

Securing Downstream Petroleum Infrastructure in Nigeria: A Risk-Based Framework for Pipeline and Depot Protection

Chibuzor Amarahobu^{1*}, Festus-Michael Uwagboe², Francis Ojeakhena³

¹NNPC Energy Services Ltd (EnServ), Nigeria, chibuzoramarahobu2@gmail.com

²Suncor Energy, Fort McMurray, Alberta, fest.uwagboe@gmail.com

³TotalEnergies Upstream Nigeria, francis.ojeakhena@totalenergies.com

*Corresponding Author: Chibuzor Amarahobu, chibuzoramarahobu2@gmail.com

Abstract

This review examines the security of Nigeria's downstream petroleum infrastructure through a risk-based framework centred on pipelines and depots as critical components of national fuel distribution. It aims to identify the principal threats affecting these assets, assess the factors that shape infrastructure criticality, evaluate available protection strategies, and integrate governance, resilience and operational considerations into a coherent security architecture. The study adopts a structured narrative review of relevant literature published up to 2022, drawing on evidence concerning pipeline integrity, depot hazards, cyber-physical security, geospatial risk assessment, emergency accessibility, infrastructure governance and resilience management.

The findings show that downstream infrastructure is exposed to interacting threats that include vandalism, illegal tapping, corrosion, equipment failure, fire and explosion, cyber intrusion, flooding, communication constraints and delayed emergency response. The review further demonstrates that uniform protection is inefficient because risk varies according to threat likelihood, asset vulnerability, consequence severity, supply importance and response accessibility. Effective protection therefore requires layered controls that combine surveillance, integrity management, automated monitoring, predictive maintenance, physical security, reliable power supply and coordinated emergency preparedness. Governance quality, institutional accountability, intelligence sharing and credible engagement with host communities are equally important to sustained security performance.

The study concludes that Nigeria should institutionalize a continuously updated, risk-based security framework for downstream assets. Recommended priorities include national risk registers, geospatial threat mapping, standardized security indicators, stronger cyber-security, predictive maintenance, joint inter-agency exercises and pre-positioned emergency resources. Such measures would strengthen resilience, reduce disruption and support safer, more reliable petroleum distribution. Together, these interventions provide a practical pathway for protecting strategic assets while improving energy security and continuity.

Keywords: downstream petroleum infrastructure; pipeline security; depot protection; risk assessment; critical infrastructure resilience; Nigeria

1. Introduction

1.1 Nigeria's Downstream Infrastructure Security Context

Nigeria's downstream petroleum infrastructure constitutes a strategically important network of pipelines, depots, storage tanks, loading facilities and distribution interfaces that connects refined petroleum products with industrial, commercial and household demand. The security of this network is therefore inseparable from national energy availability, market stability and the continuity of economic activity. However, infrastructure protection in Nigeria is complicated by extensive asset dispersion, uneven surveillance coverage, ageing facilities and exposure to densely populated, environmentally sensitive and difficult-to-access locations. Field-based evidence from Nigerian transport infrastructure demonstrates that physical assets operating under demanding environmental conditions require systematic condition assessment because deterioration can reduce functionality and increase vulnerability when defects remain unidentified or untreated (Bolaji et al., 2019).

Structural resilience is equally important because downstream facilities depend on supporting civil works, access roads, drainage systems, equipment foundations and associated transport corridors. Repeated loading, material variability and environmental exposure can progressively weaken infrastructure and alter its performance, reinforcing the need to integrate physical-condition monitoring with security planning rather than treating protection solely as a policing function (Alaka & Tiarniyu, 2019).

The Nigerian context is distinguished by persistent deliberate interference with petroleum infrastructure. Spatial analysis of pipeline attacks has shown that interdiction incidents are geographically differentiated and are associated with complex interactions among infrastructure distribution, local conditions and illicit activity. Such patterns imply that uniform protection across an entire network may misallocate scarce security resources; higher-risk corridors require differentiated surveillance, patrol intensity and response capability based on evidence of exposure and consequence (Anifowose et al., 2012).

Pipeline vandalism in the Niger Delta further illustrates the interaction between security, governance and environmental conditions. Empirical analysis has linked vandalism with institutional and management weaknesses, while also demonstrating the substantial socioeconomic and environmental consequences of recurring attacks. This makes downstream protection a multidimensional security problem in which physical safeguards must be reinforced

by credible governance, environmental management and institutional accountability (Umar & Othman, 2017).

Legal deterrence alone has also proved insufficient. Nigeria maintains statutory provisions directed at sabotage and petroleum-related offences, yet persistent vandalism has exposed implementation, enforcement and criminal-justice limitations. Effective infrastructure protection consequently depends on the operational capacity to detect, investigate and prosecute violations alongside preventive controls at vulnerable assets (Okumagba, 2021).

International scholarship similarly frames petroleum pipelines as cyber-physical and socio-technical systems exposed to accidental, natural and intentional threats. Security research increasingly emphasizes integrated risk assessment, resilience, leakage control, corrosion management and protection against deliberate disruption rather than reliance on isolated physical barriers (Chen et al., 2021).

This orientation is particularly relevant to Nigeria because risk-based integrity management enables operators to prioritize assets according to failure likelihood, consequence severity and condition data. Contemporary pipeline management has therefore moved from largely prescriptive inspection toward risk-informed approaches that combine monitoring, maintenance, reliability analysis and targeted intervention throughout the asset life cycle (Khan et al., 2021).

