (friendly, hostile or neutral).
    b. The next adversary group is violent nonstate-sponsored organizations such as terrorist groups. These groups may be more organized and have a clear goal to inflict harm against India or its key interests. Again, our ability to deter this group from attacking our networks is currently low.
    c. Unlike criminal hackers or nonstate-sponsored adversaries, state-sponsored groups can be effectively deterred. The difference between this group and the others is our ability to inflict an appropriate level of punishment on a nation-state to deter unfavourable behaviour guided by that state. The threat of economic sanctions, military action, or other political/diplomatic responses by India could markedly affect certain states. [23]

- **Solution Architecture : -**

Many industry and government reports have identified that cyber intruders have become a serious threat to the secure operation of a smart grid. To identify and eliminate cyber vulnerabilities in a smart grid, methods to detect cyber intrusions and mitigate their impact need to be developed.

A. Vulnerabilities and Risk Mitigation in Cyber Infrastructures

To prevent unauthorized access to a private network, firewalls are installed behind an access point (e.g., router and gateway) in order to filter incoming network traffic as a front line defense. Using the properties of packets, such as time delay, source/destination IP address and port numbers, firewalls are capable of inspecting and discarding suspicious packets. However, the performance of firewalls relies on a pre-defined rule set. Since a commercial grade firewall has hundreds of configurable rules [24], which can often conflict in many cases [25]. Furthermore, developing accurate firewall rules requires that the utility have perfect knowledge of all cyber assets in their network and all authorized communications. In addition, firewalls have other limitations as they cannot protect against spoofed messages which may bypass their filter rules, and they may also contain software vulnerabilities that may allow an attacker to bypass their protection. Network packets travelling in a WAN may not be protected by firewalls as there is often a concern that the devices may introduce excessive communication latency. To ensure confidentiality and integrity of the grid data, cryptographic protection mechanisms of communication protocols are critical. Many communication protocols and devices like MODBUS and Distributed Network Protocol 3.0 (DNP3) used in SCADA, SAS, PMU and DER systems [26], [27] were developed before cyber security becomes a serious concern and do not implement strong cryptographic protection and hence may not be well protected against cyber attacks [28]. Moreover, DNP3 is used in WAN communication that increases security risks as WAN is accessible to many users. To secure communication protocols, MODBUS authentication frameworks have been proposed [29], [30]. A lightweight security authentication scheme [31], [32] and a secured frame format are proposed for DNP3 [33].

B. Vulnerability Assessment in a Smart Grid and Defense mechanisms

It is necessary to study the interactions between the cyber system and physical system in a cyber attack event. As a core component in control systems, SCADA is a primary target for attackers. SCADA integrates smart grid subsystems (e.g., AMI, DER, and DA) in a distribution system. Cyber attacks become damaging once intruders gain access to the SCADA network. Reference [34] provides an assessment framework to evaluate the vulnerabilities of SCADA systems.

Power system operators rely on SCADA and SAS to perform operations via communications between a control center and remote sites. An IEC 61850 based substation automation system contains various IEDs. Reference [35] indicates that multicast messages defined in IEC 61850 (e.g., GOOSE and SV) do not include cyber and information security features. They are vulnerable to spoofing, replay, and packet modification, injection and generation attacks. Although IEC 62351 proposes comprehensive security measures (e.g., authentication) to secure IEC 61850 based communication protocols, the weaknesses still exist by analyzing the specifications of both IEC standards [36]. An attack example is demonstrated in [37] in which attackers are able to modify the GOOSE packets to trip circuit breakers. In a massive attack event, attackers can trigger a sequence of cascading events by compromising critical substations, causing a catastrophic outage. A high level penetration of smart meters brings advantages to distribution system operation.

C. Vulnerability Assessment in Distribution Systems

However, smart meters don't come with all good, they too have downsides. Smart meters also bring cyber security concerns, e.g., privacy, smart meter data modification attacks, unauthorized remote load control, and interoperability problem. Note that intruder(s) may access the AMI network from various nodes in a public area, such as smart meters and local data collectors. These problems indicate that a single layer of cyber security protection cannot provide a higher level of cyber security. Several cyber attacks targeting the AMI have been identified, including energy theft, false data injection, and leakage of the customer information [38-41].

