

Outsourced Security in Nigeria's Oil and Gas Sector: Contractor Selection, Performance Monitoring and Cost Control

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 strategic management of outsourced security within Nigeria's oil and gas sector, with particular emphasis on contractor qualification, performance oversight, expenditure control, governance, and technological modernization. The study adopts a structured narrative review approach, drawing on multidisciplinary literature concerning private security, contractor management, critical infrastructure protection, procurement, operational resilience, performance measurement, cost optimization, and digital security technologies. The analysis shows that effective outsourcing depends on rigorous prequalification, risk-based procurement, clearly defined contractual obligations, and continuous verification of contractor competence, integrity, regulatory compliance, and operational readiness. It further demonstrates that security performance should be assessed through balanced indicators encompassing patrol completion, response time, access control, training compliance, incident reporting, technology availability, and corrective-action closure. Cost effectiveness emerges not from indiscriminate expenditure reduction, but from lifecycle cost analysis, value-for-money assessment, resource optimization, and the alignment of contractor remuneration with measurable outcomes. The review also identifies governance and inter-organizational coordination as essential to operational resilience, particularly where operators, contractors, regulators, public security agencies, and host communities must respond collectively to physical, environmental, and cyber threats. Emerging technologies, including digital twins, SCADA, wireless sensors, artificial intelligence, and secure data platforms, offer significant opportunities for predictive monitoring and targeted deployment, but require robust cybersecurity and data-governance safeguards. The study concludes that outsourced security should be governed as an integrated strategic capability rather than a transactional service. It recommends institutionalized contractor due diligence, integrated performance dashboards, periodic contract optimization, joint resilience planning, and sustained investment in interoperable security technologies.

Keywords: outsourced security; oil and gas; contractor management; performance monitoring; cost control; operational resilience

DOI: 10.18091/ijsts.v8i1.11

1. Introduction

1.1 Security Risks in Petroleum Operations

Petroleum operations are intrinsically exposed to layered security risks because their production, processing, storage and transportation systems combine high-value commodities, hazardous materials and geographically dispersed infrastructure. Pipelines, flow stations, terminals, offshore installations and depots may therefore become attractive targets for theft, sabotage, terrorism and organized criminal interference. Globally, petroleum infrastructure is increasingly treated as critical infrastructure because its disruption can generate cascading operational, environmental, economic and societal consequences. Research on pipeline transportation consequently places deliberate attacks alongside leakage, corrosion and system resilience as major dimensions of contemporary petroleum risk management (Chen *et al.*, 2021).

In Nigeria, these vulnerabilities are amplified by the spatial configuration of petroleum operations across the Niger Delta, where extensive pipeline networks intersect waterways, settlements, agricultural areas and difficult terrain. Pipeline vandalism is particularly consequential because deliberate interference may simultaneously interrupt production, release hydrocarbons, damage ecosystems and expose neighbouring communities to fires and other hazardous events. Empirical evidence associates vandalism in the Niger Delta with governance deficiencies, weak institutional arrangements, environmental degradation and management-related conditions, demonstrating that petroleum-security risks cannot be understood solely as technical failures (Umar & Othman, 2017).

Operational exposure is also influenced by mobility and physical accessibility. Petroleum security depends upon ~~the capacity to deploy patrol personnel, supervisors and response teams rapidly~~ between installations, yet transportation networks may contain concentrated accident risks that complicate routine surveillance and emergency deployment. Evidence from Nigerian intercity corridors demonstrates distinct spatial clustering of road traffic crashes, indicating the importance of location-sensitive route assessment when organizing mobile security operations around geographically dispersed assets (Alaka, Tihamiyu & Bolaji, 2021). Emergency capability is equally significant, since network-service analysis has identified gaps in emergency-response coverage along Nigerian intercity highways, illustrating how distance and road connectivity can constrain

timely intervention when security incidents occur around remote infrastructure (Tiamiyu, Alaka& Ajayi, 2021).

