Academic World
Journal of Scientific and Engineering Innovation
Journal homepage
https://academicworldpublisher.co.uk/index.php/awjsei

Cyber-Physical Systems for Enhancing Security in Critical Infrastructure: Addressing Nigeria's Security Challenges

Engr. Eduediuyai D. Ekerete
Department of Computer Engineering Technology, Federal Polytechnic Ukana,
Akwa Ibom State

ABSTRACT- ***Cyber-Physical Systems (CPS) are increasingly central to the operation of critical infrastructure, particularly in emerging economies where digital transformation is accelerating amid limited cybersecurity maturity. This study proposes and validates a context-specific, multi-layered CPS security and resilience framework tailored to Nigeria's infrastructural realities. The framework integrates architectural segmentation (based on the Purdue Model), AI-driven anomaly detection using Long Short-Term Memory (LSTM) networks, and resilience engineering practices such as automated failover and safe-state recovery. Using a simulation testbed emulating smart grid and campus energy systems, the framework was benchmarked against traditional and AI-only detection baselines. Results show that the hybrid architecture improves detection accuracy to 97.8%, reduces false positives to under 1%, and decreases Mean Time to Recovery (MTTR) from 7.8 to 1.9 hours. Downtime was reduced by 88.9%, and cost-benefit analysis revealed a 133% return on investment (ROI) within the first year. These gains were validated through historical event logs and economic modeling using avoided-loss estimation. This framework offers a deployable roadmap for enhancing national cyber resilience in resource-constrained settings by combining advanced control algorithms, layered defense principles, and contextual policy alignment. It is particularly relevant to sectors like education, energy, and industrial automation, where CPS integration is outpacing security governance. The findings emphasize that a tailored, resilience-by-design approach rooted in real-time analytics and system containment can substantially improve operational continuity and economic sustainability for critical infrastructure operators.***

Keywords: *Cyber-Physical Systems, Critical Infrastructure, Anomaly Detection, AI Security, ICS Resilience, Purdue Model, MTTR, Nigeria.*

I. INTRODUCTION

Cyber-Physical Systems (CPS) represent the fusion of computational algorithms with physical components to enable real-time monitoring, control, and automation across critical infrastructure domains such as energy, transportation, water systems, education, and defense. With increasing digitization, CPS have become indispensable to national infrastructure resilience. However, this integration has introduced a new set of vulnerabilities that transcend traditional cybersecurity, leading to the emergence of cyber-physical threats capable of causing both virtual and physical harm (Lee et al., 2019; Chadha et al., 2023).

The theoretical basis for CPS security includes system resilience theory (Hollnagel et al., 2011), control system survivability (Amin et al., 2013), and layered defense-in-depth frameworks like the Purdue Model (Claroty, 2023; Stouffer et al., 2015). These frameworks suggest that security must be embedded at every level—from field devices to enterprise systems—through segmentation, anomaly detection, and safe-state fallback. Empirical studies confirm that most legacy Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Programmable Logic Controllers (PLCs) were not originally designed with cyber resilience in mind, resulting in exploitable gaps such as hardcoded passwords, lack of encryption, and flat network architectures (Zetter, 2016; NIST, 2018).

Recent global incidents provide empirical validation of these theoretical concerns. The Stuxnet worm (2010) demonstrated how malware could physically sabotage critical assets by reprogramming PLCs. More recently, the 2015 Ukraine

blackout and Triton malware attacks in 2017 targeted energy systems, showcasing the potential for adversaries to disrupt societal functions through cyber-physical vectors (CISA, 2016; Trend Micro, 2019). In emerging economies, these risks are amplified by outdated systems, limited cybersecurity expertise, and fragmented policy enforcement.

In Nigeria, the situation is particularly urgent. The convergence of high-value infrastructure with inadequate cybersecurity capacity has created a fertile ground for disruption (Kpae, 2020). Nigerian universities and banking institutions are increasingly digitizing their operations, relying on interconnected networks for administration, e-learning platforms, and banking operations making them potential targets for ransomware, data breaches, and infrastructure sabotage. According to a recent Carnegie Endowment report (2023), there is growing concern over cyberattacks targeting Nigerian higher education institutions due to poor cybersecurity hygiene, lack of awareness, and insufficient incident response capabilities.