African experience also demonstrates that petroleum infrastructure security is shaped by wider political and regional conditions. Pipeline development in East Africa has been influenced by interstate relations, security perceptions and concerns surrounding route exposure, showing that infrastructure protection extends beyond engineering reliability to geopolitical and institutional risk (Cannon & Mogaka, 2022). For Nigeria, this broader perspective supports a downstream security architecture that treats pipelines and depots as critical national assets requiring coordinated physical protection, integrity management, intelligence, emergency preparedness and risk-prioritized resource allocation. Such integration is essential where a single successful breach can simultaneously disrupt product supply, generate environmental damage, expose communities to hazards and impose substantial recovery costs.

1.2 Pipeline and Depot Protection Challenges

Protecting Nigeria's downstream petroleum pipelines and depots presents a complex security problem because geographically dispersed assets must remain continuously accessible, observable and operational despite exposure to deliberate interference, technical failure and environmental disruption. Long-distance pipelines cross settlements, waterways, agricultural areas and remote corridors, while depots concentrate highly combustible products within installations where unauthorized access, equipment malfunction or delayed incident detection can generate severe consequences. Effective protection therefore requires simultaneous

management of asset integrity, surveillance, communications, emergency access and surrounding environmental conditions.

A major challenge is the timely detection and localization of abnormal events. Pipeline leakage may originate from corrosion, mechanical failure, accidental damage or unlawful interference, yet monitoring technologies differ considerably in sensitivity, deployment requirements and ability to identify small or rapidly developing leaks. Consequently, reliance on a single detection method can create surveillance gaps across heterogeneous pipeline networks (Adegboye, Fung& Karnik, 2019). In Nigeria, this technological problem is compounded by the geography of emergency intervention. Evidence from Kwara State demonstrates that network configuration can produce significant variations in emergency-response accessibility, underscoring the importance of locating response resources according to actual travel coverage rather than simple geographic proximity (Tiamiyu et al., 2021).

Communication reliability presents another operational vulnerability. Protective systems increasingly depend on digital reporting, mobile connectivity, remote sensors and coordinated field teams. Yet Nigerian evidence shows that telecommunications coverage and road accessibility can deteriorate simultaneously beyond major urban centres, potentially constraining both electronic communication and physical response to incidents affecting remote infrastructure (Alaka et al., 2022).

Environmental exposure further complicates protection planning. Flooding can isolate access roads, delay patrols, impair surveillance infrastructure and restrict emergency vehicles precisely when rapid intervention is required. Satellite-based mapping of flood-exposed Nigerian roads illustrates the value of spatial intelligence for identifying potentially inaccessible corridors and anticipating seasonal disruption to response operations (Alaka, Bolaji & Tiamiyu, 2022).

Protection challenges also extend beyond technical barriers. Mozambique’s natural-gas experience demonstrates how extractive infrastructure can become embedded within environments characterized by community displacement, socioeconomic grievance and armed insecurity, thereby transforming infrastructure protection into a broader socio-political task (Namaganda et al., 2022). Nigerian pipeline and depot security must therefore address interacting physical, technological, environmental and human vulnerabilities rather than treating vandalism, operational failure and emergency response as separate risk domains.

1.3 Review Scope and Analytical Objectives

This review examines the security of Nigeria’s downstream petroleum infrastructure through a risk-based analytical perspective, with particular emphasis on pipelines and petroleum depots as critical components of national fuel distribution. Its scope encompasses the principal physical, operational, technological, environmental and institutional threats capable of disrupting asset

integrity, product movement and emergency response. Attention is directed to deliberate interference such as vandalism, theft and unauthorized access, alongside equipment failure, infrastructure deterioration, cyber-physical vulnerabilities, flooding, communication limitations and weaknesses in surveillance or response coverage.

The review further evaluates how these threats interact with asset criticality and consequence severity. Rather than treating all infrastructure as equally vulnerable, the analysis considers how differences in location, operational importance, accessibility, population exposure, product volume and recovery difficulty should influence security priorities. This approach supports the identification of assets requiring enhanced monitoring, stronger preventive controls and faster intervention capability.

A central objective is to assess the adequacy of existing protection practices and determine how physical security, integrity management, digital monitoring, geospatial intelligence, emergency preparedness and institutional coordination can be integrated within a coherent protection architecture. The review also examines the importance of regulatory oversight, inter-agency collaboration, operator accountability and community-sensitive security arrangements.

Ultimately, the analytical objective is to develop a structured framework for prioritizing downstream infrastructure risks and allocating protective resources according to assessed vulnerability, threat likelihood and potential consequence. This provides a basis for more preventive, intelligence-led and resilience-oriented pipeline and depot protection in Nigeria.

2. Threats to Downstream Petroleum Infrastructure

Nigeria's downstream petroleum infrastructure operates within a multidimensional threat environment in which deliberate attacks, progressive asset deterioration, process failures and digital vulnerabilities may independently or collectively compromise supply continuity. Pipelines, storage depots, pumping installations and loading facilities are particularly consequential because disruptions can propagate beyond individual assets into fuel shortages, transportation constraints, environmental contamination and substantial economic losses. Nigeria's petroleum system has historically faced recurrent challenges associated with vandalism, product theft, ageing assets, maintenance deficiencies and operational inefficiencies, illustrating the close relationship between infrastructure security and dependable petroleum distribution (Ogbuigwe, 2018).

Intentional third-party interference constitutes one of the most persistent threats to pipeline systems. Unauthorized tapping, malicious damage, and excavation can produce immediate rupture or introduce defects that progressively undermine structural integrity. Because malicious actors may adapt their behaviour in response to surveillance and enforcement, conventional probability-based assessment cannot adequately capture every dimension of intentional

interference. Pipeline security therefore requires threat-informed risk assessment capable of distinguishing accidental damage from purposeful intrusion and prioritising vulnerable corridors accordingly (Cui, Quddus & Mashuga, 2020).

