Science World Journal Vol. 20(No 4) 2025
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

https://dx.doi.org/10.4314/swj.v20i4.39

A CYBERSECURITY THREAT ASSESSMENT FRAMEWORK FOR THE NIGERIAN POWER SECTOR

*[1]Ovye Emmanuel Embugus, [2]Francisca Ogueleka, [1]Gilbert I.O. Aimufua, [2]Muhammed I. Umar

[1]Centre for Cyberspace Studies, Nasarawa State University, Keffi
[2]Department of Computer Science, University of Abuja

*Corresponding Author Email Address: embugus222@gmail.com

ABSTRACT

The modernization and digitalization of the Nigerian power sector, while enhancing operational efficiency, have significantly expanded its cyber-attack surface. This study conducts a comprehensive cybersecurity threat assessment to evaluate the risk posture of the sector's critical infrastructure. Employing a mixed-methods approach underpinned by a pragmatic philosophy and Design Science Research strategy, the study developed a tailored Threat-Vulnerability-Asset (TVA) framework. The framework involved a four-stage process: identification and ranking of critical assets, mapping of associated cyber threats, and prioritization of these threats based on their potential impact (calculated using a modified DREAD model) and likelihood of occurrence. The analysis identified Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMS), and Wide Area Networks (WANs) as the most critical assets. The assessment revealed that Targeted Malware and Advanced Persistent Threats (APTs) on SCADA systems pose the gravest danger (Risk Rating: 0.89), followed by Routing Attacks on WANs (0.79) and Data Interception on Advanced Metering Infrastructure (0.79). The study concludes that the convergence of high-impact and high-likelihood threats, exacerbated by legacy systems and inadequate security controls, presents a severe risk to national energy security. It recommends a multi-layered mitigation strategy, including enhanced regulatory frameworks, network segmentation, real-time monitoring, and public-private collaboration to bolster the sector's cyber resilience.

Keywords: Cybersecurity, Power Sector, Threat Assessment, Critical Infrastructure, Nigeria, TVA Framework, SCADA, Risk Prioritization.

INTRODUCTION

The electric power grid is a cornerstone of modern society, indispensable for economic stability, public safety, and socio-economic development (Ogundari and Otuyemi, 2019). Globally, the power sector is undergoing a profound transformation driven by digitalization, leading to the integration of Information Technology (IT) and Operational Technology (OT). This creates a smarter, more efficient grid but also introduces unprecedented cybersecurity vulnerabilities (Awosope, 2018). Cyber threats, ranging from ransomware deployed by cybercriminals to sophisticated state-sponsored attacks, can disrupt essential services, cause physical damage to infrastructure, and result in significant financial and reputational losses (Ngoma, 2018; Alese et al., 2014). Real-world incidents, such as the 2015 cyberattack on Ukraine's power grid, which left over 80,000 customers without electricity, serve as stark reminders of these vulnerabilities.

In Nigeria, recent power sector reforms have introduced new players and technologies focused on modernizing the national infrastructure. However, this integration of new IT/OT systems inevitably increases susceptibility to cyber-attacks. The sector's digital maturity is still emerging, characterized by a hybrid of legacy systems and modern digital solutions, creating a complex and often fragile security posture. Prior research has highlighted various challenges, including infrastructure vulnerabilities (Ibanga, Fwah, & Idowu, 2024) and the need for regulatory frameworks (Kumar et al., 2015). However, a significant gap exists in providing a holistic, data-driven threat assessment that identifies critical assets, maps specific threats, and quantifies risk based on impact and likelihood to present a clear picture of the sector's risk posture (Achuama, 2024; Ugboke, Ogunjimi, & Eze, 2024). Existing studies often fail to deliver models that prioritize threats to guide effective resource allocation for mitigation.

This study aims to fill this gap by conducting an end-to-end cybersecurity threat assessment of the Nigerian power sector. Guided by three research questions—(i) What are the critical assets? (ii) What are the most common threats? (iii) Which threats present the gravest danger?—the research develops and applies a structured TVA framework. The subsequent sections detail the materials and methods, present the conceptualization and application of the assessment framework, discuss the findings, and conclude with recommendations and directions for future work.

MATERIALS AND METHODS

This research adopted a pragmatic philosophy, which emphasizes the research problem over methodological purity and allows for the use of pluralistic approaches to derive solutions (Creswell, 2014). An abductive approach, harnessing the strengths of both inductive and deductive reasoning, was employed. The methodological choice was mixed methods, combining qualitative and quantitative techniques. The qualitative aspect involved a comprehensive literature review to identify critical assets and the cybersecurity threat landscape. The quantitative aspect involved the development of models for asset ranking and threat impact/likelihood calculation.

The research strategy was Design Science Research (DSR), which is suited for the design and development of artifacts—in this case, the threat assessment framework and models (Peffers et al., 2007). The DSR process involved: Problem Identification: Articulated in the introduction; Solution Objectives: To develop a framework for conducting a cybersecurity threat assessment; Design & Development: Creation of the TVA framework, asset ranking formula, and DREAD-based impact model; Demonstration: Power sector infrastructure owners were the unit of analysis;

Evaluation: Data gathered was analyzed to compute risk scores and Communication: Results are communicated in this paper.

Data Collection was conducted in five phases, namely; (1) Asset Identification: Secondary data analysis of literature and sector reports (e.g., NERC, 2024), (2) Threat Identification: Literature review to map threats to each identified asset, (3) Data Verification: Elite interviews with experts from 15 purposively selected power sector companies to verify the identified assets and threats, (4) Asset Ranking: The same experts ranked assets using a 5-point scale across eight impact evaluation components (Asset Value, Data Sensitivity, System Criticality, Financial Impact, Operational Disruption, Reputation Impact, Legal/Compliance Risk, and Human Safety); (5) Threat Impact/Likelihood Data: Secondary data from standard risk assessment reports (e.g., NIST, NERC, ENISA) was used to populate the impact and likelihood models.

Data Analysis involved quantitative computations:

- **Asset Ranking:** A total score for each asset was computed using the formula: *Total Score = Σ (Component Score_i)* for i=1 to 8.
- **Threat Impact:** A normalized DREAD score (DS~N~) was calculated as: *DS~N~ = ((D1 + R + E + A + D2)/5)/4*, where D=Damage, R=Reproducibility, E=Exploitability, A=Affected Users, D=Discoverability.
- **Threat Likelihood:** The Probability of Action (PoA) was calculated as: *PoA = Number of contacts resulting in hostile action (NCRHA) / Total number of contacts (TNC).*
- **Risk Rating:** The overall risk rating for a threat-asset pair was derived from the product of its Impact and Likelihood scores.

Conceptualisation of Threats Assessment Framework

The cybersecurity threat assessment for the power sector was conceptualized as a four-stage process: Asset Identification, Asset Ranking, Threat Identification, and Threat Prioritization, culminating in a Threat-Vulnerability-Asset (TVA) analysis as presented in Figure 1

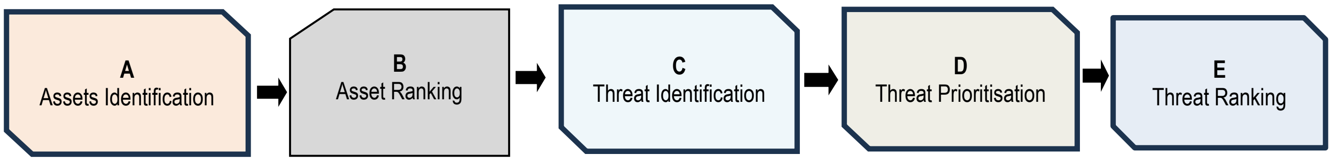

Figure 1: Process Flow Cybersecurity Threat Assessment of the Power Sector

Asset and Threat Identification

Through a systematic review, 11 critical cyber-physical assets of the power sector were identified, ranging from generation control systems to advanced metering infrastructure. Each asset was mapped with its associated cyber threats (Fallahi, Yildirim, Zhao, & Qiu, 2025). For instance, Generation and Transmission Control Systems were mapped to threats like Targeted Malware/APTs and DOS/DDOS, while SCADA systems were associated with threats including Unauthorized Remote Access and False Data Injection attacks Fallahi, Yildirim, Zhao, & Qiu, 2025) as shown in Table 1.

Table 1: Power Sector Assets and Threats Identification

S/N	Assets	Threats
1	Advanced Metering Infrastructure (AMI)	Privacy Breaches, Mass Disconnect/Reconnect Attacks, Meter Tampering and Energy Theft and Data Interception and Eavesdropping
2	Backup Power and Redundant Systems	Remote Access Exploits and Unauthorized Control, Firmware Vulnerabilities and Default Credentials, Denial-of-Service (DoS) and Load Manipulation Attacks, Supply Chain Compromise, Manipulation of Monitoring and Alerting Systems, Physical Access Breaches, Insider Threats and Misconfiguration and Lack of Monitoring and Logging
3	Generation and Transmission Control Systems	Targeted Malware and Advanced Persistent Threats (APTs), Remote Access Exploits, DOS/DDOS, Manipulation of Setpoints and Control Logic, Insider Threats and Sabotage, Supply Chain Compromises, Communication Protocol Vulnerabilities, Lack of Network Segmentation, Time Synchronization Attacks (GPS Spoofing)
4	Substation Automation Systems	Protocol-Based Exploits (IEC 61850, DNP3, Modbus), Unauthorized Access to IEDs, Compromise of Substation HMI or Engineering Workstations, Man-in-the-Middle (MitM) Attacks, Time Synchronization Attacks, DOS/DDOS, Insider Threats, Supply Chain Infections and Flat Network Architectures
5	Data Acquisition	Unauthorized Access and