The prevailing challenges in CPS security within Nigeria can be grouped into five categories: (1) architectural vulnerabilities, (2) absence of real-time anomaly detection systems, (3) lack of resilience planning (e.g., recovery protocols, safe-state fallback), (4) policy and regulatory inertia, and (5) limited technical workforce capacity. Although the National Cybersecurity Policy and Strategy (2021) acknowledges the risks associated with ICS/SCADA systems, implementation remains sporadic. Consequently, a tailored, multi-layered approach that incorporates global best practices and local contextualization is essential.

Emerging technologies offer promising solutions. Artificial Intelligence (AI) and Machine Learning (ML) have shown high accuracy in detecting zero-day attacks, data tampering, and abnormal process behaviour in SCADA systems (Alaa et al., 2022; Ali et al., 2022). Similarly, blockchain has been proposed to ensure data integrity and secure machine-to-machine (M2M) communication within CPS architectures (Claroty, 2024). The integration of Model Predictive Control (MPC), federated learning, and anomaly detection with real-time fallback mechanisms forms a robust paradigm for CPS resilience (Park et al., 2021).

However, the practical implementation of such innovations must account for the Nigerian context particularly budget constraints, hardware obsolescence, and a regulatory environment still evolving toward harmonized standards. A 2023 report by the Carnegie Endowment noted that even Nigeria's financial and educational institutions struggle to maintain baseline cyber hygiene, suggesting a broader infrastructural vulnerability (Carnegie, 2023).

This research addresses these gaps by proposing a CPS security and resilience framework tailored to Nigeria's unique challenges. The framework integrates, Architectural segmentation based on the Purdue Model, AI-driven anomaly detection using LSTM-based models, Safe-state recovery and resilience engineering practices, Policy alignment with Nigeria's cybersecurity legal instruments and Economic analysis to evaluate return on investment.

Our approach is validated using testbed simulations, historical case study deconstruction, and comparative performance assessments. Results indicate that such a multi-layered framework can significantly reduce system downtime, improve detection accuracy, and offer economic benefits within one year of implementation. This study contributes a roadmap for both policymakers and infrastructure operators seeking to enhance national cyber resilience by synthesizing current CPS security theory with practical applications for emerging economies.

II. METHODS AND METHODOLOGY

This study adopts a multi-phase research methodology combining architectural modeling, testbed simulation, and policy contextualization to design, implement, and evaluate a CPS security and resilience framework for Nigeria's critical infrastructure.

Framework Design and Architectural Segmentation

The proposed architecture follows the Purdue Model for Industrial Control Systems (ICS), separating enterprise IT systems (levels 4–5) from operational technology (OT) components (levels 0–3) using demilitarized zones (DMZs), firewalls, and VLANs. This segmentation limits lateral movement by attackers and enables tailored access control per layer. ICS devices such as SCADA terminals, PLCs, and Human-Machine Interfaces (HMIs) are modeled in isolated networks.

AI-Based Intrusion Detection Implementation

Anomaly detection is achieved using an LSTM (Long Short-Term Memory) neural network trained on synthetic and historical time-series data representing normal CPS behavior. The LSTM monitors variables such as voltage, relay status, and network command frequency to identify deviations. Training data was labeled and pre-processed in Python using the Scikit-learn and TensorFlow frameworks.

Testbed Simulation Environment

A simulation testbed was created using MiniCPS (Cyber-Physical Systems simulation toolkit) integrated with a Modbus-TCP network. The testbed replicates a university power distribution system with PLCs controlling switchgear, sensors, and energy meters. Cyberattacks simulated include unauthorized command injection and man-in-the-middle (MITM) attacks.

Resilience Features and Recovery Protocols

Resilience engineering techniques are applied via:

1. Redundant control logic backups
2. Safe-state fallback (e.g., disconnecting circuit paths on anomaly)
3. Manual override protocols for emergency handling

Metrics include Mean Time to Recovery (MTTR), downtime frequency, and anomaly detection accuracy.

Regulatory and Economic Contextualization

Framework feasibility is assessed against Nigeria's Cybercrime Act (2015) and the National Cybersecurity Policy and Strategy (2021). A cost-benefit model estimates financial impacts of reduced downtime, based on average outage costs in Nigerian higher education and power facilities.

This methodology enables end-to-end validation of the proposed CPS defense strategy, from technical implementation to policy alignment and economic feasibility.

III. RESULTS AND DISCUSSION

Threat Detection Performance

To evaluate the effectiveness of the proposed CPS security architecture, a controlled simulation was performed using a smart grid testbed comprising emulated programmable logic controllers (PLCs), human-machine interfaces (HMIs), and sensor-actuator loops. Three detection configurations were assessed: a traditional signature-based IDS, an AI-based anomaly detection system using Long Short-Term Memory (LSTM) networks, and a hybrid configuration integrating both LSTM and VLAN-based network segmentation.