To ensure system reliability, [42] proposes baseline requirements and suggests implementation guidelines for data delivery systems in power grids.

Table 1. Major standards for operating a smart grid.

Subsystem Name	Standard Name	Applied System
SCADA	IEC 60870-6	Monitoring and control over a WAN.
PMU	IEEE C37.118	Phasor data exchange.
Substation	IEEE 61850	Substation communication networks and systems.
	IEEE C37.1	Definition, specification, and application for monitoring and control function.
	IEEE 1379	Communication and interoperation of IEDs and RTUs.
	IEEE 1646	Communication delay time among internal or external devices.
	IEEE C37.111	Define file format of measurement from IEDs.
AMI	ANSI C12 series (i.e.,	Define communication protocol for metering applications.

Table. 2. Major Standards for operating a smart grid

Table Source:- [4]

D. **Anomaly and Intrusion Detection Systems**

As previously mentioned, ADSs and IDSs are critical for detecting if an attacker has compromised grid systems and gained access to power grid networks. While these techniques have been heavily researched for IT systems, the unique communication protocols and operations requirements of the smart grid require the development of techniques that are tailored towards these environments. This section will explore the current types of IDSs and how they are integrated and validated on CPS testbeds.

Table 2. Structure of cyber protection systems.

Detection Technique	IDS Type	Active/Passive Detection
Knowledge based	Network based	Passive (intrusion detection)
Behavior based	Host based	Active (intrusion prevention)

Table. 3. Structure of Cyber Protection Systems
Table Source:-[4]

Protection Range	Category	Detection System
SCADA	Network based	[43-45]
	Host based	[46,47]
Substation	Network based	[48]
	Host based	[49]
	Integrated	[35],[50] and [51]
Wide area monitoring system (WAMS)	Host based	[52]
GPS (PMU)	Host based	[53]
Distribution system	Host based	[54]
AMI	Host based	[55-58]

Table. 4. Intrusion detection techniques in a smart grid.
Table Source:-[4]

E. **Network Separation**

Traditional network separation through demilitarized zones (DMZ) and virtual networks is a standard tool for securing networks. More recently, software-defined networking (SDN) has been providing a more flexible alternative to DMZ and virtual networks, which are usually configured once at the creation of a network and cannot easily be changed during operation. With SDN, changes to network separation can be configured quickly, e.g., to counter cyber attacks. Likewise, SDN can be used to enforce network compliant behaviour, e.g., specified using communication rules by the operator of the communication network. [59]

F. **Physical Security**

As grid operators often use their own physical networks for communication, physical security is directly related to cybersecurity. Recommended measures to ensure physical security for substations include the protection of information on substations, such as engineering drawings and power flow

models, and surveillance and monitoring measures, such as video cameras and motion detectors, as well as the restriction of physical access . With an increasing integration of novel, easily-accessible assets, such as smart meters and charging infrastructure for electronic vehicles , into the communication infrastructure of smart grids, the challenge of physical security is further exaggerated.[59]

- **Prototypes: -**

  - *Optimized smart grid model: -*

The paper approaches smart grid (SG) applications in two different ways. One approach considers the SG as a centralized cloud-based structure, while the other models SG in a modular way. Each architecture has its own advantages, so it is worth the effort to compare them.