Material degradation presents a less visible but equally consequential threat. Localized corrosion can generate concentrated wall loss and stress amplification, eventually producing leakage or catastrophic failure where defects remain undetected (Alamri, 2020). Buried pipelines are additionally exposed to soil chemistry, coating degradation, moisture, and electrochemical processes that may accelerate external corrosion over prolonged operating periods (Wasim & Djukic, 2022). Internally, accumulated deposits can establish aggressive localized environments, making under-deposit corrosion particularly difficult to identify through conventional monitoring and allowing deterioration to progress beneath apparently stable operating conditions (Sliem et al., 2021).

Depot infrastructure concentrates large volumes of combustible products within comparatively confined facilities, producing significant fire, explosion and escalation potential. Evidence from petroleum-product handling facilities in Nigeria's Niger Delta demonstrates that deficiencies in operational controls, equipment conditions and emergency preparedness can materially elevate fire risk (Jia, Nwaogazie & Mmom, 2022). Storage-tank accidents can also generate cascading effects through thermal radiation, blast pressure, pollutant release and secondary ignition, thereby extending consequences beyond facility boundaries (Doregar Zavareh et al., 2022).

Table 1. Illustrative threat profile for Nigerian downstream infrastructure

Threat domain	Typical manifestation	Primary assets exposed	Potential consequence	Risk-control priority
Deliberate interference	Vandalism, illegal tapping, sabotage	Pipelines, valves, manifolds	Product loss, fire, supply disruption	Surveillance, patrols, intrusion detection
Structural degradation	Internal/external corrosion	Pipelines, tanks	Leakage, rupture, contamination	Integrity inspection, predictive maintenance
Process failure	Overpressure, ignition, equipment malfunction	Depots, loading systems	Fire, explosion, operational shutdown	Process safety and preventive maintenance
Cyber intrusion	SCADA manipulation,	Control and	Loss of control, concealed faults	Segmentation, authentication,

	malware, data compromise	telemetry systems		secure data exchange
Environmental hazard	Flooding, erosion, extreme weather	Pipelines, access routes, depots	Damage, isolation, delayed response	Geospatial monitoring and resilience planning
Human/organizational failure	Poor procedures, weak supervision	All critical assets	Escalation of otherwise controllable incidents	Training, governance and emergency readiness

Digitalization adds a further cyber-physical layer of vulnerability. Oil and gas infrastructure has experienced malware, network exploitation and attacks targeting industrial control environments, creating pathways from information-system compromise to operational disruption or physical damage (Stergiopoulos, Gritzalis & Limnaios, 2020). This is particularly important where SCADA systems support remote monitoring and control, because compromised integrity or authentication of operational data can distort real-time decisions and delay recognition of abnormal conditions (Shittu et al., 2022).

3. Risk Assessment for Critical Assets

Risk assessment provides the analytical foundation for protecting Nigeria's downstream petroleum infrastructure because pipelines and depots differ substantially in exposure, operational significance, failure probability and potential consequence. A risk-based approach therefore requires operators to move beyond uniform security allocation and identify which pipeline segments, storage tanks, pumping installations, manifolds and loading facilities would generate the greatest human, environmental and supply-chain consequences if compromised. Effective assessment begins with systematic hazard identification followed by estimation of likelihood, vulnerability and consequence, allowing scarce surveillance, inspection and emergency-response resources to be concentrated where risk is greatest.

For Nigeria's cross-country pipelines, assessment is complicated by incomplete incident records and interactions among human, mechanical and environmental failure mechanisms. Bayesian modelling of a Nigerian petroleum pipeline demonstrated that third-party interference, operational damage, corrosion, material defects and natural hazards can be analysed jointly even where historical failure information is uncertain, enabling probability estimates to be updated as new evidence emerges (Hassan et al., 2022). This is particularly valuable for downstream networks where threat conditions vary spatially and dynamically.

Geographic concentration should consequently form an explicit component of asset criticality analysis. Spatial-clustering methods can identify recurring concentrations of adverse events

rather than treating incidents as randomly distributed across corridors, providing a transferable basis for recognising vandalism hotspots, recurrent leakage locations and sections requiring intensified intervention (Alaka, Tiamiyu & Bolaji, 2021). Risk prioritisation must also account for accessibility. Network-routing research in Lagos demonstrates how congestion and weak connectivity can alter travel efficiency, which is relevant when estimating patrol reach, isolation time and emergency-response capability around vulnerable assets (Tiamiyu & Alaka, 2020).

Disruptive conditions can further alter normal accessibility assumptions. Nigerian mobility evidence from periods of major movement restriction illustrates how network utilisation and travel behaviour can change substantially under abnormal operating conditions, reinforcing the need for scenario-based rather than static response assessments (Ajayi, Alaka & Tiamiyu, 2020).

Table 2. Illustrative risk-ranking framework for critical downstream assets

Assessment dimension	Pipeline application	Depot application	Indicative risk signal	Management response
Threat likelihood	Vandalism, corrosion, excavation	Intrusion, ignition, equipment failure	Frequent or credible initiating events	Intensify surveillance and inspection
Asset vulnerability	Exposed corridor, ageing pipe	Weak perimeter, ageing tanks	Limited resistance to threat	Harden or rehabilitate asset
Human consequence	Proximity to settlements	Workforce/community exposure	High casualty potential	Strengthen exclusion and evacuation controls
Environmental consequence	Rivers, wetlands, farmland	Soil and groundwater exposure	Sensitive receptors nearby	Increase containment capability
Supply criticality	Trunk or feeder importance	Regional distribution role	Large downstream dependency	Prioritise redundancy and rapid restoration
Response accessibility	Road and communications access	Fire-service and evacuation access	Long intervention time	Pre-position emergency resources
Overall priority	Combined risk score	Combined risk score	High/medium/low classification	Risk-proportionate protection

Quantitative consequence analysis is equally necessary because identical failure probabilities can produce very different outcomes. Pipeline consequence assessment should incorporate casualties, environmental contamination, property loss, business interruption and other direct and indirect effects rather than relying only on the geographical radius of an accident (Chen et al., 2019). For depots, quantitative risk models can combine probability of failure with thermal-radiation, flash-fire and vapour-cloud-explosion consequences, thereby differentiating storage components according to the severity of credible loss-of-containment scenarios (Attia & Sinha, 2021).