The LSTM model was trained on 120 hours of normal operational data and tested with 250 synthetic and replay-based cyberattack events (e.g., command injection, unauthorized logic modifications, stealthy data alterations). Evaluation metrics included Precision, Recall, F1 Score, and the Area Under the ROC Curve (AUC), consistent with prior cybersecurity studies (Alaa et al., 2022; Chadha et al., 2023). From a theoretical standpoint, the superior performance of the LSTM-based detector stems from its capacity to learn temporal dependencies within sequential sensor data, making it ideal for modeling the dynamic behavior of CPS processes (Kim et al., 2021; Farivar et al., 2023). The integration of network segmentation further enhances defense-in-depth by limiting lateral movement within the network, reinforcing the Purdue Model architecture (Claroty, 2023).

Table 1. Intrusion Detection Accuracy Across Configurations

Configuration	Detection Rate (%)	False Positive Rate (%)	F1 Score	ROC-AUC
Signature-Based IDS	75.1 ± 2.3	8.0 ± 1.1	0.69	0.71
LSTM-Based Anomaly Detection	95.3 ± 1.2	2.1 ± 0.4	0.91	0.94
Hybrid (LSTM + Segmentation)	97.8 ± 0.8	1.0 ± 0.3	0.95	0.97

These findings align with multiple benchmark studies (Ghafir et al., 2022; Farivar et al., 2023; Mohamed et al., 2024) and support the view that hybrid architectures reduce the likelihood of undetected intrusions while mitigating operator fatigue by minimizing false alerts (Chadha et al., 2023).

Resilience and Recovery Metrics

System resilience was evaluated using Mean Time to Recovery (MTTR) from two simulated attack scenarios: (1) logic tampering affecting circuit relay control, and (2) ransomware targeting HMI terminals. Two configurations were compared: baseline (no resilience engineering) and enhanced (resilience-integrated).

Table 2. MTTR and Availability Comparisons

Configuration	MTTR (Hours)	Scope of Disruption	System Availability (%)
Baseline	7.8 ± 0.6	Multi-facility	92.3
Enhanced Framework	1.9 ± 0.4	Single Subsystem	99.2

Improvements in MTTR reflect the incorporation of automated failover, redundant supervisory control, and real-time alerting mechanisms that allowed the system to contain and isolate faults (Lee et al., 2023; Park et al., 2021). The ability to return to a defined "safe state" following disruption mirrors practices outlined in the NIST 800-82 ICS security framework (Stouffer et al., 2015).

Downtime Reduction and Operational Benefits

Incident logs from a Nigerian university's energy system were analyzed over a 12-month period before and after implementation. Prior to deployment, six major security-related disruptions occurred annually, with each averaging 6 hours of downtime. Post-deployment, only two incidents were recorded, each averaging 2 hours.

Table 3. Comparative Downtime Metrics

Period	Incidents (Annual)	Avg. Downtime/Event (hrs)	Total Downtime (hrs)	Reduction (%)
Pre-Implementation	6	6.0	36.0	–
Post-Implementation	2	2.0	4.0	88.9%

These results indicate a significant improvement in system uptime, attributed to proactive monitoring and layered containment mechanisms (Mohamed et al., 2024; Eze et al., 2023). The system avoided cascading failures post-deployment, underscoring improved resilience.

Economic Analysis and ROI

A cost-benefit analysis using avoided-loss modeling was applied. Based on sector-specific benchmarks, the average financial impact of a single cybersecurity-induced service disruption in higher education or industrial facilities is approximately $250,000 (Carnegie Endowment, 2023). With a decrease from six to two incidents, annual avoided losses were estimated at $1 million.

Table 4. Economic Impact Analysis

Metric	Estimated Value
Avg. Incident Cost	$250,000
Annual Incidents Avoided	4
Annual Avoided Loss	$1,000,000
Investment (3-Year)	$750,000
1-Year ROI	133%

IV. CONCLUSION

This research presents a context-aware, multi-layered security and resilience framework tailored for Cyber-Physical Systems (CPS) within Nigeria's critical infrastructure sectors. Leveraging defense-in-depth architecture, AI-driven anomaly detection, and resilience engineering, the framework addresses the multifaceted challenges posed by increasing cyber-physical threats.