As it is seen in Figure a, in the centralized model the grid control appears as an independent service unit alongside generation, transmission, distribution, and different types of load. It demonstrates that cloud-based databases and distributed applications play a huge role in the proper operation of the grid. On the other hand, however, it simplifies the complexity of the system, which has several drawbacks and makes the model unrealistic. In contrast, the layered architecture makes it possible to analyze smart grids in a modular way (see Figure b); consequently, a hierarchical structure can be examined without getting rid of the system's complexity. [61]

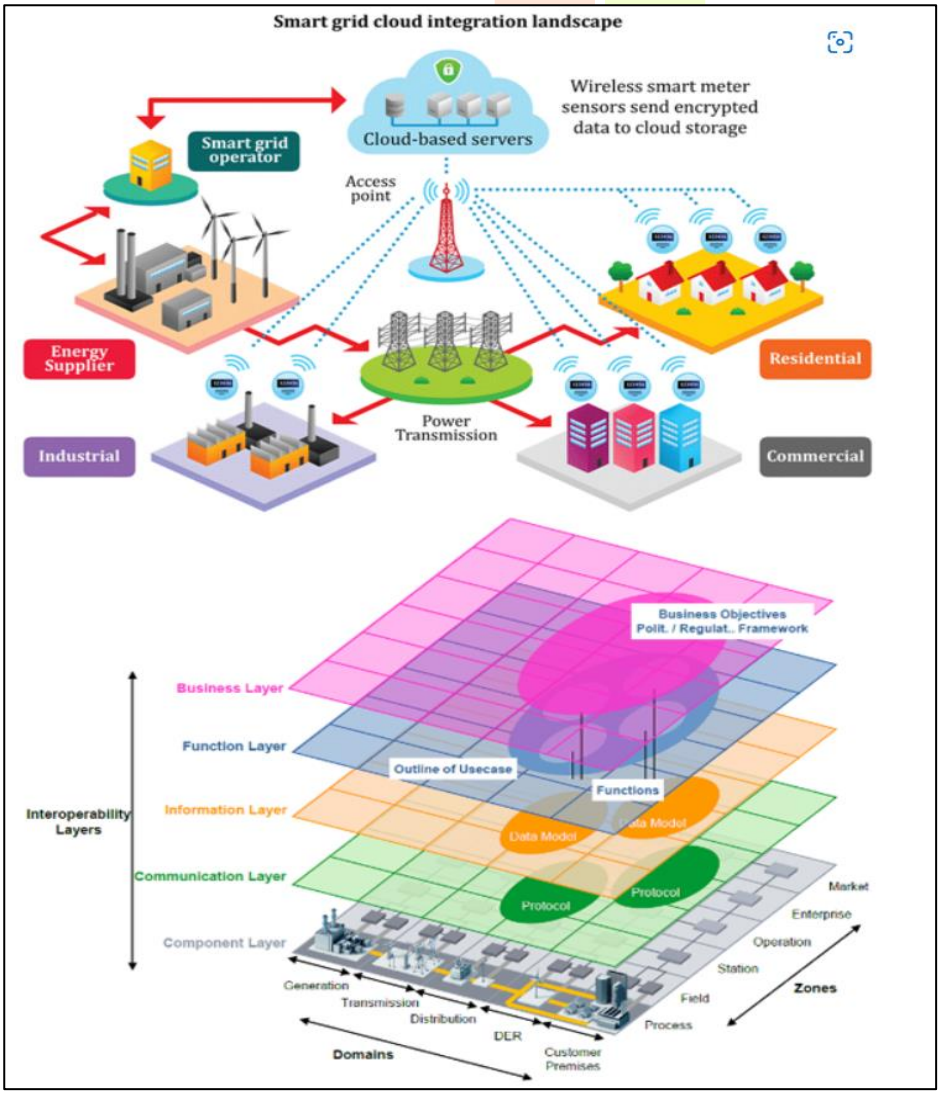

Fig. 4. Smart grid cloud Integration landscape
Figure a: Centralized SG structure (Khalil et al., 2017) **Figure b**: Layered SG architecture (Energy N. et al., 2018)

Image source: - [61]

➢ *Testbed for Intrusion and Anomaly Detection Systems: -*

Considering the integrated SCADA and SG structure presented above, a new approach for a testbed is proposed. This framework must be complex enough to represent the system properly, yet simple and transparent for comfortable work. The software includes two databases - one for the attacks, and one for the system components. The attacks can be broken into sub attacks using the tree-model, of which all of them can be built up. The attributes of them are: the entry point, the targeted component and their function. The components are stored based on their system-level, communication-type and co-operating components. The program connects these two databases, models the power grid, simulates the attacks and operates the graphical user interface. [61]