	Servers	Privilege Escalation, Malware and Ransomware Infections, Data Integrity and Injection Attacks, Denial-of-Service (DoS) Attacks, Insider Threats, Unpatched Vulnerabilities and Legacy Systems, Communication Protocol Exploits, Credential Theft and Reuse, Data Exfiltration and Espionage
6	Wide Area Networks (WANs) and Communication Infrastructure	Eavesdropping and Interception, Man-in-the-Middle (MitM) Attacks, Routing Attacks (e.g., BGP Hijacking, Route Injection), Compromise of Network Devices (Routers, Switches, Modems), Unsecured Remote Access and VPNs, Spoofing and Impersonation Attacks, Satellite Communication Hijacking or Jamming, DDOS/DOS and insider threats.
7	Supervisory Control and Data Acquisition (SCADA) Systems	Malware and Ransomware Attacks, Advanced Persistent Threats (APTs), DOS/DDOS, Insider Threats, Unauthorized Remote Access, Exploitation of Zero-Day Vulnerabilities, Communication Network Compromise, Phishing and Social Engineering, Outdated and Unpatched Systems, Physical Attacks, False Data Injection (FDI) Attacks, Weak Authentication and Authorization; Supply Chain Attacks and Vulnerable Wireless Connections
8	Intelligent Electronic Devices (IEDs)	Data Integrity Attacks, Configuration Errors and Credential Management Issues and Insecure Protocols (e.g., IEC 61850, DNP3, Modbus)
9	Energy Management Systems (EMS)	Same as in SCADA except Man-in-the-Middle (MITM) Attacks
10	Programmable Logic Controllers PLCs)	Same as in SCADA
11	Remote Terminal Units (RTUs)	Same as in SCADA except for Firmware and Software Exploits and Configuration and Credential Weaknesses

Source: (Fallahi, Yildirim, Zhao, & Qiu, 2025; African Development Bank Group, 2024; Nigerian Electricity Regulatory Commission [NERC], 2024); Madurasinghe & Venayagamoorthy, 2022 and 6Wresearch, 2023)

Asset Ranking

Asset ranking plays a critical role in power sector cybersecurity threat assessment by enabling organizations to prioritize the protection of their most critical infrastructure. Through systematic evaluation of assets based on factors such as system criticality, data sensitivity, financial impact, and potential operational disruption, stakeholders can determine which components—such as SCADA systems, energy management systems (EMS), and substation automation—pose the greatest risk if compromised. This prioritization helps in allocating security resources efficiently, ensuring that the most vulnerable and high-impact assets receive focused attention (Fallahi, Yildirim, Zhao, & Qiu, 2025). To carry out the ranking of the assets identified in Table 4.1, the impact evaluation components in Table 2 form the basis of the evaluation of and ranking of each asset. The research adopted the quantitative methodology, consequently, the impact metric and scale defined on a scale of 1-5 as presented in Table 3.

Table 2: Impact Evaluation Component

S/N	Component	Code	Description
1	Asset Value	AV	How critical is the asset (system, data, service) to the organization's operations or mission?
2	Data Sensitivity	DS	Would exposure of the data result in financial loss, legal action, or reputational damage?
3	System Criticality	SC	Would disruption cause business downtime, safety issues, or affect national security (in CI)?
4	Financial Impact	FI	Direct and indirect costs (e.g., loss of revenue, regulatory fines, recovery expenses).
5	Operational Disruption	OD	Delays, outages, or loss of production, especially in OT environments.
6	Reputation Impact	RI	Loss of customer trust, negative press, or stock price drop.
7	Legal & Compliance Risk	LCR	Penalties from non-compliance with laws (e.g., GDPR, HIPAA, NERC CIP).
8	Human Safety	HS	In environments like power plants or hospitals, cyberattacks can endanger lives.

Source: Modified from (NIST, 2012; NERC, 2014 and ISO, 2018)

Table 3: Impact Metrics and Scale

Scale	Metric	Description
1	Low	Limited operational disruption or negligible financial loss. Affects non-critical systems or a small number of users.
2	Medium	Noticeable degradation in operations, but core grid services

https://dx.doi.org/10.4314/swj.v20i4.39

		remain functional. May require manual intervention or temporary workarounds.
3	High	Disruption to core systems, moderate financial loss, or failure to meet compliance requirements. Could trigger public concern or utility penalties.
4	Critical	Widespread service outage, major financial impact, and potential safety concerns. Requires emergency response and full organizational coordination.
5	Catastrophic	National-scale disruption or physical destruction of power infrastructure. Severe loss of life, national security implications, or geopolitical consequences.

Source: Modified from (NIST SP 800-30, 2020; NERC CIP, 2018; and ISO/IEC 27005, 2017)

To rank the assets, the following formula was used to compute each assets' total score based on the 8-impact evaluation component.

$$\text{Total Score}=\sum_{i=1}^{8}\text{Component Score } i \qquad (1)$$

Where **total score** represents the score per each identified power sector asset based on *i* which represent the impact evaluation component, since the impact evaluation component are 8, *i* is from 1 to 8, component score *i* is the individual score for the evaluation components. The data generated for scoring individual assets based on the impact evaluation components were generated from standard risk assessment reports in (NIST, 2012; International Society of Automation [ISA], 2018; NERC, 2023; DOE, 2022; FERC, 2021; ENISA, 2020 and (IEEE Power & Energy Society, 2019)).

Table 4: Asset Ranking Table

#	Asset	AV	DS	SC	FI	OD	RI	LCR	HS	Total Score
1	Generation and Transmission Control Systems	5	5	5	5	5	5	5	5	40
2	SCADA Systems	5	5	5	5	5	5	5	5	40
3	Energy Management Systems (EMS)	5	5	5	5	5	5	5	5	40
4	Backup Power and Redundant Systems	4	3	5	4	5	4	3	4	32
5	Substation Automation Systems	4	4	4	4	4	4	4	4	32
6	Intelligent Electronic Devices (IEDs)	4	4	4	4	4	4	4	4	32
7	Programmable Logic Controllers (PLCs)	4	4	4	4	4	4	4	4	32
8	Remote Terminal Units (RTUs)	4	4	4	4	4	4	4	4	32
9	Wide Area Networks (WANs)	4	4	4	4	4	4	4	3	31
10	Data Acquisition Servers	4	5	4	4	4	4	5	3	33

#	Asset	AV	DS	SC	FI	OD	RI	LCR	HS	Total Score
11	Advanced Metering Infrastructure (AMI)	3	4	3	3	3	3	4	2	25

Source: Author's computation based on equation 1

Threat Prioritisation

Based on the asset ranking in Table 4, the researcher mapped the threats to each assets as identified in Table 1 and present based on the order of ranking in Table 5. This data will be used to carry out threat prioritisation in the following section.

Table 5: Ranked Power Assets Mapped with Threats

#	Asset	Total Score	Threats
1	Generation and Transmission Control Systems	40	Targeted Malware and Advanced Persistent Threats (APTs), Remote Access Exploits, DOS/DDOS, Manipulation of Setpoints and Control Logic, Insider Threats and Sabotage, Supply Chain Compromises, Communication Protocol Vulnerabilities, Lack of Network Segmentation, Time Synchronization Attacks (GPS Spoofing)
2	SCADA Systems	40	Malware and Ransomware Attacks, Advanced Persistent Threats (APTs), DOS/DDOS, Insider Threats, Unauthorized Remote Access, Exploitation of Zero-Day Vulnerabilities, Communication Network Compromise, Phishing and Social Engineering, Outdated and Unpatched Systems, Physical Attacks, False Data Injection (FDI) Attacks, Weak Authentication and Authorization; Supply Chain Attacks and Vulnerable Wireless Connections
3	Energy Management Systems (EMS)	40	Same as in SCADA except Man-in-the-Middle (MITM) Attacks
4	Backup Power and Redundant Systems	32	Remote Access Exploits and Unauthorized Control, Firmware Vulnerabilities and Default Credentials, Denial-of-Service (DoS) and Load Manipulation Attacks, Supply Chain Compromise, Manipulation of Monitoring and Alerting Systems, Physical Access Breaches, Insider Threats and Misconfiguration and Lack of Monitoring and Logging
5	Substation Automation Systems	32	Protocol-Based Exploits (IEC 61850, DNP3, Modbus), Unauthorized Access to IEDs, Compromise of Substation HMI or Engineering Workstations, Man-in-the-Middle (MitM) Attacks, Time Synchronization Attacks, DOS/DDOS, Insider Threats, Supply Chain Infections and Flat Network Architectures
6	Intelligent Electronic Devices (IEDs)	32	Data Integrity Attacks, Configuration Errors and Credential Management Issues and Insecure Protocols (e.g., IEC 61850, DNP3, Modbus)
7	Programmable Logic Controllers (PLCs)	32	Same as in SCADA
8	Remote Terminal Units (RTUs)	32	Same as in SCADA except for Firmware and Software Exploits and Configuration and Credential Weaknesses
9	Wide Area Networks (WANs)	31	Eavesdropping and Interception, Man-in-the-Middle (MitM) Attacks, Routing Attacks (e.g., BGP Hijacking, Route Injection), Compromise of Network Devices (Routers, Switches, Modems), Unsecured Remote Access and VPNs, Spoofing and Impersonation Attacks, Satellite Communication Hijacking or Jamming, DDOS/DOS and insider threats.
10	Data Acquisition	33	Unauthorized Access and Privilege Escalation,

	Servers		Malware and Ransomware Infections, Data Integrity and Injection Attacks, Denial-of-Service (DoS) Attacks, Insider Threats, Unpatched Vulnerabilities and Legacy Systems, Communication Protocol Exploits, Credential Theft and Reuse, Data Exfiltration and Espionage
11	Advanced Metering Infrastructure (AMI)	25	Privacy Breaches, Mass Disconnect/Reconnect Attacks, Meter Tampering and Energy Theft and Data Interception and Eavesdropping

Source: Author

Impact Computation

Threat prioritization for the power sector infrastructure is a function of the potential impact and likelihood of occurrence of these threats to the identified assets and their threats mapping. Thus, to compute the potential impact of a threat on an asset, the DREAD model was used as presented in Table 6 was modified and applied.

Table 6: DREAD Model

DREAD Element	Definition
D – Damage Potential	How much damage could be caused?
R – Reproducibility	How easily can the attack be repeated?
E – Exploitability	How easy is it to exploit the vulnerability?
A – Affected Users	How many users or systems would be impacted?
D – Discoverability	How easy is it to discover the vulnerability or exploit?

Source: (Zhang, et al, 2021).