Environmental hazards can further intensify these vulnerabilities. Seasonal flooding may isolate production facilities, damage access roads, impair patrol movements and disrupt established response routes. Satellite-based mapping of flood-exposed Nigerian roads demonstrates how geospatial information can reveal infrastructure accessibility constraints during severe flooding (Alaka, Bolaji& Tiamiyu, 2022). For oil and gas operators, such disruption has a direct security dimension because weakened accessibility may reduce surveillance frequency, extend reinforcement times and create temporary gaps in protective coverage.

Intentional attacks require equally sophisticated risk assessment. Petroleum pipelines are linear assets whose entire length cannot ordinarily receive identical levels of physical protection. Security resources must therefore be directed according to threat probability, asset attractiveness, vulnerability and potential consequences. Game-theoretic analysis demonstrates how risk-based approaches can identify higher-risk pipeline segments and support more efficient allocation of limited protective resources against intentional attack (Rezazadeh *et al.*, 2019). Political instability and terrorism also extend risk beyond individual facilities, requiring organizations to integrate political-security analysis into corporate risk management rather than relying exclusively upon conventional site protection (Lambrechts & Blomquist, 2017).

The contemporary threat environment is additionally multidimensional. Oil and gas infrastructure may face physical attack, insider threats, cyber intrusion, regulatory failures and environmental hazards simultaneously, making isolated security controls increasingly inadequate (Pashchenko *et al.*, 2024). Such complexity becomes particularly important in outsourced security arrangements because contractor personnel may possess extensive access to facilities, operational information and surveillance systems. Outsourcing therefore redistributes protective functions without eliminating the operator's underlying accountability for infrastructure security; international experience demonstrates that private and non-state actors have become significant participants in critical energy-infrastructure protection, making governance and oversight indispensable (Zabyelina & Kustova, 2015).

Within the Niger Delta specifically, pipeline insecurity is intertwined with vandalism, conflict, host-community relationships and broader governance conditions, requiring security arrangements that respond to the social as well as physical operating environment (Jatto, 2024). Consequently, petroleum-security risk in Nigeria is best understood as a convergence of deliberate interference, infrastructural exposure, environmental disruption, access limitations and institutional vulnerabilities. This risk profile directly shapes outsourced-security requirements, demanding contractors capable of surveillance, intelligence coordination, route protection, incident escalation, emergency support and resilient deployment across complex petroleum networks.

1.2 Growth of Outsourced Security Services

The expansion of outsourced security services reflects a broader reconfiguration of organizational boundaries in which firms increasingly transfer specialized, non-core functions to external providers while retaining strategic oversight. In complex industries such as oil and gas, this model is attractive because security demand is geographically dispersed, threat-sensitive and labour-intensive. Outsourcing can therefore provide access to specialist capabilities, scalable manpower and technology without requiring operators to maintain every protective function internally. International evidence identifies cost discipline, concentration on core competencies and access to specialist capabilities as central drivers of outsourcing, while emphasizing the growing importance of performance-based supplier relationships (Kakabadse & Kakabadse, 2005).

Within Nigeria, the growth of private security provision also reflects persistent demand for supplementary protective capacity beyond conventional public policing. Evidence from Lagos demonstrates that private security companies have become significant actors in crime prevention, although their effectiveness depends substantially upon operational collaboration and information exchange with the police (Chinwokwu, 2018). For petroleum operators, this plural security environment facilitates the contracting of guarding, patrol, access-control, surveillance and response functions while statutory security responsibilities remain distributed among relevant state institutions.