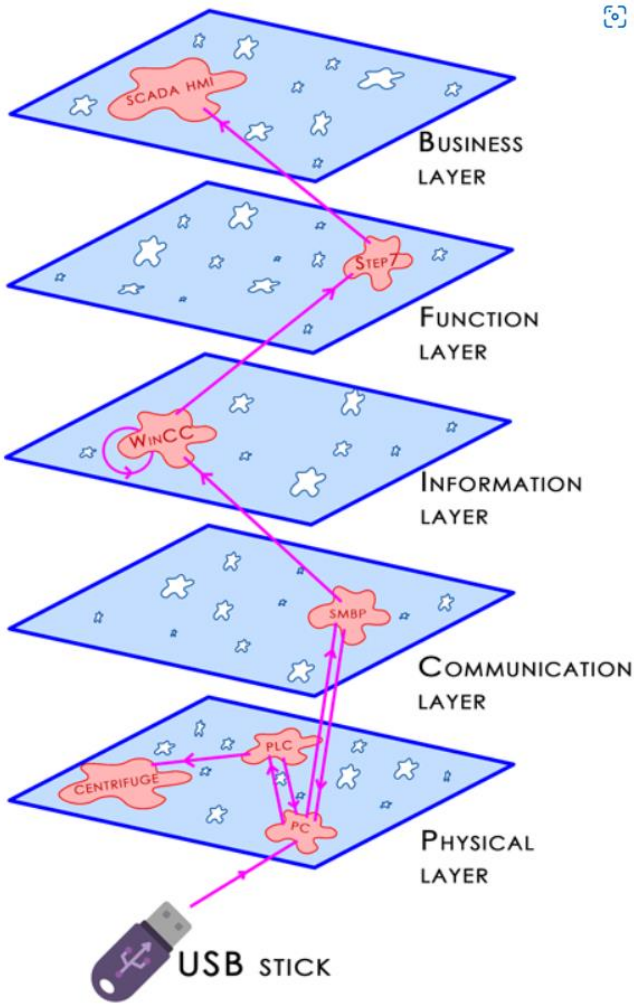

Fig. 5. Stuxnet rolling simulation

Image source: - [61]

Implementation of Behavioural intrusion prevention system that uses machine learning to detect malicious behaviors in the network traffic can be found here:-
https://github.com/stratosphereips/StratosphereLinuxIPS

➢ *Pen testing: -*

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.

smod is a modular framework with every kind of diagnostic and offensive feature needed in order to pentest modbus protocol. It is a full Modbus protocol implementation using Python and Scapy. Similarly, other protocols like IEC 870-5-10x, DNP3 can be tested for vulnerabilities.

Source:- https://github.com/0x0mar/smod

Sample Code:-

```
import sys
import os

sys.path.append(os.path.abspath(os.path.dirname(__file__) + '/System'))
from System.Core import Interface

Interface.init()
Interface.mainLoop()
```

- **Benchmark for success: -**

Smart grid cybersecurity must address both inadvertent compromises of the electric infrastructure, due to user errors, equipment failures, and natural disasters, and deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists. The primary goal is to develop a cybersecurity risk management strategy for the smart grid to enable secure interoperability of solutions across different domains and components. [60]

Depending upon our critical infrastructure we have divided our benchmarks into 6 broad categories;-

1. **Operating systems benchmarks** cover security configurations of core operating systems, such as Microsoft Windows, Linux, and Apple OSX. These include best-practice guidelines for local and remote access restrictions, user profiles, driver installation protocols, and internet browser configurations.
2. **Anomaly and Intrusion Detection benchmarks** covers if an attacker has compromised grid systems and gained access to power grid networks.
3. **Control systems benchmarks** address security configurations of core component in control systems**.**
4. **Network device benchmarks** offer general and vendor-specific security configuration guidelines for network devices and applicable hardware from Cisco, Palo Alto Networks, Juniper, and others.
5. **Network separation (Air Gap) benchmarks** offer network separation through demilitarized zones (DMZ) and virtual networks.
6. **Physical Security benchmarks outline** guidelines to ensure physical security for substations.

