INTERNATIONAL JOURNAL OF COMPUTING, INTELLIGENCE, AND SECURITY RESEARCH (IJCISR)
Available Online @
ijcsir.fmsisndajournal.org.ng
IJCISR 2(1) 2023
Original Research

DESIGN FRAMEWORK OF CYBER SECURITY SOLUTIONS TO THREATS AND ATTACKS ON CRITICAL INFRASTRUCTURE OF ELECTRICITY POWER SYSTEMS OF NIGERIA COMPANIES

[1]Ismaila Idris, [2]Ilyas Adeleke, [3]Andrew Anogie Uduimoh, [4]Joshua J. Tom
[1,2,3]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[4]Elizade University, Ilara, Mokin, Nigeria

Abstract

The entire value chain of the Electric Power System (EPS) is grossly misaligned thereby creating a serious challenge in operations and decision-making process. There is serious threat being faced by the stakeholders of the EPS due to vulnerabilities of the entire system (i.e. generation, distribution and consumption). The threats imply different potential activities that can be determined or influenced either by stilted or natural instrumentality against the EPS. These threats do not necessarily correspond to failures except that they can consequently lead to failure which will hinder the confidentiality, integrity and availability (CIA) of data plus the entire information system of the EPS if requisite steps are not taken. This research carried out a comparative study on EPS with emphasis to threats and its challenges including a set objective for an EPS value chain that is well secured. The framework will aid information security and event management of electricity power system.

Keywords: Design Framework**,** Cybersecurity, Electric Power System, Threats, Attacks, Critical Infrastructure, Nigeria Companies.

1.0 Introduction

The electric power system from inception has changed the landscape of civilization of human endeavour. The electric power infrastructure has been meeting human needs successfully for centuries, transforming every aspect of human endeavours. The increase in industrial, social and technological advancements has made it difficult for the developments in power grid to keep up with the extreme demand in Power supply. Therefore, the need for an advanced intelligent power grid that is manageable, scalable and reliable, generating power through environmentally means yet interoperable and cost effective. This need gave rise to a reliable, flexible, efficient and secure energy infrastructure called "Smart Grid"(Komninos et al., 2014). Smart grid and control systems have become smart. Achieving a smart power system requires bringing the energy flow in sync with information flow in the system (Illia, et al 2020). This is possible by controlling and observing the EPS through ubiquitous technologies such as sensing, measurement, and information processing technologies (Yang et al., 2022). The security requirements of EPS differ from IT system requirements/challenges. The orders of importance for EPS is Availability, Integrity and Confidentiality not the usual CIA Triad of importance (Ahmed & Zhou 2020). The security requirement defined by availability as it applies here is to ensure continued and uninterrupted supply of electric power to consumers. Hence, to avoid different cases of intermittent distribution of energy resources, there must be continuous monitoring and communication of load availability and demand to a central controller (Suprabhath, 2023).

1.1Cybersecurity Risks and Challenges Associated with EPS National Grid (Nigeria)

According to Kaplan and Garrick (1981) risk and risk analysis (assessment); are defined as the consequence of an incidence or a hazard and the product of the probability of that hazard occurring. Their assertion was that risk analysis needs to answer the following three question: what can go wrong? What is the likelihood or probability that it can go wrong? What is the resultant effect or consequence? Also in a research conducted by the Mission Support Center Idaho National Laboratory, (2017), it was identified that ICS which is IT and network based used in monitoring and controlling the sensitive processes and physical functions of other critical infrastructure is also critical to EPS for executing fundamental processes. The EPS is comprised of different ICS systems comprises of generation, transmission, distribution and control, with highly advanced ICS platforms intercommunicating with other ICS platforms, and each of these systems may be susceptible to similar vulnerabilities irrespective of function. Some of the vulnerabilities are:

a. Different entry points that threat actors can exploit remotely.
b. The integration system of ICS makes it open to an increasing number of vulnerabilities.
c. Networked devices connected directly to the internet.
d. Creation of more network paths and connections as a result of larger demand for sensitive data collection and exchange between utilities, customers and market coordinators.

Threat is defined as different kind of likely actions that may be caused either by stilted or natural means, against a functional system (Mendel, 2017). The connectivity of critical infrastructure have become increasingly complex, making it a target by cybersecurity threats, an exploit can place a nation's economy, security, public safety and health at risk.(NIST, 2014). The challenges posed by the threats to the EPS system are enormous. In order to address these challenges, the adoption of European Union Agency for Network and Information Security (ENISA) standards Marinos, (2013)recommended as follows;

a. Consider external and internal threats that could be traced to the EPS system
b. Decompose and classify the elements of identified threats in item (a) above
c. Capture available knowledge and methodologies adopted in previous researches.