The organizational case for outsourcing is strengthened where geographically dispersed operations require capabilities that cannot be efficiently centralized. Capability-building approaches for distributed operations highlight the importance of developing specialized talent pools capable of deployment across multiple operational locations (Falemi, Akhigbe & Akin-Oluyomi, 2020). Equally, aligning externally delivered activities with enterprise strategy is essential if outsourced services are to reinforce operational continuity rather than function as detached support arrangements (Akin-Oluyomi & Akhigbe, 2023). Workforce optimization becomes especially important where expansion, shift requirements and fluctuating operational demands create staffing volatility, thereby increasing the attractiveness of scalable contractor deployment (Falemi, Akhigbe & Akin-Oluyomi, 2023).

African experience further demonstrates that private security expansion creates hybrid security arrangements in which public and private actors increasingly interact in everyday protective functions. South African evidence illustrates how these interactions may blur conventional institutional boundaries and generate complex questions of authority and accountability (Diphooorn, 2016). In Nigeria's oil and gas sector, outsourced security has consequently evolved beyond a simple cost-reduction mechanism toward a strategic means of obtaining flexible manpower, specialized expertise, broader geographic coverage and responsive protective capacity across dispersed petroleum assets.

1.3 Review Scope and Objectives

This review examines outsourced security management in Nigeria's oil and gas sector through three interrelated dimensions: contractor selection, performance monitoring, and cost control. Its scope covers the strategic, operational, and governance considerations that shape how petroleum companies engage external security providers to protect personnel, production assets, pipelines, terminals, logistics corridors, and other critical infrastructure. Particular attention is given to the need for structured contractor prequalification, due diligence, competency assessment, regulatory compliance, workforce capability, technological readiness, and demonstrated capacity to operate within complex and high-risk environments.

The review also evaluates how contractor performance should be monitored after appointment. It considers the role of measurable service standards, key performance indicators, incident reporting, patrol effectiveness, response times, audit mechanisms, supervisory oversight, and accountability systems in determining whether outsourced security arrangements achieve expected protection outcomes. Because effective security cannot be separated from financial sustainability, the discussion further addresses expenditure control, cost drivers, value-for-money assessment, contract optimization, and the balance between budget discipline and adequate risk coverage.

Beyond these core themes, the review explores the governance structures required to coordinate operators, private security contractors, public security agencies, regulators, and host communities. It also considers the growing influence of surveillance technologies, digital monitoring, analytics, and integrated risk-management systems on outsourced security delivery. The central objective is to develop a coherent analytical basis for understanding how Nigerian oil and gas companies can structure outsourced security arrangements that are capable, accountable, cost-conscious, and resilient while remaining responsive to evolving operational threats and institutional expectations across diverse onshore, offshore, and midstream operating contexts nationwide.

2. Security Contractor Selection

2.1 Contractor Qualification and Due Diligence

Contractor qualification is a foundational safeguard in outsourced security management because deficiencies accepted during procurement can later become operational vulnerabilities, compliance failures and avoidable cost burdens. In Nigeria's oil and gas sector, security contractors may control access to pipelines, terminals, production installations, warehouses, logistics routes and other strategically important assets. Selection must therefore extend beyond business registration and competitive pricing to establish whether a prospective provider possesses the financial stability, organizational competence, ethical integrity, workforce capability and operational resilience required for petroleum-security environments.

A disciplined prequalification system should begin with objective eligibility criteria. Previous contractor-selection research demonstrates that financial capacity, technical competence, management capability, historical performance and organizational resources are important determinants of successful contractor performance (Hatush & Skitmore, 1997). Applied to security outsourcing, this requires systematic verification of corporate ownership, operating licences, insurance arrangements, financial statements, litigation history, prior contracts, management structure and capacity to sustain continuous deployments throughout the contractual period.

Formal prequalification should also distinguish documentary compliance from demonstrated capability. Models of contractor prequalification emphasize structured screening before contract award so that organizations can identify unsuitable providers before commercial considerations become dominant (El-Sawalhi, Eaton & Rustom, 2007). Petroleum operators should therefore validate personnel strength, supervisory ratios, training programmes, communication systems, emergency-response procedures, vehicles, surveillance capacity and evidence of comparable experience in high-risk industrial environments.