If the adversaries are able to find loopholes in our critical asset and thereby breach into our systems, it is considered as a failure in prevention of a cyber warfare attack for the Cybersecurity team. If adversaries are unable to find an attack vector, it is considered as a success in prevention of a cyber warfare attack.

However if further, the malware, after getting into our assets is able to conceal itself from Anomaly and Intrusion detection systems and wreak havoc on our assets, or spy on our systems, it is considered as a failure for the Cybersecurity team under Cyber warfare attack. But if we are able to identify and neutralise the threat in our critical infrastructure , it is called success.

On the contrary, the definitions of success and failure flip while we are launching an offensive on an adversary. We are entitled to call it a success if and only if we are able to breach into enemy critical infrastructures and and conceal our attack-malware from their anomaly and intrusion detection systems.

References

1. P.W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons", Case Western Reserve Journal of International Law 47 (2015); http://scholarlycommons.law.case.edu/jil/vol47/iss1/10
2. Dorothy E. Denning, "Stuxnet: What Has Changed?", Future Internet 2012, 4, 672-687; doi:10.3390/fi4030672, https://www.mdpi.com/1999-5903/4/3/672
3. "The History of Stuxnet: Key Takeaways for Cyber Decision Makers", Cyber Conflict Studies Association; https://acehacker.com/microsoft/cybersecurity/resources/The-History-of-Stuxnet.pdf
4. Chih-Che Sun, Adam Hahn , Chen-Ching Liu, "Cyber Security of a Power Grid: State-of-the-Art" https://www.sciencedirect.com/science/article/abs/pii/S0142061517328946
5. https://www.wsj.com/articles/SB10001424052702304020104579433670284061220%20
6. https://medium.com/clean-energy-for-billions/indian-blackouts-of-july-2012-what-happened-and-why-639e31fb52ad
7. U.S. NIST, "Guidelines for smart grid cyber security (Vol. 1 to 3)," NIST IR-7628, Aug. 2010,
8. Rajendra Kumar Pandey, Mohit Misra, "Cyber Security Threats - Smart Grid Infrastructure" , https://www.iitk.ac.in/npsc/Papers/NPSC2016/1570293178.pdf
9. U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special Publication 1108, Jan. 2010.
10. D. Jin, D.M.Nicol, G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," Proceedings of the 2011 Winter Simulation Conference, 2011.
11. I. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure Modbus protocol," Critical Infrastructure Protection III, Vol. 311, C. Palmer and S. Shenoi, Eds. Boston, MA: Springer-Verlag, 2009, pp. 83–96.
12. Eduard Kovacs, "Flaws in rockwell PLCs expose operational networks," Security Week, Oct. 28, 2015.
13. P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security and Privacy, Vol. 7, No. 3, May/Jun. 2009, pp. 75-77.
14. E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," IEEE Communications Magazine, Jan. 2013, pp. 42-49.
15. C. Bennett and S.B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks" Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD, Jan. 2010,pp. 1-6.
16. North American Electric Reliability Council, "SQL slammer worm lessons leanred for consideration by the electricity sector," Jun. 2013.
17. O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," Proc. 1st IEEE SmartGridComm 2010, Gaithersburg, MD, Oct. 2010, pp. 220-225.
18. Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," Proc. of the IEEE, Vol. 100, No.1, Jan. 2012, pp. 195-209.
19. Martin C. Libicki, "Expectations of Cyber Deterrence", Source: Strategic Studies Quarterly , Vol. 12, No. 4 (WINTER 2018), pp. 44-57 Published by: Air University Press Stable, The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence (securityintelligence.com)
20. https://qbeeurope.com/unpredictability/cyber-a-tough-risk-to-pin-down/
21. https://www.jstor.org/stable/pdf/26533614.pdf?refreqid=excelsior%3A54aae243da28c2415e91053c57b3997a&ab_segments=&origin=&acceptTC=1
22. Lawrence J. Trautman, Peter C. Ormerod," Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things", University of Miami Law School