However, various smart grid security threat and challenges have been highlighted in Marinos & Lourenço (2018), Livingston, et al, (2019) and Mendel, (2017) some of which will be discussed later on. Table 1 shows cybersecurity threat and attack from 2009-2017

Table 1: The Threat Landscape on EPS (Livingston et al., 2019)

S/No.	Cyberthreat	Description / Organisation / Country of Attack	Year of attack
1.	Shodan	Searched for Internet-connected devices on search engines (it included control system devices).	2009
2.	Stuxnet	Iranian nuclear facilities SCADA control systems irreparably damaged centrifuge equipment.	July 2009
3.	Metasploit	It’s a security tool that can be utilized by hackers to explore systemvulnerabilities. It has been used to exploit ICS systems.	October 2010
4.	Shamoon	It’s a virus that was used to destroys data and disrupt operations. 15 state and private infrastructures in Saudi Arabia.	August 2012
5.	Ukraine Power Grid 1 (BlackEnergy)	230,000 residents in western Ukraine were plunged into darkness when the power was turned off by deploying SCADA- related plugin to control ICS.	December 2015
6.	Ukraine Power Grid 2 (CrashOverride)	Brought the transmission substation down by using legitimate grid process against itself, therefore causing power outage.	2016
7.	Shamoon 2	This second Shamoon virus was executed again against Saudia Arabia, it affected some private and state agencies companies.	January 2017
8.	Trisis/Triton	A petrochemical plant in Saudi Arabia was targeted, not only to sabotage the plant operations by destroying data or shutting it down, but also to set off an explosion.	August 2017

The generality of classification of threats in its entirety is referred to as the threat taxonomy. A Cyber threat actor is a person or entity who participate in action or process that is characterized by harm or intended to cause harm using and electronic devices or networks. The threat actors include; Hostile nation or foreign intelligence services (adversaries), Terrorist group, Provisional spies, Criminal group, disgruntled employees or insiders, Hacktivists and Hackers.

1.2 The EPS Cyber Security Risk Analysis and Assessment System (CSRAS)

In the EPS security objectives of solving cybersecurity threat and challenges, specific objectives must be set out in order to remain focused on issues. This will involve "deepening" the generic threat assessment by considering all peculiarities of EPS, a vital critical infrastructure of a nation. Therefore, the objectives are;

i. To do a threat assessment on the fundament on which smart grid security measures will be based.

ii. To deliver input to all stakeholders in the nation's EPS and other national agencies activities, in particular in the area of standardisation.

In addition to above, The CSRAS was developed for analysing security requirements and technical security controls. The CSRAS assessment process comprises of the following four steps:

a. Designation of Critical assets of the EPS-SG,
b. Analysis of essential requirements for Critical EPS-SG assets,
c. Vulnerability analysis of the Critical EPS-SG assets, and
d. Reporting

1.3 Methodology of Cybersecurity Solution Model for the EPS

Implementation of cybersecurity solutions across the stakeholders of the Nigerian EPS requires the design and development of a Security Operation Center (SOC) where all form of security measure will be implemented and deployed on their respective network infrastructure. The architecture of the proposed model is divided into 5 security levels of Defense-in-Depth Strategy. To efficaciously protect the EPS-SF asset from cyber-attacks the Defense-in-depth strategy should be employed and sustained in EPS-SG systems. This level requires that definition of security level and suitable security level be attributed to each EPS-SG asset (Lee et al. 2012).

NIST SP 800-82 (NIST 800-82 2011) recommends a Defense-in-depth strategy including the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities, and other managerial security programs. A graded approach where systems are zoned according to groups and security levels are attributed to each zone was recommended by IAEA technical guidance (IAEA, 2011). Five security levels and graded protective requisites are applied to each zone respectively: at level 0, the Internet; at level 1 corporate WAN; at level 2, site local area network; at level 3, data acquisition network such as SCADA, RTUs, Digital Data Logger etc; at level 4 control system network. The Open design and robustness of the SCADA system makes it easy to operate and maintain (Larouche et al. 2023).

The RG5.71 as well needs application of Defense-in-depth strategies to secure EPS-SG asset from cyber-attacks and proposed a defensive architecture that configures concentrical cyber security defensive levels. Systems that needs higher degrees of security are place within a greater number of boundaries The defensive architecture is illustrated in Figure 1. It captures the flow of defence from the five different levels of GenCos Data, TransCos, DisCos Data, IDS/IPS and the NERC utility app.