To compute the impact of individual threats on assets, we compute the DREAD score for each threat based on a 5-point scale score between 0 (very low) to 4 (critical) presented in Table 7. The average of the five gives a DREAD score (DS). The following equation computes the DREAD score.

$$DS = (D_1 + R + E + A + D_2)/5 \qquad (2)$$

Where DS is the DREAD score, the other variables are as presented in Table 6. Note that D_1 represents damage potential and D_2 - discoverability, the subscript numbers (1 and 2) enable us to differentiate between the Ds in the formula. However, based on Table 8, the DREAD score must be between 0.00 – 1.00, thus, to maintain the score within that range, equation 3 is formulated so as to normalise the value of DS between 0.00-1.00.

$$DS_N = ((D_1 + R + E + A + D_2)/5)/4 \qquad (3)$$

Where DS_N is the normalised value of DS, note the division by 4 is done for normalisation since there are 5 DREAD elements in Table 6 and the highest value achievable in Table 7 is 4, multiplication of 4 x 5 gives 20 and a division of the value of DS by 4 keeps the value of DS_N between 0.00 – 1.00 in all cases.

Table 7: DREAD Measure Scale (DMS)

Quantitative	Level	Interpretation
0	Very Low	Negligible risk — minimal attention needed
1	Low	Low risk — monitor but usually no urgent action required
2	Medium	Moderate risk — some mitigation or planning should be considered
3	High	High risk — active remediation and controls needed
4	Critical	Severe risk — immediate action required to prevent major impact

Source: Modified from (NIST, 2021)

Table 8 presents the DREAD impact classification scale that is used to classify threats based on their DREAD scores. It enables us to have a frame for threat prioritisation and mitigation efforts.

Table 8 DREAD Impact Categorisation Scale

DREAD Score Range	Level	Interpretation
0.00 – 0.20	Insignificant	Negligible risk — minimal attention needed
0.21 – 0.40	Minor	Low risk — monitor but usually no urgent action required
0.41 – 0.60	Moderate	Moderate risk — some mitigation or planning should be considered
0.61 – 0.80	Major	High risk — active remediation and controls needed
0.81 – 1.00	Catastrophic	Severe risk — immediate action required to prevent major impact

Source: Author

Likelihood of Threat Computation

$$PoA = \frac{NCRHA}{TNC} \qquad (4)$$

Where:
(PoA) is Probability of Action which is the likelihood of threats successfully exploiting an asset
NCRHA is the Number of contacts resulting in hostile action, i.e. number of contacts resulting in successful breach, and;

Table 9: Likelihood Classification Scale

LEF Range	Level	Interpretation
0.00 – 0.20	Rare	May occur only in exceptional circumstances
0.21 – 0.40	Unlikely	Could occur at some time
0.41 – 0.60	Possible	Might occur at some time
0.61 –	Likely	Will probably occur in most

0.80		circumstances
0.81 – 1.00	Almost certain	It's expected to occur in most circumstances

Source: ISO/IEC 27005, (2022)

In this research, data is presented on the impact of threats and the likelihood of threats. Figures 1 to 11 present the data on the threats ranking per the various assets. Figure1 present the threats ranking for the asset: Generation and Transmission Control Systems.

Impact of Threats Data

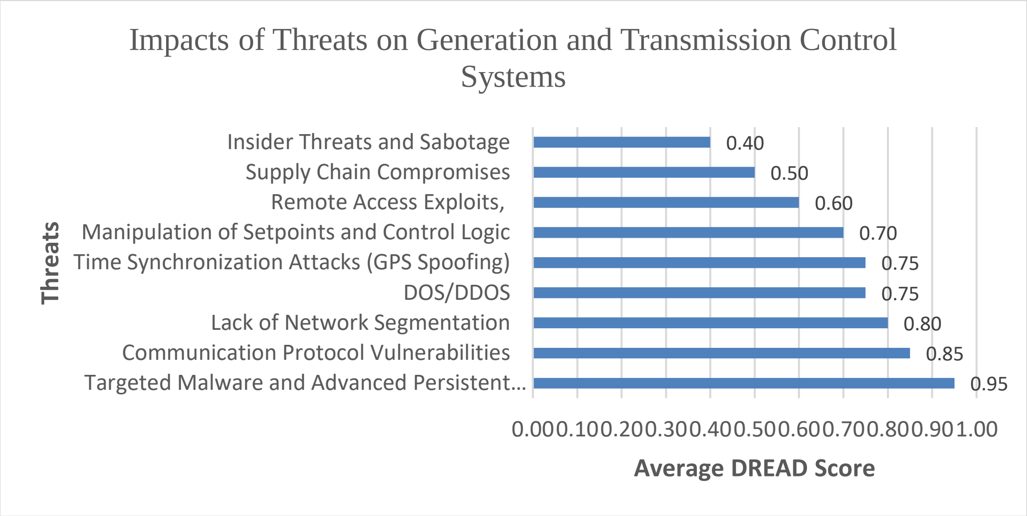

Figure 1: *Threats Ranking for Generation and Transmission Control System*

The data in Figure 1 shows that 9 threats were identified for the named assets, based on Table 8, two (2) threats fall within the catastrophic category, 5 are within the major category, and the remaining 3 fall in the moderate and minor category. The implication is the that the threats within the catastrophic category potentially pose the most danger for this asset followed by those in the major category.

Figure 2 presents the threat ranking for SCADA systems, the data in the figure shows that 13 threats were identified, based on the threat impact categorisation scale in Table 8, 5 of the threats have catastrophic and major impacts each; 2 are of moderate impact and 1 potentially has minor impact.

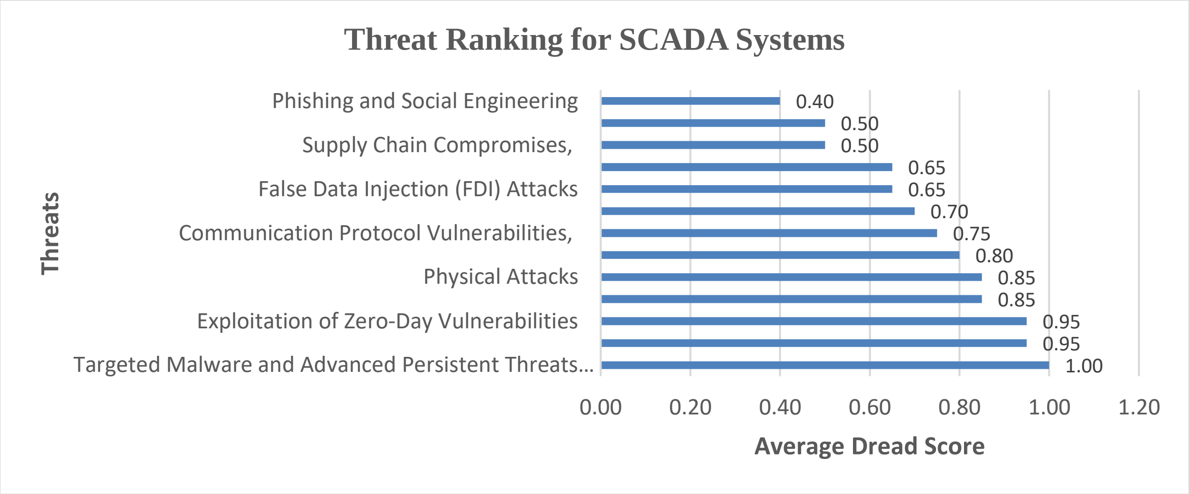

Figure 2*: Threat Ranking for SCADA Systems*

Figure 3 depicts the threats ranking for Energy Management Systems (EMS), 14 threats were identified to be associated with this asset. The impact computation and ranking show that 4 of the threats are potentially catastrophic while 7 and 3 are of major and moderate impacts respectfully.

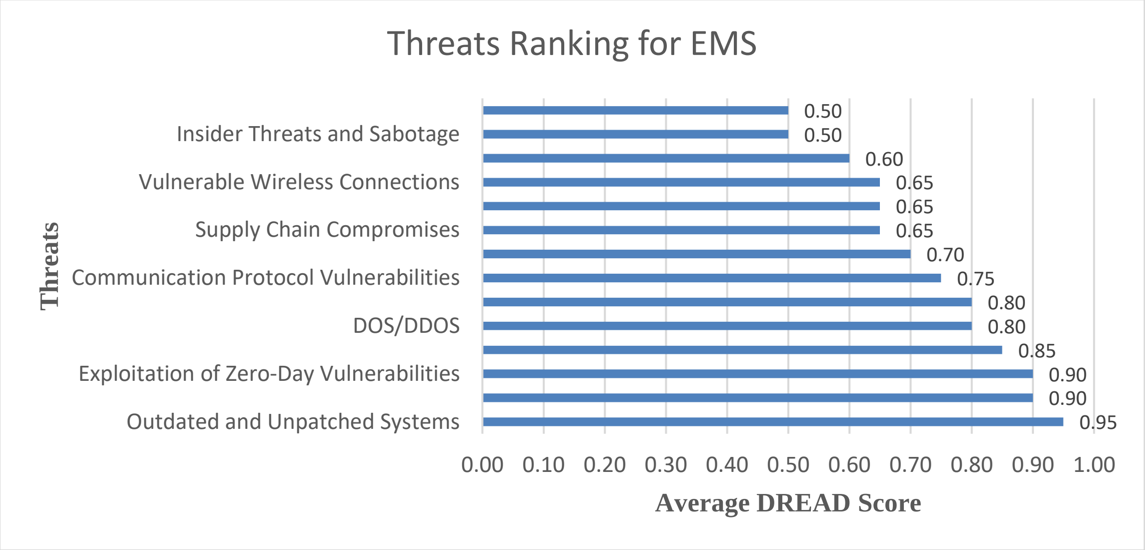

***Figure 3**: Threats Ranking for EMS*

In Figure 4, the data related to the threats associated backup and power redundancy systems is presented, 8 threats are identified and mapped to this asset, 3 of them potentially have catastrophic impact, 4 and 1 are of major and moderate impacts respectfully.