23. https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF
24. D. Chapman, A. Fox, and R. Stiffler, “Cisco Secure PIX Firewalls,” Cisco Press, 2001.
25. A. Hari, S. Suri, and G. Parulkar, “Detecting and Resolving Packet Filter Conflicts,” in Proc. of the IEEE INFOCOM 2000. Conf. Comput. Commun., 2000, pp. 1203-1212
26. Modbus application protocol specification, V1.1B Modbus Organization, 2006. [Online]. Available: http://www.modbus-IDA.org
27. E. Padilla, K. Agbossou, and A. Cardenas, “Towards Smart Integration of Distributed Energy Resources using Distributed Network Protocol Over Ethernet,” IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1686-1695, Jul. 2014.
28. A. Shahzad, S. Musa, A. Aborujilah, and M. Irfan, “Industrial Control Systems (ICSs) Vulnerabilities Analysis and SCADA Security Enhancement using Testbed Encryption,” in Proc. of the ACM 8th Intl. Conf. Ubiquitous Inf. Management and Commun. (ICUIMC '14), pp. 7, New York, NY, Jan. 2014.
29. R. C. W. Phan, “Authenticated Modbus Protocol for Critical Infrastructure Protection,” IEEE Trans. Power Del., vol. 27, no. 3, pp. 1687-1689, July 2012.
30. G. Hayes and K. El-Khatib, “Securing Modbus Transactions using Hash-Based Message Authentication Codes and Stream Transmission Control Protocol,” in 2013 Third Intl. Conf. Commun. and Inf. Technol. (ICCIT), Beirut, 2013, pp. 179-184.
31. G. Gilchrist, “Secure Authentication for DNP3,” in Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Elect. Energy 21st Century, Pittsburgh, PA, USA, 2008, pp. 1–3.
32. R. Amoah, S. Camtepe, and E. Foo, “Securing DNP3 Broadcast Communications in SCADA Systems,” IEEE Trans. Industrial Informatics, vol. 12, no. 4, pp. 1474-1485, Aug. 2016.
33. K. Y. Song, K. S. Yu, and D. Lim, “Secure Frame Format for Avoiding Replay Attack in Distributed Network Protocol (DNP3),” in 2015 Intl. Conf. Inf. and Comm. Technol. Convergence (ICTC), Jeju, 2015, pp. 344-349.
34. C. W. Ten, C. C. Liu, and G. Manimaran, “Vulnerability Assessment of Cybersecurity for SCADA Systems,” IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1836-1846, Nov. 2008.
35. J. Hong, C. C. Liu, and M. Govindarasu, “Detection of Cyber Intrusions using Network-Based Multicast Messages for Substation Automation,” in 2014 IEEE Power & Energy Society Innovative Smart Grid Technol. Conf. (ISGT), Washington, DC, 2014, pp. 1-5.
36. M. Strobel, N. Wiedermann, and C. Eckert, “Novel Weaknesses in IEC 62351 Protected Smart Grid Control Systems,” in 2016 IEEE Intl. Conf. Smart Grid Commun. (SmartGridComm), Sydney, NSW, 2016, pp. 266-270.
37. J. Hong, C. C. Liu, and M. Govindarasu, “Integrated Anomaly Detection for Cyber Security of the Substations,” IEEE Tran. Smart Grid, vol. 5, no. 4, pp. 1643-1653, Jul. 2014.
38. V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, “Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids,” IEEE Syst. J., vol. 8, no. 2, pp. 509-520, Jun. 2014.
39. X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, “UDP: Usage-Based Dynamic Pricing with Privacy Preservation for Smart Grid,” IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 141-150, Mar. 2013.
40. B. Krebs, FBI: Smart Meter Hacks Likely to Spread, 2012 [Online]. Available: http://krebsonsecurity.com/2012/04/fbi-smart-meterhacks-likely-to-spread/
41. H. Rosenbaum, Danville Utilities Sees Increase in Meter Tampering, 2012 [Online]. Available: http://www.wset.com/story/20442252/ danville-utilities-sees-increase-in-meter-tampering
42. D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, “Smart Generation and Transmission with Coherent, Real-Time Data,” in Proc. of the IEEE, vol. 99, no. 6, pp. 928-951, Jun. 2011.
43. Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, “Multiattribute SCADA-Specific Intrusion Detection System for Power Networks,” IEEE Trans. Power Del., vol. 29, no. 3, pp. 1092-1102, Jun. 2014.
44. Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, “Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796-808, Dec. 2011.

45. Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, “Intrusion Detection System for IEC 60870-5- 104 based SCADA Networks,” in 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5.
46. Y. Mo, R. Chabukswar, and B. Sinopoli, “Detecting Integrity Attacks on SCADA Systems,” IEEE Trans. Control Syst. Technol., vol. 22, no. 4, pp. 1396-1407, Jul. 2014.
47. R. R. R. Barbosa, R. Sadre, and A. Pras, “Flow Whitelisting in SCADA networks,” Int. J. Crit. Infrastruct. Protect., vol. 6, pp. 150–158, Aug. 2013.
48. A. Hahn and M. Govindarasu, “Model-Based Intrusion Detection for the Smart Grid (MINDS),” in ACM Proc. of the Eighth Annual CSIIRW, New York, NY, USA, 2013.
49. C. W. Ten, J. Hong, and C. C. Liu, “Anomaly Detection for Cybersecurity of the Substations,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 865-873, Dec. 2011.
50. Y. Yang, H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks,” IEEE Trans. Power Del., vol. 32, no. 2, pp. 1068-1078, Apr. 2017.
51. U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan, “An Intrusion Detection System for IEC61850 Automated Substations,” IEEE Trans. Power Del., vol. 25, no. 4, pp. 2376-2383, Oct. 2010.
52. J. Wu, J. Xiong, P. Shil, and Y. Shi, “Real Time Anomaly Detection in Wide Area Monitoring of Smart Grids,” in 2014 IEEE/ACM Intl. Conf. Comput.-Aided Design (ICCAD), San Jose, CA, 2014, pp. 197-204.
53. Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, “A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids,” IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 2659-2668, Nov. 2015.
54. R. Mitchell and I. R. Chen, “Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications,” IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1254-1263, Sept. 2013.
55. S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, “A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures,” IEEE J. Select. Areas Commun., vol. 31, no. 7, pp. 1319-1330, Jul. 2013.
56. Y. Liu, S. Hu, and T. Y. Ho, “Leveraging Strategic Detection Techniques for Smart Home Pricing Cyberattacks,” IEEE Trans. Dependable and Secure Computing., vol. 13, no. 2, pp. 220-235, Mar.-Apr. 2016.
57. X. Liu, P. Zhu, Y. Zhang, and K. Chen, “A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure,” IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2435-2443, Sept. 2015.
58. R. Berthier and W. Sanders, “Specification-Based Intrusion Detection for Advanced Metering Infrastructures,” in Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Computing, Dec. 2011, pp. 184–193.
59. Tim Krause , Raphael Ernst , Benedikt Klaer , Immanuel Hacker and Martin Henze, “Cybersecurity in Power Grids: Challenges and Opportunities”, *Sensors* 2021, *21*(18), 6225; https://doi.org/10.3390/s21186225
60. Cybersecurity for Smart Grid Systems | NIST
61. Martin Molnár and István Vokony, ”The Cyber-Physical Security of the Power Grid”, IEEE SMART GRID, The Cyber-Physical Security of the Power Grid - IEEE Smart Grid