Safety competence requires particular scrutiny because contracted security personnel work within hazardous operating environments containing hydrocarbons, pressurized systems, restricted process areas and heavy industrial activities. Nigerian research on oil and gas contractor management stresses the importance of embedding safety performance, training, monitoring and risk controls into contractor-management systems rather than treating safety as a secondary procurement consideration (Onukwulu *et al.*, 2024). Contractor due diligence should consequently review accident records, safety violations, induction practices, incident reporting, emergency drills and compliance with operator-specific health, safety and environmental requirements.

Personnel integrity is equally important. Security workers may receive privileged access to restricted locations, surveillance information, communications systems and commercially sensitive material. Due diligence should therefore assess recruitment standards, identity verification, reference checks, background screening, disciplinary procedures and mechanisms for addressing insider threats. Evidence from Tanzania's private-security sector further illustrates the importance of regulatory vetting and continuing oversight of providers rather than relying solely on initial licensing (Sambu, 2024).

Table 2. Illustrative Security Contractor Qualification Framework

Qualification dimension	Due diligence evidence	Petroleum-security relevance
Legal compliance	Licences, registration, insurance and statutory records	Confirms lawful operating status
Financial capacity	Audited accounts, credit history and liquidity	Reduces contract-disruption risk

Operational experience	Comparable contracts and client references	Demonstrates relevant security capability
Workforce quality	Training records, vetting and supervisory structure	Supports competent and reliable deployment
Safety performance	Incident history, HSE procedures and certifications	Limits exposure within hazardous facilities
Technology capability	CCTV, access control, communications and reporting systems	Supports modern surveillance requirements
Ethical integrity	Litigation history, disciplinary systems and conduct policies	Reduces fraud and insider-threat exposure
Emergency readiness	Response plans, vehicles and escalation procedures	Enables timely incident intervention
Governance capacity	Reporting systems, audit access and management controls	Strengthens accountability and oversight

Contractor assessment should therefore use a multi-criteria evaluation structure rather than a lowest-bid approach. Comparative research shows that technical competence, financial status, quality performance, reputation and cooperation are all relevant to contractor selection (Hartmann, Ling & Tan, 2009). Structured evaluation is especially important in petroleum security because contractors may perform under substantially different threat conditions across pipelines, offshore facilities, corporate offices and terminals.

Analytical selection methods can further improve decision quality by combining quantitative and qualitative information. Integrated models demonstrate that contractor assessment can accommodate multiple performance variables and uncertainty rather than relying on subjective procurement judgments alone (El-Abbasy *et al.*, 2013). Weighted scoring systems may therefore distinguish mandatory requirements from differentiating factors such as local intelligence capability, specialist surveillance expertise, rapid-response coverage and technological readiness.

The methodology used to select contractors must itself be appropriate to organizational risk. Contractor-selection research cautions that no single simplistic evaluation model is sufficient across all procurement environments and emphasizes the need for transparent, structured comparison mechanisms (Holt, 1998). Similarly, client and consultant perspectives demonstrate that technical capability, management competence and organizational reputation remain important alongside price considerations (Egemen & Mohamed, 2005).

More contemporary selection frameworks extend this approach by explicitly balancing benefits, opportunities, costs and risks within contractor decisions. Such multidimensional analysis is particularly appropriate where subcontractor performance influences broader project and organizational outcomes (Al Subaie *et al.*, 2023). For outsourced security in Nigeria's petroleum

sector, contractor qualification should therefore function as a risk-control gateway through which only providers demonstrating verified competence, integrity, regulatory compliance, financial resilience and operational suitability proceed to final contract award.