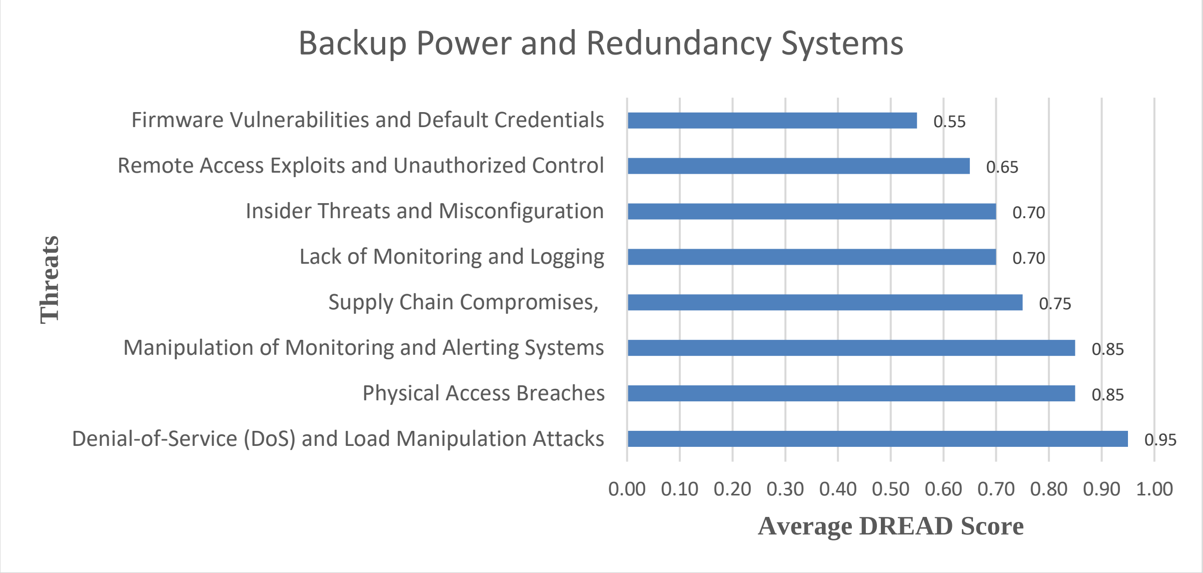

***Figure 4**: Backup Power and Redundancy Systems*

Figure 5 depicts the data of the threats associated with intelligent electronic devices (IEDs), 9 threats are associated with this asset, 2 of them have catastrophic impact, 5 and 2 are of major and moderate impacts respectfully

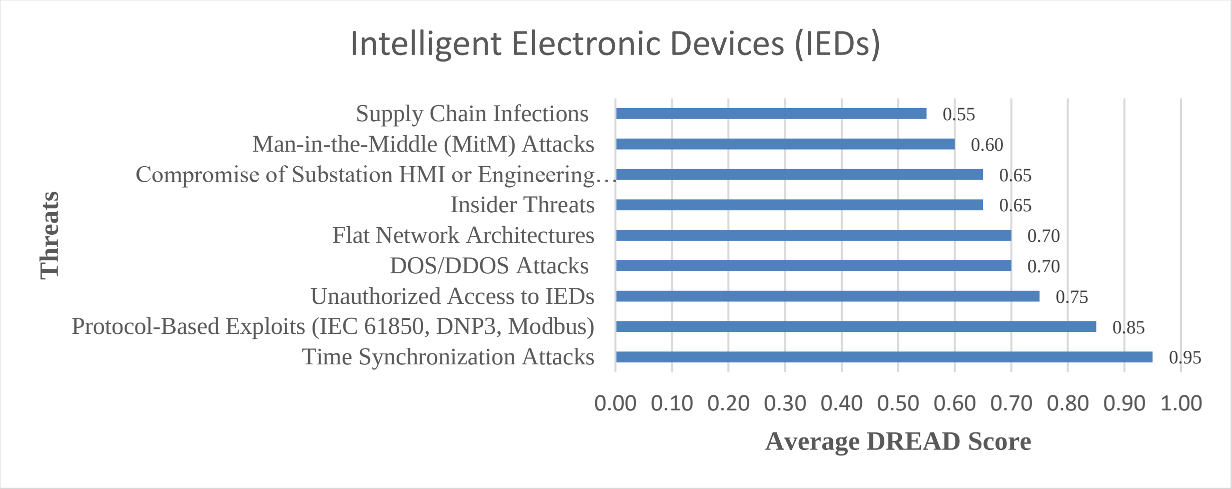

***Figure 5:** Intelligent Electronic Devices (IEDs)*

In Figure 6, the data related with substation automation systems threats is presented. 3 threats are associated with this asset. 1 and 2 are of catastrophic and major impacts respectfully.

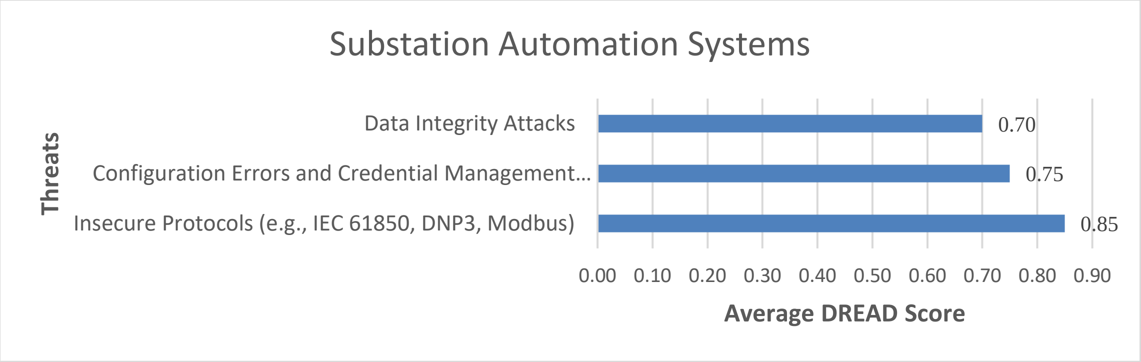

***Figure 6**: Substation Automation Systems*

Figure 7 contains a summary of data about the programmable logic controllers (PLCs); 13 threats are identified to be associated with this asset. 4 of these threats have potentials for catastrophic impact, 3 and 5 are of major and moderate impact while 1 is of minor impact.

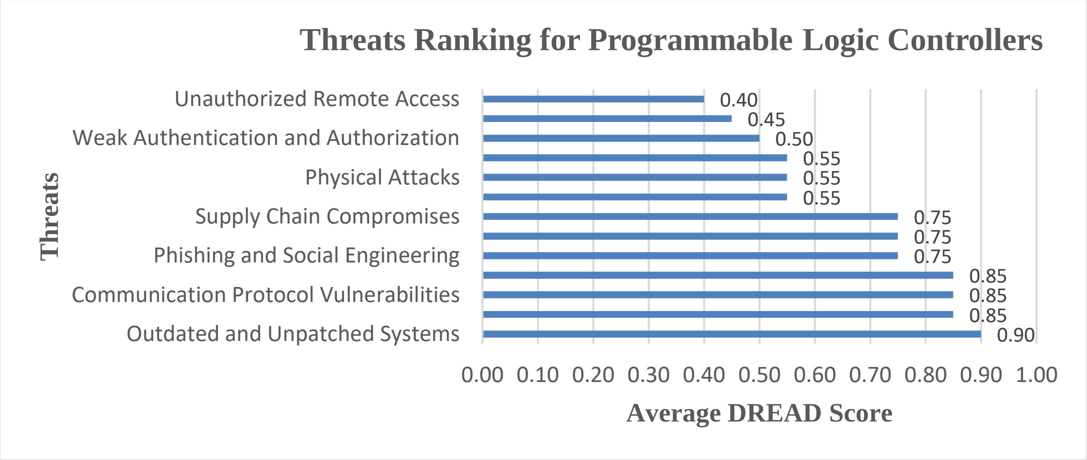

***Figure 7**: Threats Ranking for Programmable Logic Controllers*

In Figure 8, 15 threats were identified to be associated with remote terminal units (RTUs), 6 of these threats are potentially of catastrophic consequences, 8 are of major impact while 1 is of moderate impact.

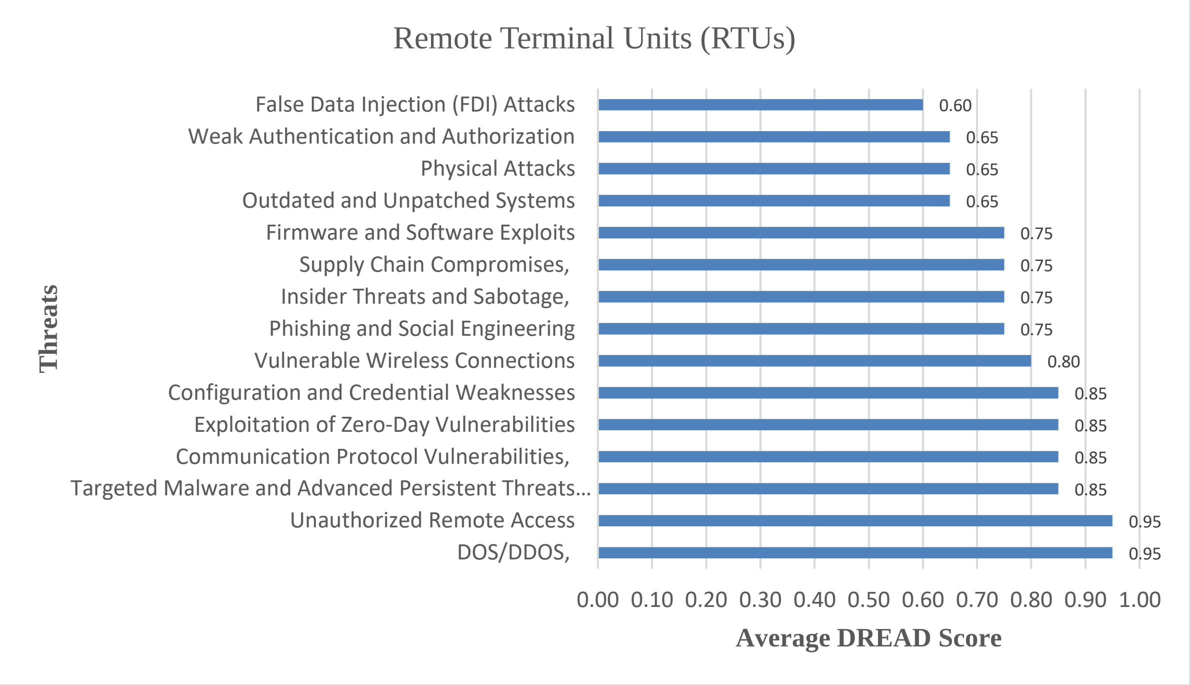

Figure 8: *Remote Terminal Units (RTUs)*

Figure 9 shows that the wide area networks (WANs) as a power sector asset has 9 threats, 4 of these threats are of catastrophic and major impact potentially, 1 is of moderate impact.