Spatial risk mapping can strengthen this prioritisation. Integrating geographic information systems with HAZOP analysis enables environmental receptors, hydrology, terrain and leakage characteristics to be combined into maps identifying comparatively vulnerable oil installations and pipeline sections (Galalizadeh et al., 2020). Where precise probabilities are unavailable, fuzzy methods provide a structured mechanism for translating uncertain expert judgments into comparative risk scores, which is particularly useful in data-constrained infrastructure environments (Kraidt et al., 2020). Experience from an Egyptian crude-oil pipeline further shows that fuzzy-clustering models can accommodate uncertainty while reducing the complexity associated with large numbers of interacting risk variables (Osman & Shehadeh, 2022).

4. Pipeline and Depot Protection Strategies

Effective protection of Nigeria's downstream petroleum infrastructure requires a layered architecture in which physical security, asset-integrity management, automation, surveillance and emergency preparedness operate as mutually reinforcing controls. Protection should not be limited to guards, fencing or periodic patrols because pipeline and depot losses can originate from deliberate interference, hidden deterioration, process malfunction or delayed detection. A risk-based strategy should therefore combine prevention, early warning, containment and recovery measures according to asset criticality and credible threat scenarios.

Pipeline protection should begin with continuous integrity surveillance supported by technologies capable of detecting abnormal pressure, flow and acoustic conditions. Contemporary leak-detection approaches include pressure-point analysis, real-time transient modelling, acoustic sensing, fibre-optic systems and external inspection methods, each offering different levels of sensitivity, localization accuracy and operational complexity. Combining complementary techniques can reduce false alarms and improve detection performance across long-distance networks where operating conditions vary substantially (Lu et al., 2020). Acoustic, infrared and ground-penetrating technologies likewise demonstrate the value of matching monitoring methods to pipeline configuration, product characteristics and environmental conditions rather than deploying a single technology throughout an entire network (Meribout et al., 2020).

Physical inspection remains indispensable because digital monitoring cannot eliminate structural defects. Evidence from an African crude-oil pipeline failure demonstrates how dents, corrosion and fatigue interactions can progressively reduce pipeline integrity and ultimately produce through-wall cracking. Inspection programmes should therefore prioritize high-risk segments using intelligent pigging, ultrasonic testing, corrosion mapping and defect-growth assessment to identify deteriorating sections before containment is lost (Hafez, 2021).

Maintenance philosophy is equally critical. Moving from corrective intervention toward predictive maintenance enables equipment condition, vibration, temperature and other operational indicators to inform maintenance decisions before functional failure occurs. Such data-driven approaches can reduce unexpected shutdowns while improving asset availability and lifecycle management across pumps, valves, loading systems and depot equipment (Sunday et al., 2020). Reliability-centred maintenance strengthens this approach by prioritizing failure modes according to their effects and operational significance rather than applying identical maintenance intervals to every component (Olutimehin & Ganiu, 2022).

At depots, automated process protection should integrate programmable logic controllers, supervisory systems, alarms, and interlocks capable of detecting abnormal operating states and initiating timely corrective actions. Integrated automation platforms improve process visibility and facilitate coordinated monitoring of industrial equipment, thereby strengthening preventive control when appropriately configured and maintained (Sunday & Omoegun, 2022).

Electrical protection also requires attention because depots contain pumps, motors, instrumentation and other energized equipment operating near combustible products. Proper grounding reduces hazardous touch voltages, facilitates protective-device operation and limits equipment damage during electrical faults, making grounding integrity an important component of facility resilience (Adeniji et al., 2020).

5. Governance and Stakeholder Security Coordination

Governance is a decisive component of downstream petroleum infrastructure security because pipelines and depots are protected through institutions, regulations, operating companies, security agencies, contractors and host communities rather than by technology alone. In Nigeria, fragmented responsibilities can create gaps between regulation, surveillance, maintenance, intelligence and incident response. A risk-based security regime therefore requires explicit allocation of authority, auditable responsibilities and mechanisms for coordinating decisions across organizational boundaries. Governance models developed for distributed operations emphasize that compliance and operational quality improve when responsibilities, reporting relationships and control expectations are formalized throughout the network (Akin-Oluyomi & Akhigbe, 2022).

Regulatory compliance must also be translated into operational controls. Nigerian evidence from IT governance demonstrates how structured governance frameworks can strengthen compliance by defining processes, accountability and monitoring arrangements, principles that are transferable to security-sensitive petroleum operations where control failures may have serious consequences (Fadero et al., 2018). Yet critical infrastructure governance becomes more difficult when operational ownership, regulatory authority and emergency responsibilities are institutionally fragmented. Research on infrastructure protection shows that reliability can depend upon coordination among actors whose mandates, incentives and information are distributed across separate organizations (De Bruijne & Van Eeten, 2007).

