IKR Publishers

IKR Journal of Multidisciplinary Studies (IKRJMS)
Journal homepage: https://ikrpublishers.com/ikrjms/
Volume-2, Issue-4 (July-August) 2026
OPEN ACCESS
ISSN: 3107-3999 (Online)

Cyber-Physical Security of Renewable Energy Microgrids: A State-of-the-Art Review of Threats, Standards and Research Gaps for Sub-Sahara Africa

Ezirim Kelechi ThankGod[1*], Aniugo Victor Onyekachi[2], Sani Abubakar Muhammed[3], Nwaokolo Ikechukwu Frank[4], Obi Obichukwu Immanuel[5], Okoronkwo Iheanyi Chinedu[6] & Aminu Momoh[7]

[1,2,3,4,5,6]Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

[7]Transmission Company of Nigeria, Akangba Sub-Region, Lagos State, Nigeria

DOI:*10.5281/zenodo.21863709*

ARTICLE INFO

Article history:
Received : 15-07-2026
Accepted : 24-07-2026
Available online : 09-08-2026

Citation: Ezirim, K. T., Aniugo, V. O., Sani, A. M., Nwaokolo, I. F., Obi, O. I., Okoronkwo, I. C., & Aminu, M. (2026). Cyber-Physical Security of Renewable Energy Microgrids: A State-of-the-Art Review of Threats, Standards and Research Gaps for Sub-Sahara Africa. *IKR Journal of Multidisciplinary Studies (IKRJMS), 2*(4), 31-34.

ABSTRACT **Review Article**

Renewable energy microgrids are critical particularly to rural electrification and energy- access in Sub-Saharan Africa (SSA), where well over 600 million people lack reliable power (IEA, 2023). These cyber-physical systems integrate solar, wind, storage, and Supervisory Control and Data Acquisition (SCADA) control, making them vulnerable to both cyber and physical attacks. This review examines the current threat landscape, existing standards, and research gaps for securing renewable microgrids in Sub -Sahara Africa. We examined 61 studies from 2017-2025 and found that SSA microgrids face rather very unique risks like legacy devices, poor connectivity, insider threats, and limited incident response capacity. While standards like IEC 62443 and NIST CSF exist, adoption in SSA is still relatively low due to cost and skills gaps. We propose a context-aware security framework combining lightweight cyber defenses, physical hardening, and community governance. Future and prospective research need to prioritize low-cost intrusion detection, secure protocols for low-bandwidth links, and policy alignment with national energy strategies.

Keywords: Cyber-Physical Security, Microgrid, Renewable Energy, SCADA, Sub-Saharan Africa, IEC 62443.

**Corresponding author: Ezirim Kelechi ThankGod*
Mechatronics Engineering Department; Federal University of Technology, Owerri, Imo State, Nigeria

Introduction

Energy access is the cornerstone of development, industrialization and civilization in Sub-Saharan Africa. Decentralized renewable microgrids powered by solar PV, wind, biofuel, geothermal and battery storage are being deployed to serve rural and peri-urban communities (Tenenbaum et al., 2014). Unlike centralized grids, microgrids rely heavily on ICT for monitoring, control, and payment, making them Cyber-Physical Systems (CPS) (Cárdenas et al., 2008).

This convergence as expected creates new vulnerabilities. A cyberattack on a microgrid inverter or battery management system can cause blackouts, associated losses, equipment damage, or safety hazards (Deng et al., 2011). On the other hand, Kuznetsov et al. (2020) maintain that a physical attack on panels or fences can disable generation as well In Sub -

Saharan Africa, these risks are amplified by harsh socio-economic environments, limited cybersecurity expertise, and reliance on imported equipment with default passwords.

Wang et al., (2022) argue that despite rapid deployment, literature on microgrid Cyber - Physical Systems (CPS) security has focused on developed nations and large utilities.

Indeed, Standards such as IEC 62443 and NIST SP 800-82 do exist, but their applicability to low-resource, off-grid contexts still remains vague and unclear (ISA, 2018; NIST, 2018).

This paper reviews among other things:

1. Threats to renewable microgrid Cyber-Physical Systems in Sub -Saharan Africa;
2. Applicable standards and frameworks; and
3. Research and policy gaps.

The aim is to provide informed guidance to researchers, developers, and policymakers toward secure and equitable energy access.