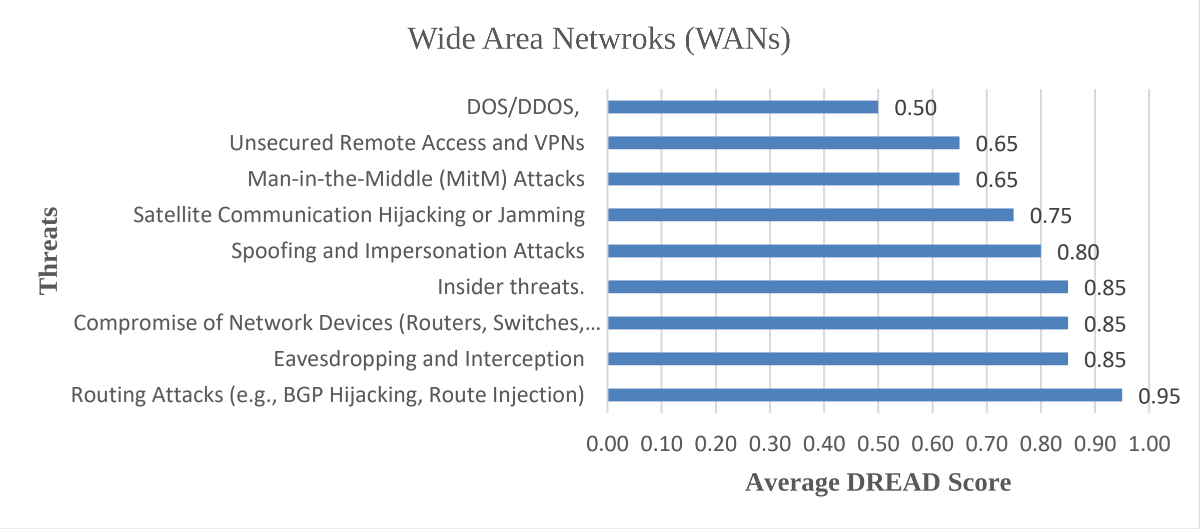

Figure 9: *Wide Area Networks (WANs)*

and Figure 10 presents data of the data acquisition servers (DASs), the data showed that this asset has 9 threats, 5 of the threats are of catastrophic impacts, 3 and 1 are of major and moderate impacts respectively.

https://dx.doi.org/10.4314/swj.v20i4.39

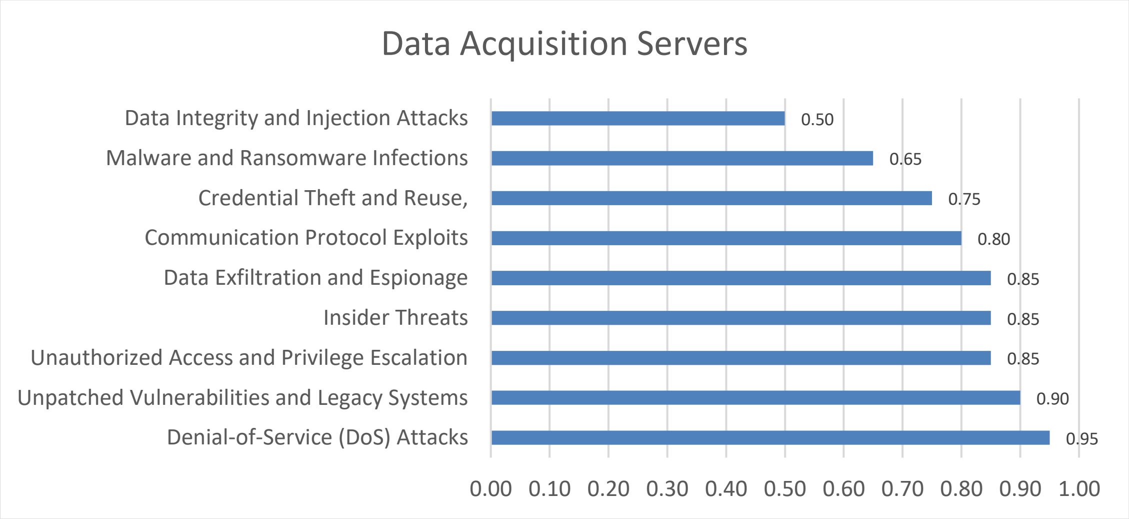

***Figure 10**: Data Acquisition Servers*

Figure 11 contains data associated with advanced metering infrastructure (AMI), 4 threats are associated with this asset, 2 of the threats are potentially catastrophic while another 2 is potentially of major impact.

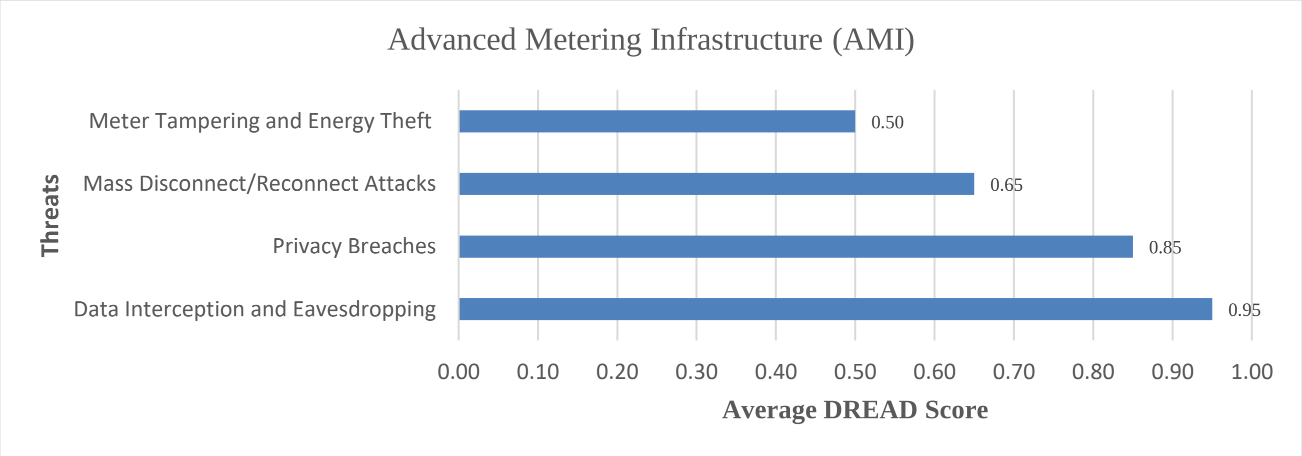

***Figure 11:** Advanced Metering Infrastructure (AMI)*

Likelihood of Threat Data Presentation

Figures 12 to 22 present the data on the likelihood that the identified threats will breach the assets associated with them. Figure 12 presents the data on the likelihood of threats associated with the generation and transmission control systems assets. The asset has 9 identified threats, based on the likelihood scale presented in Table 9, targeted malware and advanced persistent attacks and DOS/DDOS attacks are in the has the highest likelihood, 1 threat (insider threats and sabotage) is likely, 1 other is possible and the remaining 5 fall within the unlikely band.

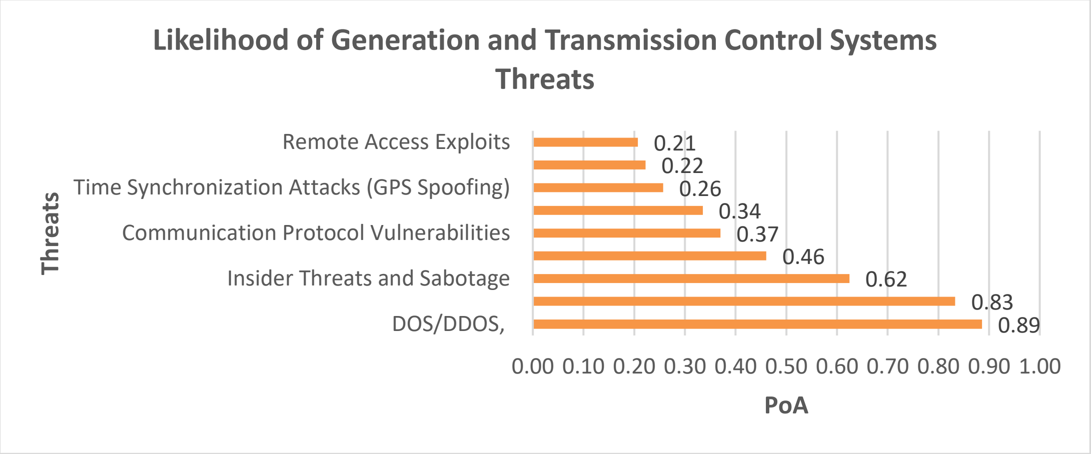

***Figure 12**: Likelihood of Generation and Transmission Control Systems Threats*

Figure 13, the Likelihood of SCADA Systems Threats is presented, the asset has 13 threats, one of these threats is in the almost certain category of likelihood, 2 are in the likely category; 3 are in the unlikely category and the remaining 7 are in the rare category of likelihood.