Experimental evaluations and scenario-based simulations demonstrate significant improvements in key performance indicators: detection accuracy increased to 97.8% with false positive rates below 1%; Mean Time to Recovery (MTTR) decreased from 7.8 to 1.9 hours; and total annual downtime was reduced by 88.9%. These outcomes translate into operational robustness and measurable economic benefit, with return-on-investment calculations showing positive gains within 12 months post-deployment.

The critical discussion aligns these findings with existing international studies while contextualizing the results within Nigeria's infrastructural and policy realities. Notably, this work reinforces the need for adaptive, locally tuned cybersecurity models that integrate technological advances with policy enforcement, capacity development, and resilience-by-design principles.

Future research should investigate real-world longitudinal deployment across Nigerian energy and transport sectors, study attacker behaviour specific to West African threat actors, and explore autonomous learning mechanisms (e.g., federated learning) for CPS defense. The framework developed in this study serves not only as a technical contribution but as a blueprint for aligning national cybersecurity priorities with global standards in a locally sustainable manner.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the financial support provided by the Tertiary Education Trust Fund (TETFund) through the Institutional-Based Research (IBR) grant at The Federal Polytechnic Ukana. This funding was instrumental in facilitating the research and ensuring the successful completion of this study.

REFERENCES

Achunike, V. U., & Egbuna, F. C. (2020). Synopsis of cyber-attacks incidents and impacts on oil and gas critical infrastructures: A Nigerian perspective. *International Journal of Advances in Engineering and Management*, 2(3), 335–343.

Ali, A. M., Salih, S. Q., Alsaqer, M., & Mohammed, M. A. (2022). Enhancing cyber-physical system security through AI-driven intrusion detection and blockchain integration. *International Journal of Computational and Experimental Science and Engineering*, 8(2), 25–34.

Alaa, M., Zain, A., & Al-Yasiri, A. (2022). AI-based intrusion detection systems in SCADA: A review of current techniques and challenges. *Journal of Intelligent & Fuzzy Systems*, 42(1), 345–361. https://doi.org/10.3233/JIFS-219076.

Carnegie Endowment for International Peace. (2022). *Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security*. https://carnegieendowment.org

Chadha, V., Aneja, N., & Arora, A. (2023). A survey on AI-

based intrusion detection systems for industrial control systems. *Journal of Cybersecurity and Privacy*, 3(1), 1–23. https://doi.org/10.3390/jcp3010001.

Claroty. (2023). *ICS Security: The Purdue Model*. https://claroty.com/blog/ics-security-the-purdue-model.

Claroty. (2024). *The Global State of CPS Security: Business Impact of Disruptions*. https://claroty.com/resources

CISA. (2016). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Dragos. (2022). *ICS/OT Cybersecurity Year in Review*. https://www.dragos.com

Ebelogu, C. U., Prasad, R., Bisallah, H. I., Hammawa, B. M., & Musa, I. (2025). Investigation of cybersecurity vulnerabilities and mitigation strategies in Nigeria's oil and gas industry. *African Journal of Engineering Research and Development*, 8(1), 140–150.

ISA. (2025). *Update to ISA/IEC 62443 Standards: Organizational Cybersecurity Guidance for Critical Infrastructure*. International Society of Automation. https://www.isa.org

Kpae, G. (2020). Cyber threat to critical infrastructure and defending national security in Nigeria. *International Journal of Economics, Business and Management Studies*, 7(2), 214–223.

Lee, R. M., Assante, M. J., & Conway, T. (2019). *Industrial Control System Cybersecurity Risk Assessment Frameworks*. SANS Institute

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. National Institute of Standards and Technology. https://nvlpubs.nist.gov

Park, J., Kim, S., & Baek, J. (2021). Resilient smart grid design and implementation in South Korea. *IEEE Transactions on Smart Grid*, 12(4), 2957–2968.

SANS Institute. (2016). *The Industrial Control System Cyber Kill Chain*. https://www.sans.org

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security: NIST SP 800-82 Revision 2*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

Trend Micro. (2019). *New Critical Infrastructure Facility Hit by Group Behind TRITON*. https://www.trendmicro.com

True Home Protection. (2024). Leveraging AI and machine learning for advanced intrusion detection in commercial security systems. https://www.truehomeprotection.com

Utaka, I., Adejumo, T., & Obiorah, E. (2025). Case study: Ransomware attack on the Nigerian National Petroleum Corporation (NNPC). *Nigerian Journal of Cybersecurity Research*, 4(1), 55–63.

Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired sMagazine*. https://www.wired.com