2.2 Risk-Based Procurement and Contract Design

Risk-based procurement in outsourced petroleum security requires contract strategy to originate from the threat profile of the asset rather than from standardized guarding specifications. Pipelines, terminals, production installations and corporate facilities present materially different exposure levels; consequently, procurement planning should translate threat likelihood, asset criticality, accessibility and potential consequence into differentiated service requirements. Analytics-based forecasting can strengthen this process by linking anticipated operational demand with resource allocation and identifying potential deployment bottlenecks before contract award (Akin-Oluyomi & Akhigbe, 2023).

In geographically dispersed Nigerian operations, procurement decisions should also incorporate location-specific evidence. Combining field observations with geospatial information provides a practical basis for decision-making where conventional datasets are incomplete, enabling security planners to identify access limitations, coverage gaps and locations requiring stronger contractor presence (Tiamiyu *et al.*, 2023). Multi-criteria prioritization similarly enables scarce resources to be allocated according to several risk variables rather than a single cost criterion (Alaka *et al.*, 2023).

Contract design should subsequently assign each material risk to the party best positioned to control, mitigate or absorb it. Evidence from Ghana demonstrates that balanced risk allocation depends upon the respective risk-management capabilities of contracting parties and can improve the practicality of contractual arrangements (Ameyaw & Chan, 2015). International PPP experience likewise shows that effective procurement requires systematic allocation of operational, financial and external risks rather than indiscriminate transfer to contractors (Bing *et al.*, 2005).

For outsourced petroleum security, contracts should clearly specify staffing levels, patrol frequency, response times, reporting obligations, technology requirements, escalation procedures, insurance, liabilities, performance deductions and change-control mechanisms. Excessive transfer of uncontrollable risks can undermine contractor cooperation and encourage defensive pricing, making balanced allocation important to contractual governance (Zhang *et al.*, 2016). Risk-based design therefore links security exposure directly to procurement specifications, pricing logic and enforceable performance obligations.

3. Contractor Performance Monitoring

3.1 Security Performance Metrics and Compliance

Effective monitoring of outsourced security in Nigeria's oil and gas sector requires performance measures that translate contractual obligations into observable, auditable and decision-relevant outcomes. Security effectiveness cannot be inferred merely from the number of guards deployed or the absence of reported incidents. Operators require a balanced measurement architecture incorporating preventive activities, operational reliability, compliance behaviour, incident outcomes and response capability. Data-driven performance frameworks are particularly valuable in geographically dispersed operations because standardized indicators enable management to compare contractors, facilities and locations while detecting persistent underperformance across multiple sites (Akin-Oluyomi & Akhigbe, 2023).

Performance metrics should combine leading and lagging indicators. Leading measures may include completed patrols, guard attendance, training compliance, equipment inspections, access-control checks, and corrective-action closure, whereas lagging measures capture breaches, theft incidents, response failures, unauthorized access, and other realized outcomes. Contemporary safety research emphasizes that leading indicators can expose weaknesses before adverse events occur, although their usefulness depends upon careful definition and interpretation within the relevant operating system (Bayramova *et al.*, 2024). This distinction is particularly important in petroleum security because low recorded incident numbers may conceal deficient preventive controls.

The offshore petroleum literature similarly demonstrates the importance of indicators capable of signalling deteriorating barriers before major events occur. Measurement systems should therefore assess both adverse outcomes and the continuing effectiveness of protective barriers rather than depending exclusively on historical incident statistics (Zhen *et al.*, 2022). In outsourced security, equivalent barrier measures could include CCTV availability, perimeter integrity, alarm functionality, patrol adherence and emergency-response readiness.