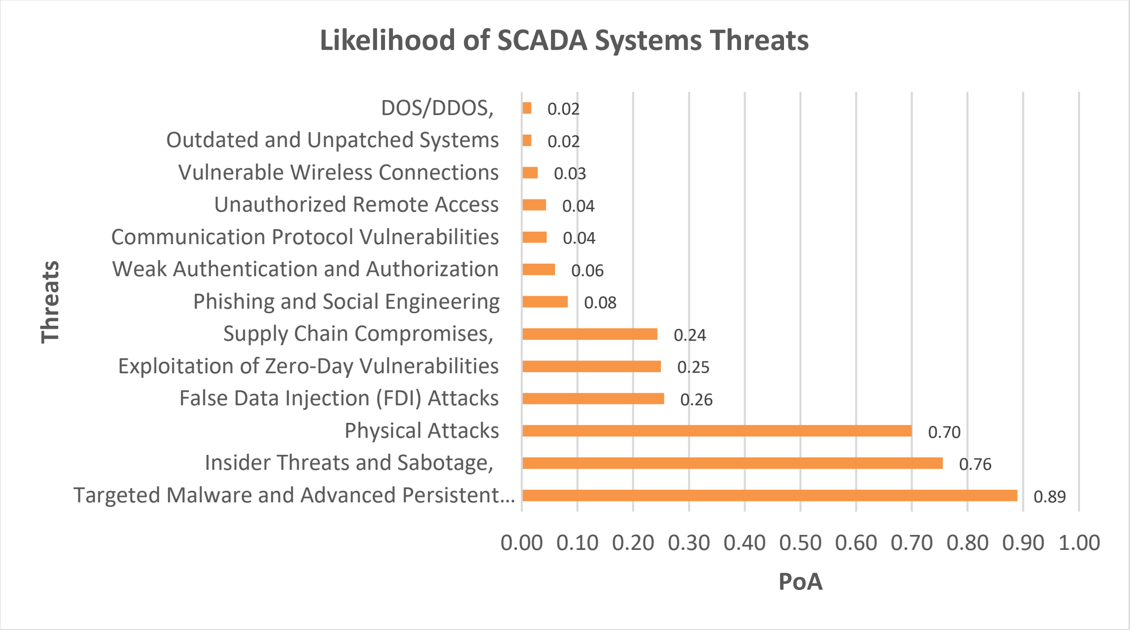

Figure 13: Likelihood of SCADA Systems Threats

Figure 14 contains the data on the likelihood of Energy Management Systems which has 14 threats. One of these threats is in the highest level of likelihood – almost certain, 2 are in the likely category; 4 are in the possible category and the remaining 7 are in the rare category of likelihood.

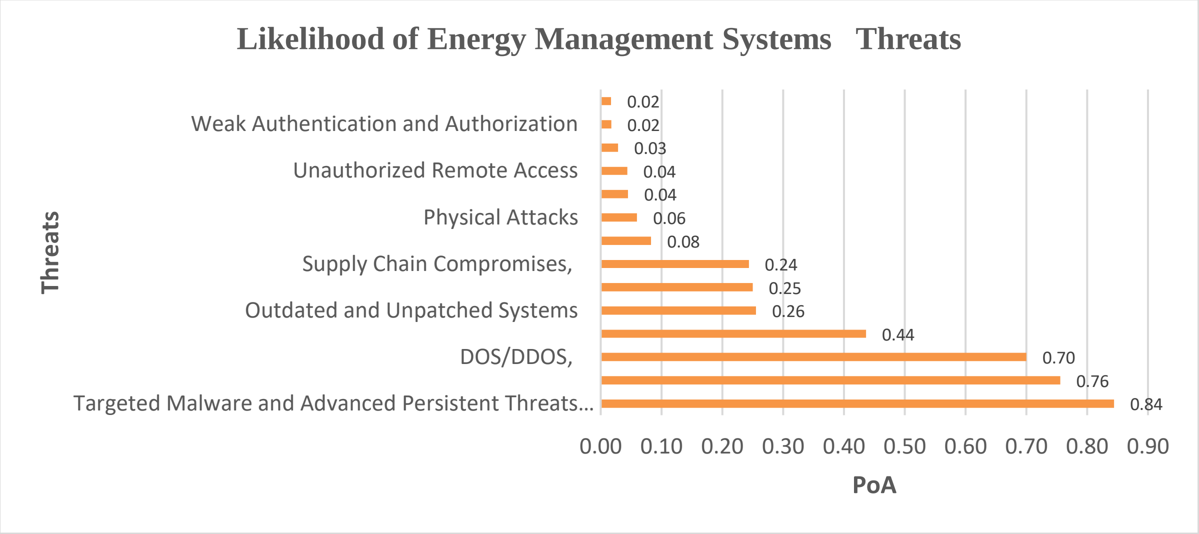

Figure 14: Likelihood of Energy Management Systems Threats

Figure 15 depicts the data for the likelihood of the materialisation of threats to backup power and redundancy systems.

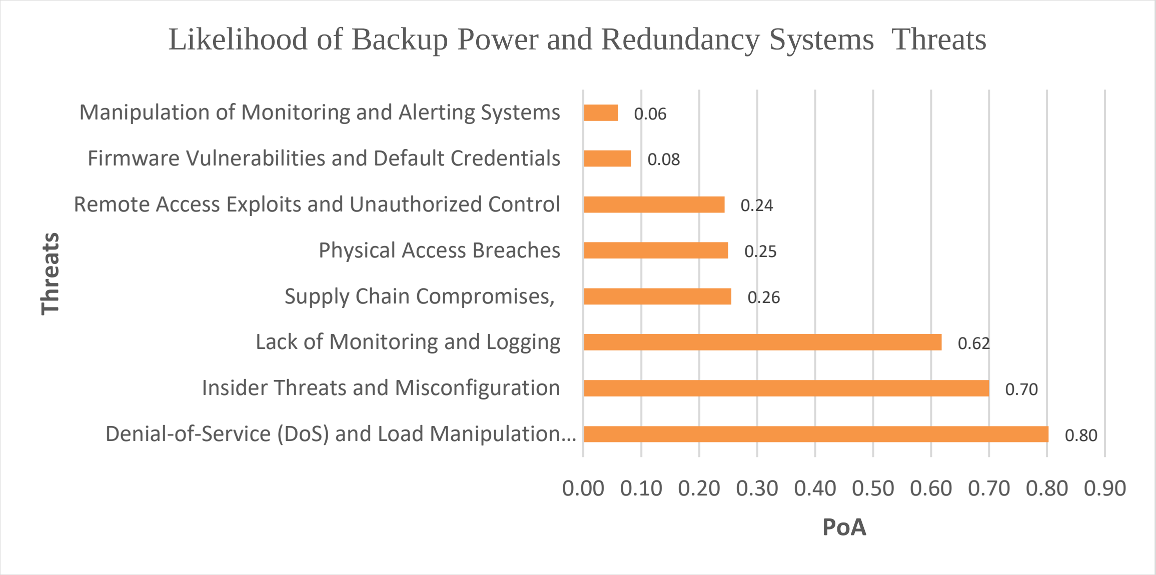

Figure 15: Likelihood of Backup Power and Redundancy Systems Threats

Figure16 presents data on Intelligent Electronic Devices (IEDs), this asset has 9 threats, out of which 1 (DOS/DDOS attacks), 1 is in the likely band, 2 in the possible and unlikely bands respectively while the remaining 3 are in the rare band.

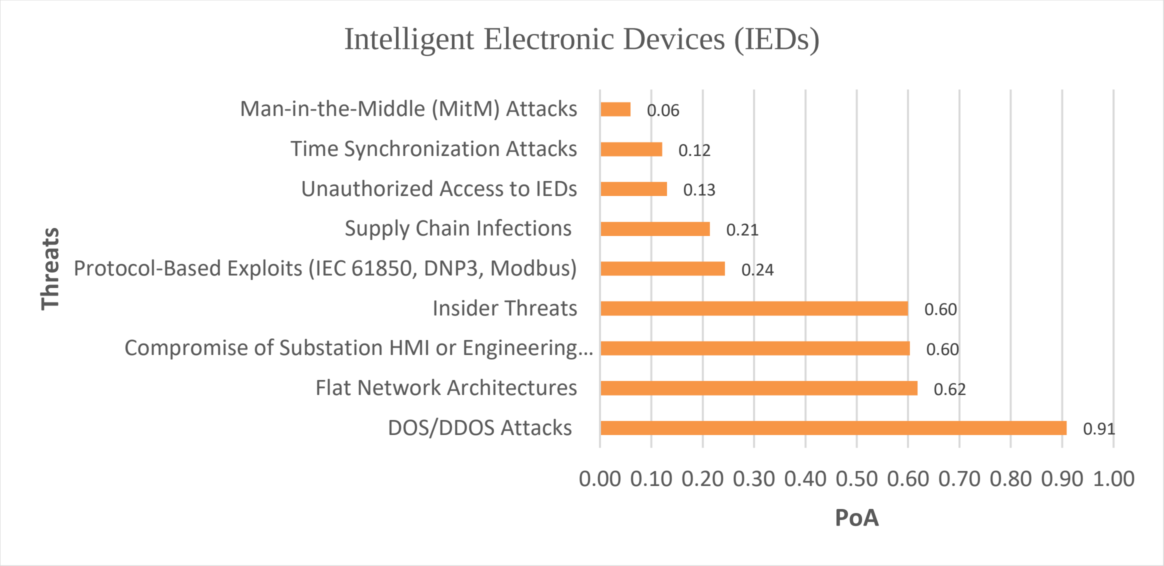

Figure 16: Intelligent Electronic Devices (IEDs)

Figure 17 the likelihood data of Substation Automation Systems threats is presented with 3 threats, 1 is in the possible band and 2 are in the unlikely band.

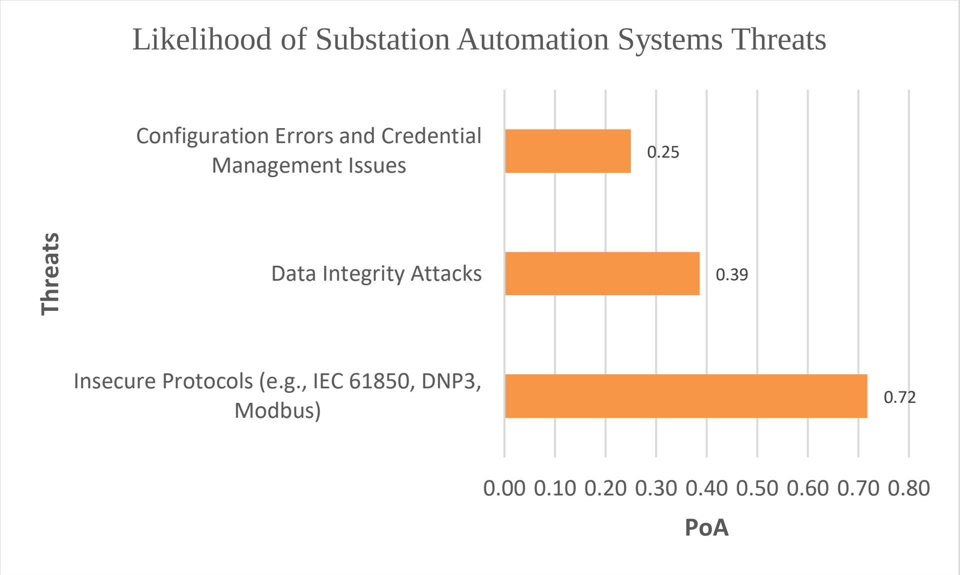

Figure 17: Likelihood of Substation Automation Systems Threats

Figure 18 presents data on the likelihood of programmable logic controllers' threats. In this assets, 13 threats are identified, 1 is in the almost certain band, 2 in the possible band while 3 and 7 are in the unlikely and rare categories respectively.