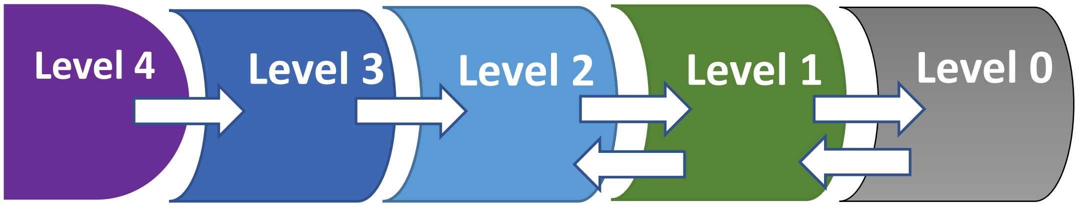

Figure1: Simplified Cyber Security Defensive Architecture

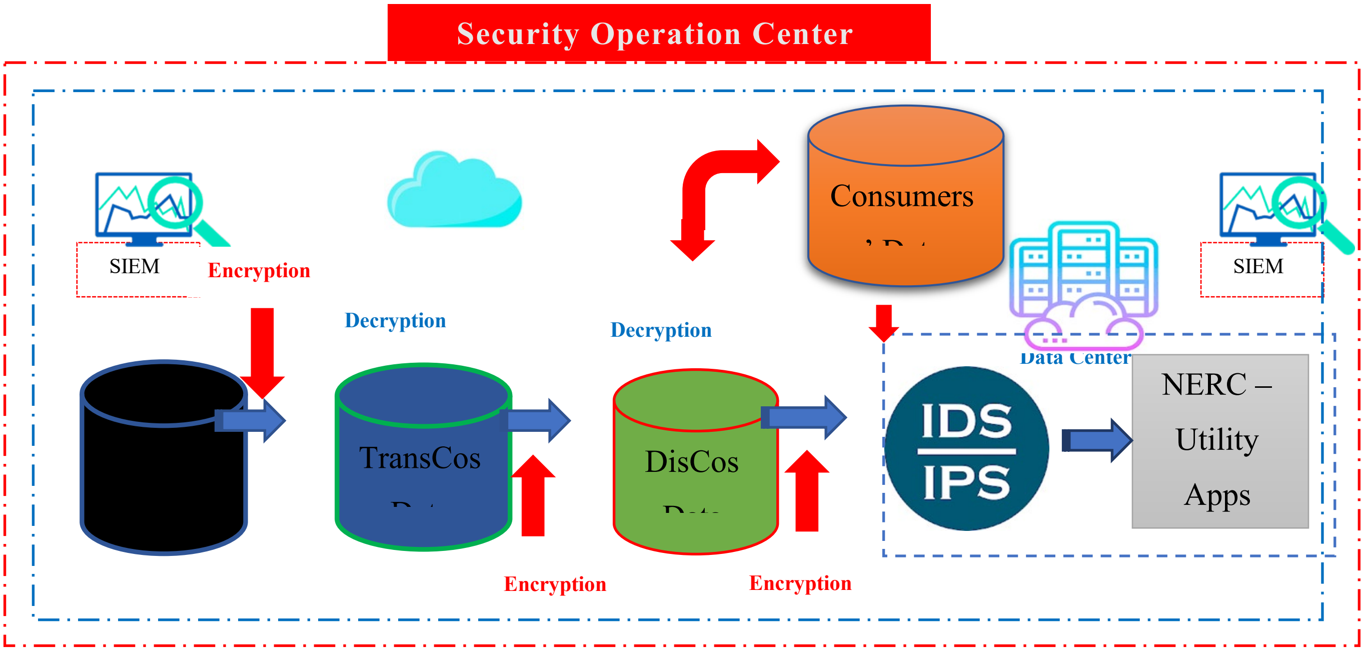

Figure 2: Proposed NERC’s / NESI SOC Model for EPS Stakeholders.

As shown in the figure 2, the SOC will be equipped with Security Information and Event Management (SIEM) for monitoring all security events, the Intrusion Detection and Prevention systems (IDS / IPS) for all cloud services and many other security tools across all the NESI stakeholders. Various data related to generation of power originated from GenCos plants will be encrypted and transmitted to TransCo. At TransCos domain, the data is decrypted and supplied to appropriate ICS device. The flow continues to the DisCos domain through encryption and later decrypted for internal use at the DisCos domain. Data exchange continue to and fro consumers encrypted and decrypted and finally, the data will transit NERC data center through IDS/IPS. This process ensures an end to end secured transmission of data from the origination to destination without being compromised.

