International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 14 Issue 4 ǁ April 2026 ǁ PP. 184-186

Cybersecurity Threat Detection for ICT Infrastructure in Nigeria's 33kv Distribution Network: A Case Study of PHED

Ifeanyi Chukwuma Aginam, Eseosa omorogiuwa
Centre for Information and Telecommunication Engineering (CITE), University of Port Harcourt, Rivers State, Nigeria

Abstract
When Nigeria's power grid started relying more on ICT, operations got a lot smoother. But let's be real cyber risks shot up too. This study takes a hard look at how to spot those cybersecurity threats in the 33kv distribution network, zeroing in on the Port Harcourt Electricity Distribution Company (PHED). I dug in with a hands-on approach vulnerability assessment, system log dives, threat modeling, and just watching how the ICT and SCADA parts behave in the real world. I gathered primary data from on-site tests and vulnerability scans, and backed those up with technical documents, standards, and what's already out there in the literature. For the tricky partactually finding and sorting the threats I went with heavy hitters like OpenVAS/Greenbone, STRIDE, and the MITRE ATT&CK framework for industrial systems. Here's what turned up: a bunch of major issues, including old firmware, weak authentication, poor network segmentation, and not enough real-time monitoring. When you put the usual antivirus methods against a more layered detection setup, the old way misses a lot especially the advanced threats. So what helps? Defense-in-depth makes a difference, as do centralized monitoring, regular staff training, and clear, policy-driven cybersecurity rules. All of this isn't just theory. These findings help fill in the gaps for Nigeria's power sector and offer practical steps to actually protect these essential networks. Keywords: Cybersecurity, 33kv Distribution Network, SCADA, Threat Detection, PHED, Critical Infrastructure

Keywords
Cybersecurity, Threat Detection, SCADA, 33kV Distribution Network, ICT Infrastructure, Smart Grid, Nigeria

---

Date of Submission: 12-04-2026 Date of Acceptance: 26-04-2026

I. INTRODUCTION

1. Introduction Electric power distribution networks now lean heavily on Information and Communication Technology (ICT) and SCADA systems to keep things running smoothly. Nigeria's 33kv distribution networks have gotten a real upgrade from these tools service is better, operations are more efficient but all this progress comes with a downside. As things get more connected, the risk of cyber-attacks on critical infrastructure grows. Bringing old operational technology together with new ICT has left Nigerian utilities more exposed to cyber threats that could cause outages, damage equipment, hurt the bottom line, or even endanger public safety. Yet, despite how vital these networks are, most utilities here still tend to play defense relying on firewalls and antivirus software. That kind of approach just doesn't cut it against today's advanced and persistent threats. This study steps in to close that gap. It looks closely at how cyber threats are detected in the PHED 33kv distribution network and offers practical improvements, rooted in international best practices like IEC 62443, NIST SP 800-82, and the MITRE ATT&CK framework for industrial control systems.

2. Related Work People have been ringing the alarm about how vulnerable modern power systems are getting, especially now that old-school electrical grids are tied up with new information and communication tech. A lot of researchers point out that power distribution networks in places like developing countries are running on outdated gear and shoestring budgets. That means their cybersecurity just can't keep up with the speed and tricks of new cyber threats. So, these critical systems end up open to things like service outages, data tampering, or just plain unauthorized access. A bunch of studies say you can't just slap standard IT security tools onto industrial control systems or the operational tech that runs power networks. The rules are different. Industrial environments need everything to work in real time, all the time, and they use communication protocols that weren't built with security in mind. Stuff like firewalls and antivirus programs from the corporate world? They mostly miss the mark when it comes to catching or stopping the kind of attacks that go after SCADA systems or the guts of power networks. To deal with all this, the industry's rolled out several standards and frameworks. You've got things like the Purdue Enterprise Reference Architecture, which basically slices up networks between IT and OT systems,

IEC 62443 for security in automation and control systems, and NERC CIP standards aimed at keeping big electric systems safe. These frameworks try to lay out the best ways to handle things like access, network segmentation, monitoring, and how to respond when things go wrong. But here's the thing: even though these standards look great on paper and get cited all the time, hardly anyone's actually dug into how well they work in places like Nigeria. Most of what's out there talks about power systems in richer countries, where money, tech, and rules aren't such a hurdle. So there's this glaring hole in the research when it comes to what's really going on with cybersecurity in Nigerian power distribution especially at the 33kv level. That's where this study comes in. We dig into threat detection in a real Nigerian 33kv distribution network the PHED 33kv network. By looking at actual setups, vulnerabilities, and what the detection systems catch, this research gives some real, on-the-ground insight into the cybersecurity headaches Nigerian power companies deal with. It also shows why these companies need security solutions that actually fit their world, not just copy-pasted standards from somewhere else.