Public-private collaboration is consequently essential, but collaboration itself does not guarantee effective protection. Critical-infrastructure partnerships require clear incentives, information-sharing arrangements, trusted communication and government capacity to coordinate networks without obscuring responsibility for security outcomes (Dunn-Cavelty & Suter, 2009). For Nigeria, this implies coordination among regulators, petroleum operators, police, civil-defence organizations, emergency services and security contractors, supported by protocols for incident escalation, intelligence exchange and joint exercises.

Host-community relationships constitute another governance layer. Research on multinational oil companies in Nigeria shows persistent scepticism among host communities where corporate initiatives are perceived as inadequate or disconnected from local expectations, indicating that security legitimacy cannot be separated from stakeholder relations (Eweje, 2007). Partnership initiatives in the Niger Delta similarly demonstrate that collaborative development arrangements may underperform when power asymmetries, weak institutional capacity and insufficient community participation constrain their effectiveness (Idemudia, 2009). Security coordination should therefore incorporate community reporting channels, grievance mechanisms and locally credible liaison structures without transferring statutory protection responsibilities to communities.

The wider African experience reinforces this requirement. Evidence from extractive operations in the Democratic Republic of Congo shows that corporate security governance can combine participatory practices with exclusionary forms of control, creating tensions where community involvement appears instrumental rather than genuinely representative (Hönke, 2012). Nigerian operators should consequently distinguish engagement from transactional surveillance relationships and establish safeguards against coercion, elite capture and opaque contracting.

Finally, governance arrangements must remain resilient during major disruptions. Conventional command structures may become insufficient when critical infrastructure experiences cascading failure, because effective response can depend upon adaptive action by frontline personnel, local authorities and affected communities (Boin & McConnell, 2007). Pipeline and depot protection should therefore be governed through defined roles, interoperable communication, contingency

planning, performance indicators and post-incident review. Such coordination converts security from a collection of isolated organizational activities into an accountable, system-wide capability aligned with risk, operational continuity and public safety.

6. Integrated Risk-Based Security Framework

An integrated risk-based security framework for Nigeria's downstream petroleum infrastructure should convert dispersed protective activities into a decision system linking threat intelligence, asset criticality, vulnerability, consequence, control selection, monitoring and recovery. The framework should begin with asset classification because trunk pipelines, depots, pumping stations, valve installations and loading facilities do not possess equal strategic value or exposure. Risk evaluation should therefore identify credible initiating events, estimate likelihood and consequence, rank assets, and assign controls proportionate to the risk profile. A resilience-oriented approach extends this logic beyond prevention by incorporating absorption, adaptation and restoration after disruption, thereby aligning security with continuity of petroleum supply (Rød et al., 2020).

The second layer should integrate multi-hazard assessment. Critical infrastructure can experience interacting physical, technological, environmental and human stresses, making single-hazard protection inadequate. Resilience assessment frameworks demonstrate the value of evaluating exposure, vulnerability, robustness, redundancy and recovery capacity within one analytical structure, where cascading disruption is plausible (Argyroudis et al., 2020). For Nigerian pipelines and depots, this means assessing vandalism, corrosion, cyber compromise, fire, flooding, power loss and access constraints within a common risk register rather than through isolated departmental processes.

Continuous monitoring should constitute the third layer. Statistical process control offers a structured basis for identifying abnormal variation, defining control limits and triggering corrective intervention before deviations become operational failures. These principles can support surveillance of pressure, flow, inventory, temperature and other indicators across petroleum installations (Akanbi, Ganiu & Sunday, 2022a). Risk dashboards should combine such operational data with incident intelligence, inspection findings and geographic information so that risk scores are revised as conditions change.

A fourth layer concerns workforce deployment. Multi-shift infrastructure security requires adequate staffing, role clarity and coverage across surveillance, maintenance, control-room operations and emergency response. Workforce-balancing approaches show how personnel allocation can be structured around workload and operational demand, which is relevant where pipelines and depots require coverage (Akanbi, Ganiu & Sunday, 2022b). Resilience also depends on organizational capacity; critical-infrastructure research emphasizes preparedness,

adaptive capability and recovery as measurable attributes rather than informal expectations (Rehak et al., 2019).

Power continuity should form another protective layer because surveillance cameras, sensors, telecommunications, pumps and control systems depend on reliable electricity. Nigerian research on integrating solar power into distributed industrial operations illustrates the potential contribution of decentralized generation to continuity where grid reliability is insufficient (Sunday & Omoegun, 2018). Similarly, optimized load distribution across hybrid systems can improve continuity for critical electrical loads and reduce exposure to localized supply failure (Sunday & Omoegun, 2019).

The final layer should institutionalize reassessment. South African evidence on infrastructure governance under interconnected resource risks highlights the importance of coordinated decision-making where systems are mutually dependent and exposed to changing environmental pressures (Mathetsa, Simatele & Rampedi, 2022). For Nigeria, the framework should therefore operate as a cycle: identify, assess, prioritize, protect, monitor, respond, recover and reassess. This structure would allow security investment to follow changing risk, while ensuring that technical protection, workforce capability, energy resilience and institutional coordination function as a unified architecture rather than separate programmes.

Conclusion

This review examined the security of Nigeria's downstream petroleum infrastructure through a risk-based perspective, with particular attention to pipelines and depots as strategically important assets within the national fuel-distribution system. The study achieved its objectives by identifying the principal threats affecting these facilities, assessing the factors that determine asset criticality, evaluating available protection strategies, examining governance and stakeholder coordination, and synthesizing these elements into an integrated security framework.