The above system model has been used as a Test bed in an attack and counter attack simulation system to determine its resistance to various attacks such as DoS, phishing, code injection, broken authentication, cross site scripting (XSS), OS command injection attack, GPS Spoofing Attacks (ALmutairy et al., 2022) etc. An application system developed to mimic NESI stakeholders. The model has proven very effective and reliable.

1.4 Summary

The research review best practices of existing Cyber Security Solutions for electricity power system and identify the different methods of data collection from customer's home. Protocols for monitoring, computing, communication and control in different interface are designed. Development of a secure database support system with attack and counter-attack system under different scenarios are deployed. Approaches implemented so far in the EPS with smart grid technology and the global cybersecurity practices to enhance the security of the data and information exchange from various nodes in ICS devices to their respective software applications that requires their services. This model in addition to a large indigenous dataset from DISCOs will be used to further test and validate the work to ensure that it can be implemented for an attack and counter attack scenario in Nigeria EPS domain.

1.5 Acknowledgement

The Research is funded by the Nigeria Electricity Regulation Commission (NERC). It focuses on designing cybersecurity framework and protocols for data and information protection for Electricity Power Systems (EPS) in Nigeria. This research was carried out by the Federal University of Technology, Minna. Department of Cyber Security Science.

REFERENCES

Komninos, C., Survey, A., Grid, S., Komninos, N., Philippou, E., Pitsillides, A., & Member, S. (2014). City Research Online City , University of London Institutional Repository Survey in Smart Grid and Smart Home Security : Issues , Challenges and Countermeasures. https://doi.org/10.1109/COMST.2014.2320093

Lee, S., Lee, S., & Kim, J. (2016). A Study on Security Vulnerability Management in Electric Power Industry IoT, *17*(6), 499–507.

Livingston, Sanborn and Slaughter, Z. (2019). Managing cyber risk in the electric power sector | Deloitte Insights. Retrieved from https://www2.deloitte.com/insights/us/en/industry/power-and-utilities/cyber-risk-electric-power-sector.html

Marinos, L. (2013). European Union Agency for Network and Information Security Smart Grid Threat Landscape and Good Practice Guide Smart Grid Threat Landscape and Good Practice Guide About ENISA Smart Grid Threat Landscape and Good Practice Guide, (December).

Marinos, L., & Lourenço, M. (2018). *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*. *European Union Agency For Network and Information Security*. https://doi.org/10.2824/622757

Mendel, J. (2017). Smart Grid Cyber Security Challenges: Overview and Classification. *E-Mentor*, *2017*(1(68)), 55–66. https://doi.org/10.15219/em68.1282

Mission Support Center Idaho National Laboratory. (2017). Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. *Inl (Idaho National Laboratory)*, (August), 2–41. https://doi.org/10.2172/1337873

National Cybersecurity Policy, & Nigeria, C. National Cybersecurity Policy of Nigeria (2014).

NIST; Roadmap for Smart Grid Interoperability. (2012). NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards , NIST Special Publication 1108R2 NIST Framework and

Roadmap for Smart Grid Interoperability Standards. *Nist Special Publication*, 1–90.

NIST: Improving Critical Infrastructure Cybersecurity. (2014). Framework for improving critical infrastructure cybersecurity: Version 1.0. *Cybersecurity: Executive Order 13636 and the Critical Infrastructure Framework*, 55–98.

Yang T, Liu Y & Li W. (2022). Attack and defence methods in cyber-physical power system. IET Energy Systems Integration , 4 (2):159–70. https://doi.org/10.1049/esi2.12068.

Suprabhath K, S.; Machina, V.S.P & Madichetty, S. (2023) Cyber-attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review. Preprints.org 2023, 2023040691. https://doi.org/10.20944/preprints, 04.0691.v1.

Larouche, JB., Roy, S., Mailhot, F., Tardif, PM & Frappier, M. (2023). SCADA Radio Blackbox Reverse Engineering. In: Jourdan, GV., Mounier, L., Adams, C., Sèdes, F., Garcia-Alfaro, J. (eds) Foundations and Practice of Security. FPS 2022. Lecture Notes in Computer Science, vol 13877. Springer, Cham. https://doi.org/10.1007/978-3-031-30122-3_18.

ALmutairy, F., Scekic, L., & Wshah, S.. (2022). Detection and Mitigation of GPS Spoofing Attacks against Phasor Measurement Units using Deep Learning. IEEE Transaction on Smart Grids.