Literature Review

Renewable Microgrids in Sub-Saharan Africa

It's been established that Sub-Saharan Africa (SSA) has seen more than 5,000 solar microgrids installed since 2015, largely by private developers and NGOs (ESMAP, 2022). Typical architecture includes: PV arrays, battery ESS, diesel backup, smart meters, and a central controller with 3G/4G or VSAT backhaul. The Supervisory Control and Data Acquisition (SCADA) Control protocols like Modbus and DNP3 are relatively common in the region as well (East et al., 2009).

Cyber-Physical Threats

The intimidating Cyber Physical Systems (CPS) threats span across two domains:

1. **Cyber:** Man-in-the-middle, ransom ware, false data injection, and firmware tampering (Giani et al., 2013).
2. **Physical:** Theft of panels, vandalism, weather damage, and insider sabotage (Nkosi & Bagula, 2021).

Attackers may target payment systems to steal revenue or disrupt clinics and schools or other essential services that may threaten life on itself (Akinyele et al., 2022).

Standards and Frameworks

Key standards: IEC 62443 for ICS security (ISA, 2018), NIST Cybersecurity Framework (NIST, 2018), ISO/IEC 27001 for ISMS, and IEEE 2030.7 for microgrid control. However, compliance testing is quite expensive and requires expertise rarely available in Sub -Saharan Africa (Oyewole et al., 2021).

Context of Sub-Saharan Africa

Specific and Peculiar challenges with SSA include: Intermittent internet, power quality issues, low digital literacy, and weak regulatory enforcement (Adenle, 2020). Most operators are Small and Medium Enterprises (SMEs) with no dedicated Chief Information Security Officers (CISO).

Methodology

This state-of-the-art review used structured literature search across notable sources with specific Search terms carefully recognizing Inclusion and Exclusion Concepts.

Results

Threat Landscape

Most reported incidents in Sub -Saharan Africa microgrids are physical: theft of batteries and panels (Nkosi & Bagula, 2021). Documented cyber incidents are rare but obviously underreported. Simulated attacks show vulnerabilities: unencrypted Modbus traffic, weak authentication on web portals, and exposed cloud dashboards (Fawaz et al., 2022).

Standards Adoption

Only 12% of surveyed Sub -Saharan Africa developers reported awareness of IEC 62443 (ESMAP, 2022). NIST CSF is used informally by larger IPPs with donor funding. Most rely on vendor best practices.

Defense Mechanisms in Literature

Proposed defenses include but not limited to anomaly detection for smart meter data (Zhang & Qi, 2019), blockchain for peer-to-peer trading (Mengelkamp et al., 2018), and physical security like CCTV and community watch (Adenle, 2020). Ironically only very few are tested in SSA field conditions.

Deductions

1. **Dual Exposure:** Microgrids are exposed to both cyber and physical threats, but defenses address them separately.
2. **Standards Mismatch:** Global standards assume high connectivity and budget. They are not fit-for-purpose in Sub -Saharan Africa at the very moment.
3. **Data Gap:** Lack of incident reporting prevents risk quantification.
4. **Human Factor:** Community ownership reduces vandalism but can increase insider risk.

Discussion

The findings show a clear mismatch between global Cyber-Physical Systems (CPS) security practice and what is obtainable in Sub-Saharan Africa reality. While developed countries deploy AI-based IDS and SOCs, SSA microgrids often run on Raspberry Pi controllers with no patching (Kuznetsov et al., 2020).

Three critical issues that need attention are:

1. **Connectivity:** cloud-based security monitoring fails when 3G drops. Edge-based, lightweight detection is needed.
2. **Affordability:** A full IEC 62443 audit can cost more than the microgrid itself. Tiered, risk-based compliance is needed.
3. **Governance:** many microgrids are community-owned. Security must include social mechanisms, not just tech alone. (Tenenbaum et al., 2014).

This aligns with literature on critical infrastructure in developing economies (Amin et al., 2013), but extends to the decentralized, renewable context.

Gaps and Future Targets

The under listed suggestions are proactive to bridge the obvious gaps so far observed from the present system:

1. **Low-cost, Offline Intrusion Detection System (IDS):** Adopt Machine learning models that run on edge devices with less than <1GB RAM.
2. **Secure Low-Bandwidth Protocols:** Lightweight encryption for Modbus over 2G/3G.
3. **Sub Sahara Africa-Specific Threat Database:** To capture real incidents and attack patterns peculiar to SSA region.
4. **Standards Localization:** Adapt IEC 62443 with SSA cost and skills constraints.
5. **Cyber-Physical Co-simulation:** Engage Testbeds that model both cyberattacks and physical damage like floods or theft.