The review established that downstream infrastructure risks are multidimensional and interconnected. Pipeline vandalism, illegal tapping, corrosion, equipment deterioration, fire and explosion hazards, cyber-physical vulnerabilities, flooding, communication limitations and delayed emergency access can interact to magnify operational consequences. It also demonstrated that security resources should not be distributed uniformly across infrastructure. Asset protection is more effective when surveillance intensity, inspection frequency, emergency preparedness and maintenance interventions are determined by threat likelihood, vulnerability, consequence severity, supply criticality and response accessibility.

A further key finding is that technological protection alone is insufficient. Effective security depends on the integration of physical safeguards, integrity management, automated monitoring, predictive maintenance, geospatial intelligence, resilient power supply, competent personnel and

coordinated institutional oversight. The review also highlighted the importance of regulatory accountability, intelligence sharing, public-private cooperation and credible engagement with host communities.

Accordingly, Nigeria should institutionalize a continuously updated national risk register for critical downstream assets, supported by geospatial threat mapping, standardized security performance indicators and interoperable incident-reporting systems. Operators should adopt layered protection architectures, strengthen cyber-security and predictive maintenance capabilities, and pre-position emergency resources around high-risk corridors and depots. Regulators and security agencies should conduct periodic joint risk assessments, simulations and compliance audits. Ultimately, a preventive, intelligence-led and resilience-oriented security model offers the strongest basis for reducing disruption, protecting communities and environmental resources, and sustaining reliable petroleum distribution across the country.

References

1. Adegboye, M.A., Fung, W.K. and Karnik, A. (2019) ‘Recent advances in pipeline monitoring and oil leakage detection technologies: Principles and approaches’, *Sensors*, 19(11), 2548. DOI: <https://doi.org/10.3390/s19112548>.
2. Adeniji, I.O., Shittu, H., Opara, I.S. and Shittu, M.A. (2020) ‘Grounding system design optimization for medium-voltage distribution networks in emerging power markets’, *IRE Journals*, 3(11), pp. 547–559. DOI: <https://doi.org/10.64388/IREV3I11-1714040>.
3. Ajayi, O., Alaka, O.B. and Tihamiyu, R. (2020) ‘Essential trip making and mode substitution during COVID-19 movement restrictions in Nigerian cities’, *IRE Journals*, 4(4), pp. 442–465. DOI: <https://doi.org/10.64388/IREV4I4-1722673>.
4. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022a) ‘Comprehensive review of statistical process control (SPC) for precision weight management in global food manufacturing’, *Gyanshauryam: International Scientific Refereed Research Journal*, 5(3).
5. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022b) ‘A workforce-centric line-balancing model for throughput maximization in multi-shift operations’, *Shodhshauryam: International Scientific Refereed Research Journal*, 5(3).
6. Akin-Oluyomi, O.T. and Akhigbe, R. (2022) ‘A supply chain governance model for enhancing compliance and operational quality across retail networks’.
7. Alaka, O.B. and Tihamiyu, R. (2019) ‘Repeated-load performance of concrete produced with locally sourced aggregates for road and drainage structures’, *Iconic Research and Engineering Journals*, 2(10), pp. 673–691. DOI: <https://doi.org/10.64388/IREV2I10-1722671>.
8. Alaka, O.B., Ajayi, O. and Bolaji, O. (2022) ‘Mobile network coverage and road surface condition as joint constraints on digitally booked transport beyond state capitals’, *International Journal of Engineering and Modern Technology*, 8(5), pp. 142–168. DOI: <https://doi.org/10.56201/ijemt.v8.no5.2022.pg142.168>.

9. Alaka, O.B., Bolaji, O. and Tiamiyu, R. (2022) ‘Mapping flood-exposed road segments from freely available satellite imagery during the 2022 flood season’, *IIARD International Journal of Geography & Environmental Management*, 8(2), pp. 117–143. DOI: <https://doi.org/10.56201/ijgem.v8.no2.2022.pg117.143>.
10. Alaka, O.B., Tiamiyu, R. and Bolaji, O. (2021) ‘Spatial clustering of road traffic crash locations on intercity corridors using national road safety records’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), pp. 1086–1101. DOI: <https://doi.org/10.54660/IJMRGE.2021.2.6.1086-1101>.
11. Alamri, A.H. (2020) ‘Localized corrosion and mitigation approach of steel materials used in oil and gas pipelines – An overview’, *Engineering Failure Analysis*, 116, 104735. DOI: <https://doi.org/10.1016/j.engfailanal.2020.104735>.
12. Anifowose, B., Lawler, D.M., van der Horst, D. and Chapman, L. (2012) ‘Attacks on oil transport pipelines in Nigeria: A quantitative exploration and possible explanation of observed patterns’, *Applied Geography*, 32(2), pp. 636–651. DOI: <https://doi.org/10.1016/j.apgeog.2011.07.012>.
13. Argyroudis, S.A., Mitoulis, S.A., Hofer, L., Zanini, M.A., Tubaldi, E. and Frangopol, D.M. (2020) ‘Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets’, *Science of the Total Environment*, 714, 136854. DOI: <https://doi.org/10.1016/j.scitotenv.2020.136854>.
14. Attia, M. and Sinha, J. (2021) ‘Improved quantitative risk model for integrity management of liquefied petroleum gas storage tanks: Mathematical basis and case study’, *Process Safety Progress*, 40(3), pp. 63–78. DOI: <https://doi.org/10.1002/prs.12217>.
15. Boin, A. and McConnell, A. (2007) ‘Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience’, *Journal of Contingencies and Crisis Management*, 15(1), pp. 50–59. DOI: <https://doi.org/10.1111/j.1468-5973.2007.00504.x>.
16. Bolaji, O., Alaka, O.B., Ajayi, O. and Tiamiyu, R. (2019) ‘Field condition assessment of roadside drainage and culvert structures on urban arterials in southwestern and north central Nigeria’, *Iconic Research and Engineering Journals*, 3(1), pp. 663–683. DOI: <https://doi.org/10.64388/IREV311-1722674>.
17. Cannon, B.J. and Mogaka, S. (2022) ‘Rivalry in East Africa: The case of the Uganda-Kenya crude oil pipeline and the East Africa crude oil pipeline’, *The Extractive Industries and Society*, 11, 101102. DOI: <https://doi.org/10.1016/j.exis.2022.101102>.
18. Chen, C., Li, C., Reniers, G. and Yang, F. (2021) ‘Safety and security of oil and gas pipeline transportation: A systematic analysis of research trends and future needs using WoS’, *Journal of Cleaner Production*, 279, 123583. DOI: <https://doi.org/10.1016/j.jclepro.2020.123583>.