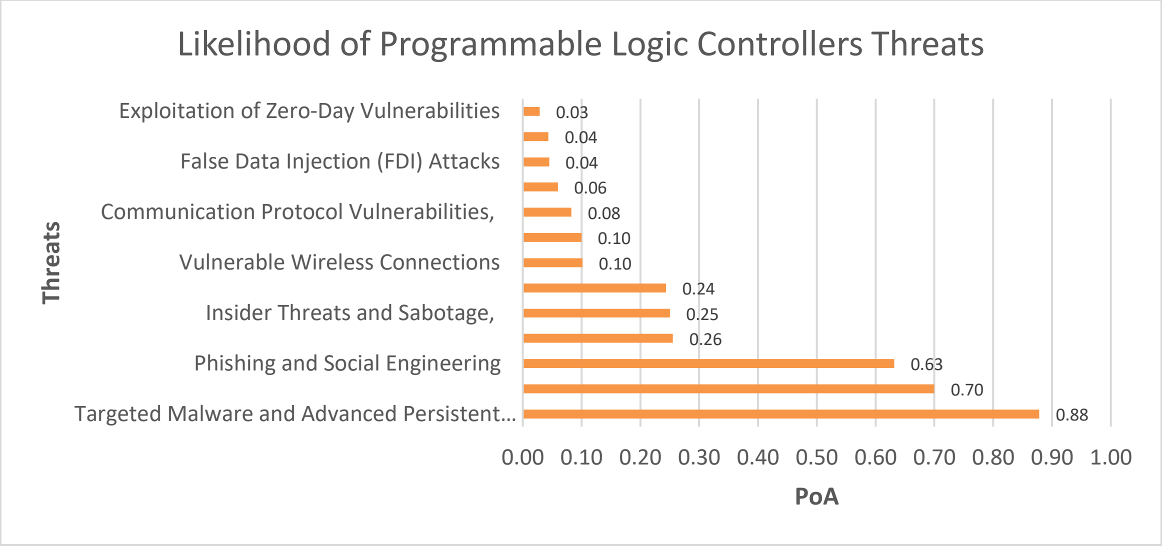

Figure 18: Likelihood of Programmable Logic Controllers Threats

Figure 19 presents the data on the Likelihood of Remote Terminal Units (RTUs) Threats. There are 15 threats identified in this asset. 2 of these threats are in the almost certain and possible categories each; 2 are in the possible and unlikely category each while the remaining 7 are in the rare category.

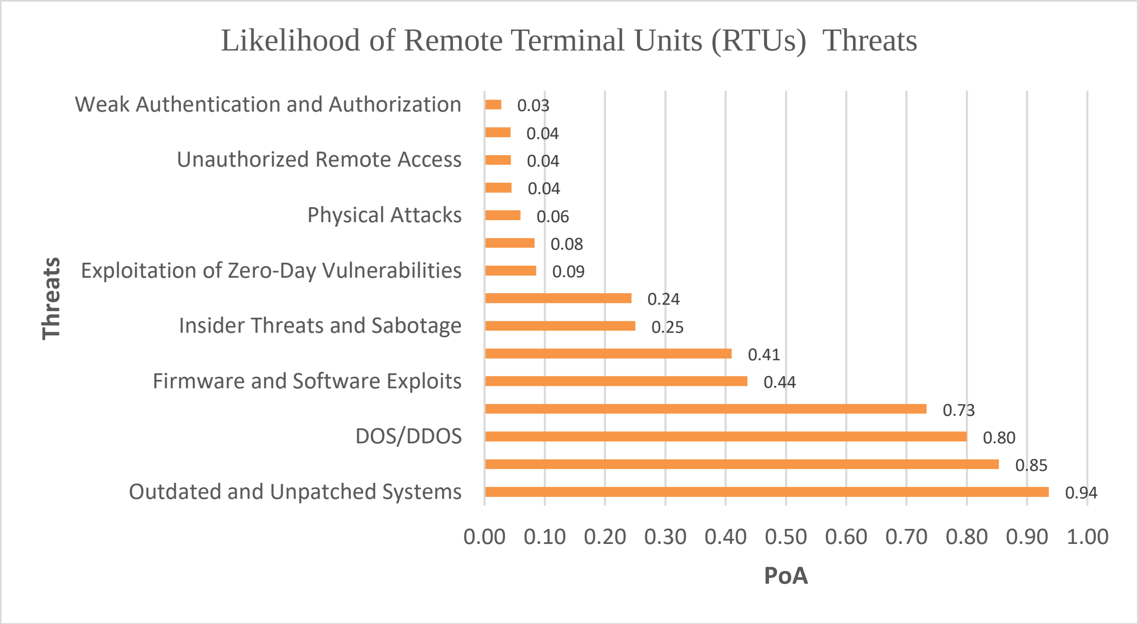

Figure 19: Likelihood of Remote Terminal Units (RTUs) Threats

Figure 20, the data for likelihood of Wide Area Networks (WANs) threats. The asset has 9 identified threats, 2 of these falls within the almost certain classification, 1 is in the likely category; 3 in the possible category, 1 is in the unlikely category and the remaining 2 are in the rare category.

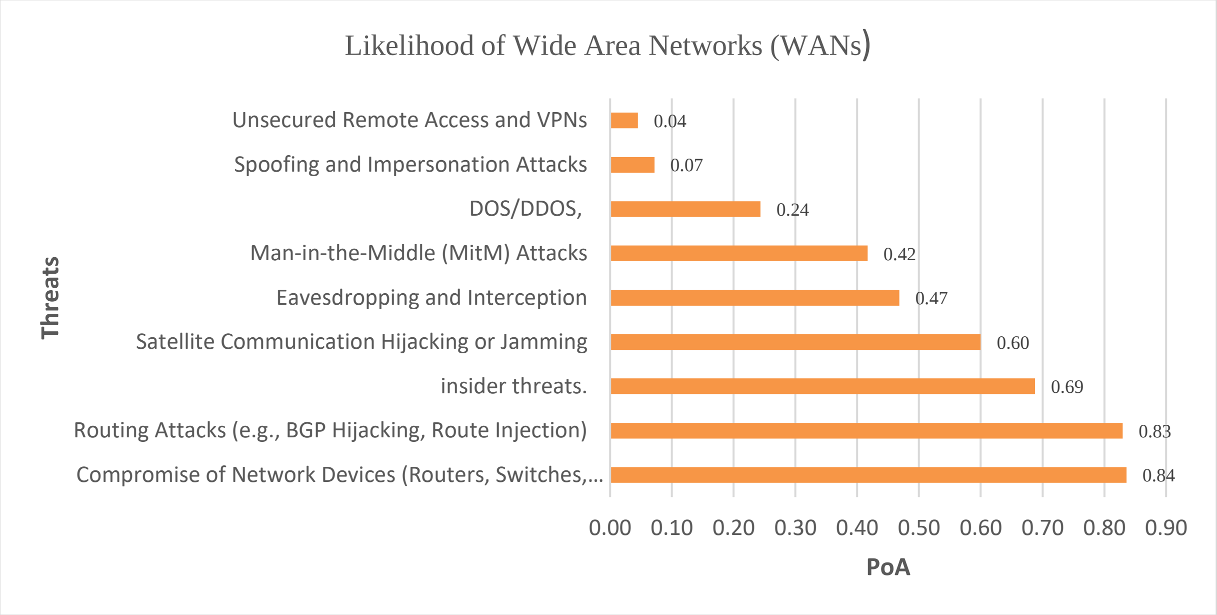

Figure 20: Likelihood of Wide Area Networks (WANs)

Figure 21, is the data about Likelihood of Data Acquisition Servers threats, this asset has 9 identified threats, 3 of these threats are in the likely and possible and bands respectfully, 1 is in the unlikely category and the remaining 2 are in the rare category.

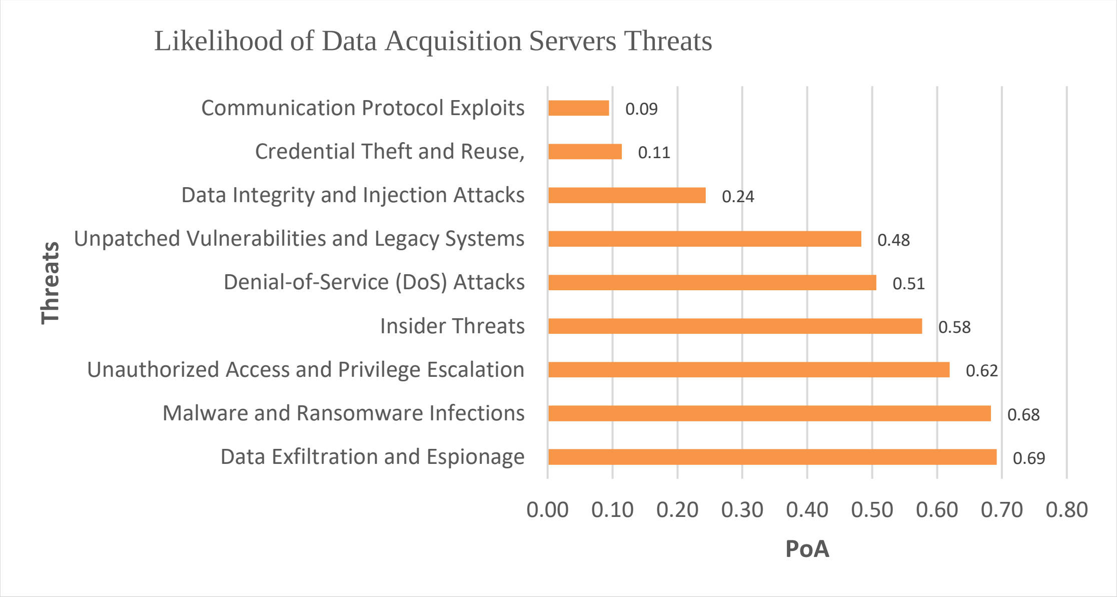

Figure 21: Likelihood of Data Acquisition Servers Threats

Figure 22 presents data on Likelihood of Advanced Metering Infrastructure (AMI) Threats, this asset has 4 identified threats, 1 of these is in the almost certain category, 2 in the likely category and 1 in the possible category.