Recommendations

The review put forth the following recommendations based on overall review analysis to major stakeholders:

For developers and operators:

1. **Security by Design:** Change default passwords, segment OT/IT networks, and enable logging even offline.
2. **Physical Hardening:** Tamper-proof enclosures, GPS tracking for batteries, and community engagement.

For policymakers:

3. **National Microgrid Security Guidelines:** Simplified version of IEC 62443 for rural systems should be in place.
4. **Capacity Building:** Partner with universities to train local technicians in CPS security.
5. **Incident Reporting Mandate:** Provide for Anonymous reporting to a regional energy ISAC.

For researchers:

1. **Field Pilots:** Test defenses in real SSA microgrids, not just simulation alone.
2. **Interdisciplinary Work:** Combine engineering, social science, and policy to encourage multidisciplinary research.

Conclusion

Cyber-physical security of renewable energy microgrids is essential for sustainable electrification in Sub-Saharan Africa and particularly in the rural areas. Present threats have been discovered to be both digital and physical, and existing standards are not fully aligned with SSA constraints. Bridging this gap requires lightweight technology, localized standards, and community-centered governance. Without action, the push for clean energy may inadvertently create a new class of vulnerable infrastructure added to the challenges of inadequate energy access it was about to solve.

References

1. Adenle, A. A. (2020). Assessment of solar energy technologies in Africa. Renewable and Sustainable Energy Reviews, 131, 110018.
2. Akinyele, D., Olabode, E., & Ajewole, T. (2022). Cybersecurity challenges in African power systems. International Journal of Electrical Power, 138, 107841.
3. Amin, S., Cárdenas, A. A., & Sastry, S. S. (2013). Safe and secure networked control systems under denial-of-service attacks. IEEE Transactions on Automatic Control, 58(3), 563–576.
4. Cárdenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2008). Challenges for securing cyber physical systems. Workshop on Future Directions in Cyber-physical Systems Security, 1–7.
5. Deng, R., Zhuang, P., & Liang, H. (2011). CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. IEEE Transactions on Smart Grid, 2(4), 724–735.
6. East, S., Butts, J., Papa, M., & Shenoi, S. (2009). A taxonomy of attacks on the DNP3 protocol. Critical Infrastructure Protection III, 47–58.
7. ESMAP. (2022). Mini grids for half a billion people: Market outlook and handbook for decision makers. World Bank.
8. Fawaz, N., Atienza, D., & Giannakis, G. B. (2022). Data poisoning attacks on smart grid load forecasting. IEEE Transactions on Information Forensics and Security, 17, 1202–1214.
9. Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., & Poolla, K. (2013). Smart grid data integrity attacks. IEEE Transactions on Smart Grid, 4(3), 1244–1253.
10. IEA. (2023). Africa Energy Outlook 2023. International Energy Agency.
11. ISA. (2018). _IEC 62443: Security for industrial automation and control systems_. International Society of Automation.

12. Kuznetsov, V., Escamilla-Ambrosio, P. J., & Giannetsos, T. (2020). A review of cybersecurity challenges in smart grids in developing countries. Energies, 13(17), 4542.
13. Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets. Applied Energy, 210, 870–880.
14. NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.
15. Nkosi, N., & Bagula, A. (2021). Physical security threats to renewable energy infrastructure in South Africa. Energy Policy, 149, 112058.
16. Oyewole, O., Ogunwuyi, O., & Adeyemi, B. (2021). Cybersecurity readiness in Sub-Saharan African energy sector. Energy Policy, 156, 112439.
17. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev 2). NIST.
18. Tenenbaum, B., Greacen, C., Siyambalapitiya, T., & Knuckles, J. (2014). From the sun to the grid: The role of solar mini-grids in sub-Saharan Africa. World Bank.
19. Wang, Y., Yang, Q., & An, D. (2022). A survey on adversarial attacks and defenses in smart grid. IEEE Communications Surveys & Tutorials, 24(2), 1210–1234.
20. Zhang, M., & Qi, H. (2019). Anomaly detection using autoencoders for SCADA systems. Applied Sciences, 9(21), 4653.