19. Chen, X., Wu, Z., Chen, W., Kang, R., Wang, S., Sang, H. and Miao, Y. (2019) ‘A methodology for overall consequence assessment in oil and gas pipeline industry’, *Process Safety Progress*, 38(3), e12050. DOI: <https://doi.org/10.1002/prs.12050>.
20. Cui, Y., Quddus, N. and Mashuga, C.V. (2020) ‘Bayesian network and game theory risk assessment model for third-party damage to oil and gas pipelines’, *Process Safety and Environmental Protection*, 134, pp. 178–188. DOI: <https://doi.org/10.1016/j.psep.2019.11.038>.
21. De Bruijne, M. and Van Eeten, M. (2007) ‘Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment’, *Journal of Contingencies and Crisis Management*, 15(1), pp. 18–29. DOI: <https://doi.org/10.1111/j.1468-5973.2007.00501.x>.
22. Doregar Zavareh, R., Dana, T., Roayaei, E., Monavari, S.M. and Jozi, S.A. (2022) ‘The environmental risk assessment of fire and explosion in storage tanks of petroleum products’, *Sustainability*, 14(17), 10747. DOI: <https://doi.org/10.3390/su141710747>.
23. Dunn-Cavelty, M. and Suter, M. (2009) ‘Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection’, *International Journal of Critical Infrastructure Protection*, 2(4), pp. 179–187. DOI: <https://doi.org/10.1016/j.ijcip.2009.08.006>.
24. Eweje, G. (2007) ‘Multinational oil companies’ CSR initiatives in Nigeria: The scepticism of stakeholders in host communities’, *Managerial Law*, 49(5/6), pp. 218–235. DOI: <https://doi.org/10.1108/03090550710841340>.
25. Fadero, S., Oyesiji, S.O., Nwakamma, S. and Jooda, D. (2018) ‘IT governance frameworks (COBIT/ITIL) and their impact on regulatory compliance in Nigerian insurance firms’, *IRE Journals*, 2(5), pp. 478–496. DOI: <https://doi.org/10.64388/IREV2I5-1722619>.
26. Galalizadeh, S., Karimi, H., Malekmohammadi, B., Sadeghi, A. and Shirzadi, S. (2020) ‘Environmental risk assessment and mapping of oil installations to Chamshir Dam water basin using GIS and HAZOP method’, *International Journal of Risk Assessment and Management*, 23(3/4), pp. 207–222. DOI: <https://doi.org/10.1504/IJRAM.2020.114358>.
27. Hafez, K.M. (2021) ‘The role of a plain dent on the failure mode of a crude oil pipeline’, *Engineering Failure Analysis*, 122, 105291. DOI: <https://doi.org/10.1016/j.engfailanal.2021.105291>.
28. Hassan, S., Wang, J., Kontovas, C. and Bashir, M. (2022) ‘An assessment of causes and failure likelihood of cross-country pipelines under uncertainty using Bayesian networks’, *Reliability Engineering & System Safety*, 218, 108171. DOI: <https://doi.org/10.1016/j.res.2021.108171>.
29. Hönke, J. (2012) ‘Multinationals and security governance in the community: Participation, discipline and indirect rule’, *Journal of Intervention and Statebuilding*, 6(1), pp. 57–73. DOI: <https://doi.org/10.1080/17502977.2012.655569>.