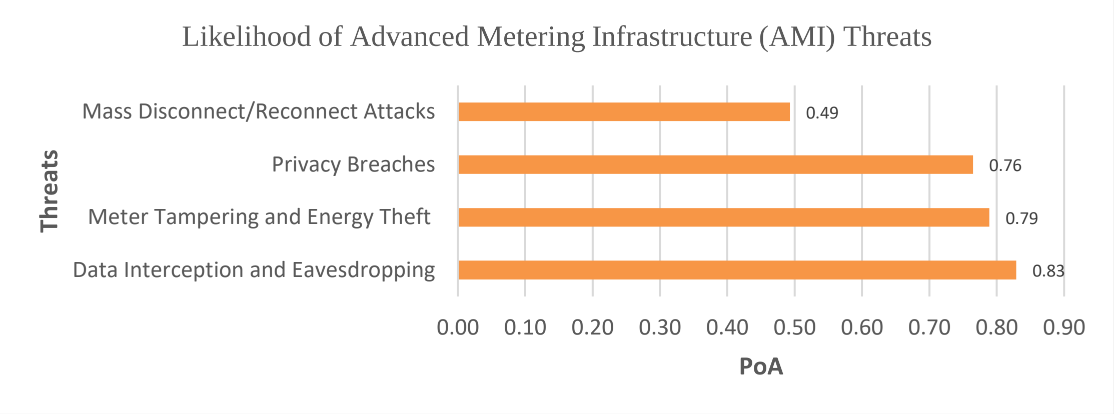

Figure 22: Likelihood of Advanced Metering Infrastructure (AMI) Threats

Threat-Vulnerability-Asset (TVA) Analysis

The purpose of a Threat-Vulnerability-Asset (TVA) analysis in threat assessment is to systematically identify, evaluate, and prioritize risks by mapping threats to specific vulnerabilities and critical assets within an organization's infrastructure. By assessing the impact (potential damage) and likelihood (probability of occurrence) of each threat, the TVA framework calculates a risk score to determine which vulnerabilities require immediate mitigation. This structured approach helps organizations allocate resources efficiently, strengthen security postures, and develop targeted defense strategies—particularly in critical systems like SCADA, energy grids, or industrial networks—where disruptions could have severe consequences. Ultimately, TVA enables proactive risk management by highlighting the most significant threats and guiding decision-makers in implementing effective countermeasures. Thus, Table 10 presents the TVA based on data generated from the impact and likelihood analysis from Figure 1 – 22.

Table 10: Threat-Vulnerability-Asset (TVA) Analysis

Asset Category	**Threats**	**Impact**	**Likelihood**	**Risk Rating**
Generation and Transmission Control Systems	Targeted Malware and Advanced Persistent Threats (APTs)	0.95	0.83	0.79
	Communication Protocol Vulnerabilities	0.85	0.37	0.31
SCADA Systems	Targeted Malware and Advanced Persistent Threats (APTs)	1.00	0.89	0.89
	Targeted Malware and Advanced Persistent Threats (APTs)	0.90	0.84	0.76
Backup Power and Redundancy Systems	Denial-of-Service (DoS) and Load Manipulation Attacks	0.95	0.80	0.76
Intelligent Electronic Devices (IEDs)	Time Synchronization Attacks	0.95	0.12	0.11
	Protocol-Based Exploits (IEC 61850, DNP3, Modbus)	0.85	0.24	0.20
Substation Automation Systems	Insecure Protocols (e.g., IEC 61850, DNP3,	0.85	0.72	0.61

Asset Category	**Threats**	**Impact**	**Likelihood**	**Risk Rating**
	Modbus)			
Programmable Logic Controllers (PLCs)	Outdated and Unpatched Systems	0.90	0.26	0.23
	Targeted Malware and Advanced Persistent Threats (APTs)	0.85	0.88	0.75
Remote Terminal Units (RTUs)	DOS/DDOS	0.95	0.80	0.76
	Targeted Malware and Advanced Persistent Threats (APTs)	0.85	0.85	0.72
Wide Area Networks (WANs)	Routing Attacks (e.g., BGP Hijacking, Route Injection)	0.95	0.83	0.79
	Eavesdropping and Interception	0.85	0.47	0.40
	Compromise of Network Devices (Routers, Switches, Modems)	0.85	0.84	0.71
Data Acquisition Servers	Denial-of-Service (DoS) Attacks	0.95	0.51	0.48
	Unpatched Vulnerabilities and Legacy Systems	0.90	0.48	0.43
	Unauthorized Access and Privilege Escalation	0.85	0.62	0.53
Advanced Metering Infrastructure (AMI)	Data Interception and Eavesdropping	0.95	0.83	0.79
	Privacy Breaches	0.85	0.76	0.65

Based on the analysis in Table10, targeted malware and APTs on SCADA systems present the highest risk with a risk rating of 0.89. This is besides the fact that SCADA systems control industrial operations, and APTs can cause widespread disruption. The high impact 0f 1.00 and likelihood (0.89) make this the top-priority threat. This is followed by Wide Area Networks (WANs) with Routing Attacks (BGP Hijacking) threat presenting a risk score of 0.79. a compromised routing can redirect or block traffic, crippling communication. High impact (0.95) and likelihood (0.83) on this threat indicate severe operational risks. Similarly, Advanced Metering Infrastructure (AMI) – Data Interception (Risk: 0.79). this has potentials for sensitive consumer data exposure (e.g., energy usage) has high impact (0.95) and likelihood (0.83), posing privacy and compliance risks. Generation/Transmission Systems & RTUs – Targeted Malware/APTs & DoS (Risk: 0.76–0.79) Attacks on these systems can destabilize power grids. DoS on RTUs (Risk: 0.76) and APTs on control systems (Risk: 0.79) are significant. Data Acquisition Servers – Unauthorized Access/Privilege Escalation (Risk: 0.53). Breaches here can lead to data manipulation or theft, with moderate likelihood (0.62) but high impact (0.85).

Conclusion and Future Work

This study successfully developed and applied a structured TVA framework to assess cybersecurity threats in the Nigerian power sector. The findings highlight an alarming vulnerability to high-impact cyber-attacks, with SCADA systems, WANs, and AMI being prime targets. The convergence of high-impact and high-likelihood threats, such as APTs and routing attacks, underscores an urgent need for proactive and targeted risk mitigation. This research contributes a novel, tailored TVA framework for cybersecurity assessment in the context of an emerging energy market. It provides an empirical, data-driven prioritization of threats specific to Nigeria's power infrastructure, moving beyond generic risk models to offer actionable insights for policymakers and utility operators. Subsequent research should focus on validating the proposed framework through real-time cyber-attack simulations and penetration testing in a live grid environment. Further studies could explore the socio-technical barriers to implementing cybersecurity measures in Nigeria, conduct cost-benefit analyses of proposed mitigations, and investigate the application of emerging technologies like blockchain for securing grid communications. Longitudinal studies are also needed to assess the evolution of these cyber risks over time.

REFERENCES

Achuama, D. (2024). Addressing the digital resilience challenge in the electricity sector in Nigeria: From risk to resilience. In *Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024)* (pp. 17–25). Academic Conferences International.

African Development Bank Group. (2024, October 24). *Estimating investment needs for the power sector in Africa 2023–2030 – Africa report*. https://www.afdb.org/en/documents/estimating-investment-needs-power-sector-africa-2023-2030-africa-report

Alese, B. K., Thompson, A. F., Owa, K. V., Iyare, O., & Adebayo, O. T. (2014). Analysing issues of cyber threats in Nigeria. In *Proceedings of the World Congress on Engineering 2014 Vol I* (pp. 1–6).

Awosope, C. A. (2014). *Nigeria electricity industry: Issues, challenges and solutions*. Covenant University Public Lecture.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

European Union Agency for Cybersecurity (ENISA). (2020). *Risk assessment methodologies for critical infrastructure protection*. https://www.enisa.europa.eu

Fallahi, F., Yildirim, M., Zhao, S., & Qiu, F. (2025, April 21). *A sensor-driven optimization framework for asset management in energy systems: Implications for full and partial digital transformation in hydro fleets*. arXiv. https://arxiv.org/abs/2504.15483

Ibanga, A., Fwah, E., & Idowu, A. (2024). Assessing the vulnerabilities: Cybersecurity challenges in power system infrastructure in Nigeria. *International Journal of Information Technology and Cybersecurity*, 4(2), 45–58.

Kumar, et al. (2015). Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. [Journal Title], Volume, [Page range].

Madurasinghe, D., & Venayagamoorthy, G. K. (2022, July 12). *Identification of substation configurations in modern power systems using artificial intelligence*. arXiv. https://arxiv.org/abs/2207.05603

National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments* (Special Publication 800-30, Revision 1). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Ngoma, S. (2018). Nigerian Electricity Regulatory Commission (NERC). (2024). *NERC annual report 2023*. https://nerc.gov.ng/resources/nerc-annual-report-2023/

North American Electric Reliability Corporation (NERC). (2023). *Critical Infrastructure Protection (CIP) standards*. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Ogundari, I. O., & Otuyemi, O. (2019). [Title of work]. In [Editor(s)], *[Book Title]* (pp. [Page range]). Publisher.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.

Ugboke, F. E., Ogunjimi, J. A., & Eze, C. I. (2024). Impacts of digitization in the technological shift of power industry. *NIPES Journal of Engineering and Technology*, 6(1), 112–124.6

Wresearch. (2023, July). *Nigeria utility asset management market (2024–2030) outlook: Trends, value, growth, forecast, revenue, size, companies, analysis, industry & share*. https://www.6wresearch.com/industry-report/nigeria-utility-asset-management-market

Nigerian Electricity Regulatory Commission. (2024, September 23). *NERC annual report 2023*. https://nerc.gov.ng/resources/nerc-annual-report-2023/