3. Methodology To really get under the hood, this study uses a case study approach, zeroing in on the PHED 33kv distribution network pretty much the way researchers tackle critical infrastructure cybersecurity elsewhere. The focus: ICT and SCADA assets like substations, network devices, servers, communication links, and the workstations operators use every day. For data, the team ran controlled vulnerability scans using OpenVAS/Greenbone, sifted through system and network logs following SIEM principles, and took a direct look at the physical and logical security controls in place. To map out the threats, they used both STRIDE and the MITRE ATT&CK framework for ICS, linking what they found to known tactics and techniques. They also pulled in technical documents from PHED and international standards for context. To make sure the results were solid, they repeated tests, cross-checked findings, and stuck to standard tools and procedures.

4. Results and Discussion The findings paint a pretty clear picture: cybersecurity gaps run throughout the PHED 33kv ICT setup. There are old systems running outdated firmware, open network services, weak or even default passwords, and barely any separation between IT and OT networks. None of this is unique other studies have spotted the same issues in power distribution networks. Looking at the logs, the team saw signs of trouble: lots of failed login attempts, strange network traffic classic signs of people poking around or trying brute-force attacks. When they mapped this stuff onto the MITRE ATT&CK framework, it was obvious the network was open to attacks at every stage: from initial access and privilege escalation, all the way to lateral movement and command-and-control. And the usual defenses just aren't keeping up. Antivirus software, on its own, missed most of the advanced threats something other research has pointed out time and again. Signature-based security just doesn't stand up in industrial environments like this.

5. Recommendations The findings here make one thing clear: Nigeria's power sector needs a solid, multi-layered cybersecurity strategy to really protect its power distribution infrastructure. And not just any plan it should stick to big-name standards like IEC 62443 for industrial control security and NIST's guidelines for securing these systems (IEC, 2018; NIST, 2015). With these frameworks, power companies can put real structure into place, covering both IT and OT environments. To catch and deal with threats faster, power utilities should roll out centralized monitoring tools think Security Information and Event Management (SIEM) systems and intrusion detection. These tools watch everything in real time, connect the dots between suspicious activities, and flag problems right away. On top of that, companies need to lock down access. Set up strict, role-based policies, use strong authentication, and regularly check who has what privileges. Regular vulnerability assessments and security audits also matter they help find and fix weak spots before attackers do, making the whole system tougher (NERC, 2022). Cybersecurity training shouldn't be a one-off thing. It needs to happen all the time. Technical staff network admins, engineers, system operators all need regular updates on new threats, how to keep systems locked down, and how to respond when something goes wrong. Ongoing professional development keeps everyone sharp and ready to handle incidents quickly and effectively. But the focus can't just stay inside the company. Cybersecurity has to stretch to the supply chain too. Power distribution companies should bake cybersecurity requirements into how they buy equipment and manage vendors. Anyone involved third-party service providers, contractors, equipment suppliers should have to meet defined security standards. This cuts down on supply-chain risks and insider threats, which are real gateways for cyberattacks on critical infrastructure (Behl & Behl, 2017). Put all these steps together, and Nigeria's power sector becomes a lot tougher. Stronger governance, better threat detection, and a faster response all lead to more reliable and resilient power distribution networks.

6. Conclusion This research makes one thing obvious: Nigeria's 33kv power distribution networks have serious cybersecurity problems, and old-school security just doesn't cut it anymore. By using structured threat detection and analysis on the PHED 33kV network, the study digs into real-world vulnerabilities and offers practical fixes. These results back up what experts are saying globally about critical infrastructure defenses need to be proactive, smart, and custom-fit for how power systems actually run (Alcaraz & Zeadally, 2015; MITRE, 2023). If you

follow this approach, you boost readiness and resilience, stay more aware of what's happening on your network, and help keep Nigeria's power infrastructure safe and reliable.

References

[1]. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53–66. Behl, A., & Behl, K. (2017).

[2]. Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems.

[3]. Computers & Security, 56, 1–27. Humayed, A., Lin, J., Li, F., & Luo, B. (2017).

[4]. Cyber-physical systems security A survey. IEEE Internet of Things Journal, 4(6), 1802–1831.

[5]. International Electrotechnical Commission (IEC). (2018). IEC 62443: Industrial communication networks – Network and system security.

[6]. IEC. MITRE Corporation. (2023). MITRE ATT&CK® for Industrial Control Systems (ICS). MITRE.

[7]. National Institute of Standards and Technology (NIST). (2015). Guide to Industrial Control Systems (ICS) Security (SP 800-82 Rev. 2).

[8]. NIST. North American Electric Reliability Corporation (NERC). (2022). Critical Infrastructure Protection (CIP) Standards. NERC.

[9]. Open Vulnerability Assessment System (OpenVAS). (2023). Greenbone Vulnerability Management Documentation. Greenbone Networks.

[10]. Port Harcourt Electricity Distribution Company (PHED). (2024). Technical and Operational Documentation on 33kV Distribution Network. PHED.

[11]. Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82.

[12]. Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling.

[13]. IEEE Transactions on Systems, Man, and Cybernetics, 40(4), 853–865. Zhang, Y., Wang, L., Sun, W., Green, R. C., & Alam, M. (2018).

[14]. Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid, 2(4), 796–808.