30. Idemudia, U. (2009) ‘Oil extraction and poverty reduction in the Niger Delta: A critical examination of partnership initiatives’, *Journal of Business Ethics*, 90(S1), pp. 91–116. DOI: <https://doi.org/10.1007/s10551-008-9916-8>.
31. Jia, N., Nwaogazie, I.L. and Mmom, P. (2022) ‘Fire risk evaluation for petroleum products handling facilities in Niger Delta Region, Nigeria’, *Current Journal of Applied Science and Technology*, 41(37), pp. 19–29. DOI: <https://doi.org/10.9734/cjast/2022/v41i373970>.
32. Khan, F., Yarveisy, R. and Abbassi, R. (2021) ‘Risk-based pipeline integrity management: A road map for the resilient pipelines’, *Journal of Pipeline Science and Engineering*, 1(1), pp. 74–87. DOI: <https://doi.org/10.1016/j.jpse.2021.02.001>.
33. Kraidi, L., Shah, R., Matipa, W. and Borthwick, F. (2020) ‘Using stakeholders’ judgement and fuzzy logic theory to analyze the risk influencing factors in oil and gas pipeline projects: Case study in Iraq, Stage II’, *International Journal of Critical Infrastructure Protection*, 28, 100337. DOI: <https://doi.org/10.1016/j.ijcip.2020.100337>.
34. Lu, H., Iseley, T., Behbahani, S. and Fu, L. (2020) ‘Leakage detection techniques for oil and gas pipelines: State-of-the-art’, *Tunnelling and Underground Space Technology*, 98, 103249. DOI: <https://doi.org/10.1016/j.tust.2019.103249>.
35. Mathetsa, S.M., Simatele, M.D. and Rampedi, I.T. (2022) ‘A water-centric approach in the assessment and governance of the water-energy-climate change nexus in South Africa’, *Frontiers in Sustainable Food Systems*, 6, 691704. DOI: <https://doi.org/10.3389/fsufs.2022.691704>.
36. Meribout, M., Khezzar, L., Azzi, A. and Ghendour, N. (2020) ‘Leak detection systems in oil and gas fields: Present trends and prospects’, *Flow Measurement and Instrumentation*, 75, 101772. DOI: <https://doi.org/10.1016/j.flowmeasinst.2020.101772>.
37. Namaganda, E., Otsuki, K. and Steel, G. (2022) ‘Learning from Africana critical theory: A historicized contextualization of the impacts of Mozambique’s natural gas project’, *The Extractive Industries and Society*, 10, 101075. DOI: <https://doi.org/10.1016/j.exis.2022.101075>.
38. Ogbuigwe, A. (2018) ‘Refining in Nigeria: History, challenges and prospects’, *Applied Petrochemical Research*, 8, pp. 181–192. DOI: <https://doi.org/10.1007/s13203-018-0211-z>.
39. Okumagba, E.O. (2021) ‘Critical analysis of laws and policies for the prevention of petroleum pipeline vandalization in Nigeria’, *Environmental Law Review*, 23(4), pp. 305–320. DOI: <https://doi.org/10.1177/14614529211057189>.
40. Olutimehin, A.O. and Ganiu, O.S. (2022) ‘Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), pp. 983–996. DOI: <https://doi.org/10.54660/IJMRGE.2022.3.6.983-996>.

41. Osman, A. and Shehadeh, M. (2022) ‘Risk assessment of interstate pipelines using a fuzzy-clustering approach’, *Scientific Reports*, 12, 13750. DOI: <https://doi.org/10.1038/s41598-022-17673-3>.
42. Rehak, D., Senovsky, P., Hromada, M. and Lovecek, T. (2019) ‘Complex approach to assessing resilience of critical infrastructure elements’, *International Journal of Critical Infrastructure Protection*, 25, pp. 125–138. DOI: <https://doi.org/10.1016/j.ijcip.2019.03.003>.
43. Rød, B., Lange, D., Theocharidou, M. and Pursiainen, C. (2020) ‘From risk management to resilience management in critical infrastructure’, *Journal of Management in Engineering*, 36(4), 04020039. DOI: [https://doi.org/10.1061/\(ASCE\)ME.1943-5479.0000795](https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795).
44. Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) ‘Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems’, *Iconic Research and Engineering Journals*, 6(3), pp. 359–380. DOI: <https://doi.org/10.64388/IREV6I3-1714041>.
45. Sliem, M.H., Fayyad, E.M., Abdullah, A.M., Younan, N.A., Al-Qahtani, N., Nabhan, F.F., Ramesh, A., Laycock, N., Ryan, M.P., Maqbool, M. and Arora, D. (2021) ‘Monitoring of under deposit corrosion for the oil and gas industry: A review’, *Journal of Petroleum Science and Engineering*, 204, 108752. DOI: <https://doi.org/10.1016/j.petrol.2021.108752>.
46. Stergiopoulos, G., Gritzalis, D.A. and Limnaios, E. (2020) ‘Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns’, *IEEE Access*, 8, pp. 128440–128475. DOI: <https://doi.org/10.1109/ACCESS.2020.3007960>.
47. Sunday, E.A. and Omoegun, G.O. (2018) ‘Integrating solar power solutions in small-scale manufacturing industries in Nigeria’, *International Journal of Scientific Research in Science, Engineering and Technology*, 4(8), pp. 832–853.
48. Sunday, E.A. and Omoegun, G.O. (2019) ‘Optimizing electrical load distribution for hybrid solar installations in developing economies’, *International Journal of Scientific Research in Mechanical and Materials Engineering*, 3(6), pp. 27–47.
49. Sunday, E.A. and Omoegun, G.O. (2022) ‘Automation of process control systems using Siemens TIA Portal: A case study approach’, *International Journal of Scientific Research in Mechanical and Materials Engineering*, 6(5), pp. 30–55.
50. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) ‘Transitioning from reactive to predictive maintenance in mechanical systems’, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(6), pp. 425–447.
51. Tiamiyu, R. and Alaka, O.B. (2020) ‘Routing of motorcycle dispatch deliveries on congested and poorly connected urban networks in Lagos’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 1(5), pp. 1183–1198. DOI: <https://doi.org/10.54660/IJMRGE.2020.1.5.1183-1198>.

52. Tiamiyu, R., Alaka, O.B. and Ajayi, O. (2021) ‘Emergency response coverage gaps on intercity highways in Kwara State: A network service-area analysis’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), pp. 1102–1118. DOI: <https://doi.org/10.54660/IJMRGE.2021.2.6.1102-1118>.
53. Umar, A.T. and Othman, M.S.H. (2017) ‘Causes and consequences of crude oil pipeline vandalism in the Niger Delta region of Nigeria: A confirmatory factor analysis approach’, *Cogent Economics & Finance*, 5(1), 1353199. DOI: <https://doi.org/10.1080/23322039.2017.1353199>.
54. Wasim, M. and Djukic, M.B. (2022) ‘External corrosion of oil and gas pipelines: A review of failure mechanisms and predictive preventions’, *Journal of Natural Gas Science and Engineering*, 100, 104467. DOI: <https://doi.org/10.1016/j.jngse.2022.104467>.