Table 3. Illustrative Security Contractor Performance Scorecard

Performance dimension	Illustrative metric	Measurement basis	Indicative management response
Guard deployment	Posts fully manned	% scheduled shifts covered	Investigate recurrent shortages
Patrol compliance	Patrols completed	% against approved schedule	Correct route or staffing failures

Response capability	Alarm response time	Average minutes per incident	Review deployment configuration
Access control	Unauthorized entries	Number per reporting period	Strengthen screening procedures
Training compliance	Mandatory training completed	% eligible personnel certified	Suspend unqualified deployment
Technology reliability	Surveillance-system uptime	% operational availability	Escalate maintenance deficiencies
Incident reporting	Reports submitted on time	% within contract timeframe	Apply reporting corrective action
Corrective actions	Findings closed promptly	% closed within deadline	Escalate persistent non-compliance

Measurement systems must also be sensitive to local operating conditions. Nigerian evidence from facilities management demonstrates that meaningful performance assessment should reflect contextual realities and incorporate financial performance, service quality and crisis-response capability rather than transplanting generic indicators without adaptation (Koleoso, Omirin & Adewunmi, 2017). Petroleum-security scorecards should consequently distinguish between urban offices, terminals, remote pipelines and production installations.

Statistical monitoring can further improve contractor oversight. Process-control principles allow managers to establish acceptable performance ranges, identify abnormal variation and distinguish isolated deviations from persistent deterioration requiring intervention (Akanbi, Ganiu & Sunday, 2022). Real-time operational data can complement such analysis by linking workforce behaviour with actual service outcomes, enabling supervisors to detect absenteeism, deployment failures or recurring procedural deviations promptly (Akhigbe, Falemi & Akin-Oluyomi, 2023).

Performance measurement must nevertheless remain connected to accountability. Outsourcing research demonstrates that shared performance indicators can strengthen coordination between service providers and clients where measures are explicitly connected to contractual expectations (De Toni *et al.*, 2007). Regulatory compliance should therefore form part of the scorecard rather than being treated as an administrative prerequisite. South African evidence illustrates that registration requirements alone do not guarantee continuing private-security compliance, underscoring the need for active oversight and verification (Ngulube, Nkwana & Buthelezi, 2024). In Nigerian petroleum operations, robust contractor monitoring should accordingly integrate operational KPIs, regulatory obligations, audit findings and corrective actions into a coherent performance-management system.

3.2 Auditing, Reporting and Accountability Systems

Auditing and reporting systems are essential to ensuring that outsourced security contractors in Nigeria's oil and gas sector remain accountable for contractual obligations, regulatory compliance and operational performance. Effective oversight requires more than periodic inspection; it demands an auditable information architecture through which deployments, patrols, incidents, corrective actions and supervisory decisions can be independently verified. Research on private security oversight in South Africa demonstrates that formal regulation alone is insufficient where accountability mechanisms are fragmented or weakly enforced, underscoring the importance of complementary internal and external controls (Berg, 2008).

Contractor audits should therefore examine staffing records, post-attendance, incident logs, equipment condition, training compliance, access-control records, response times and closure of previously identified deficiencies. Monitoring tools are effective only when reporting requirements are clearly understood and consistently applied by both purchaser and provider, because poorly designed instruments can generate information without producing meaningful oversight (Lambright, 2008). Reporting quality is equally critical: evidence from the oil and gas industry shows that disclosure usefulness depends on completeness, consistency and verifiability rather than the mere existence of reports (Comyns, 2015).

Digital systems can strengthen this accountability architecture. Blockchain-supported data exchange offers mechanisms for improving integrity, traceability and non-repudiation of operational records, thereby reducing opportunities for retrospective alteration of security information (Opara *et al.*, 2022). Attribute-based encryption can further ensure that sensitive contractor and operational data remain accessible only to personnel possessing appropriate authorization privileges (Shittu & Nabil, 2023). Likewise, RFID-enabled identification demonstrates the capacity of automated systems to generate time-stamped records of movements and transactions, principles adaptable to guard attendance, equipment control, and restricted-area access (Yusuf *et al.*, 2023).

4. Security Cost Control

4.1 Cost Drivers and Budget Management

Cost control in outsourced petroleum security requires a clear understanding of both visible contract expenditure and the less visible costs generated by the management of external service providers. In Nigeria's oil and gas sector, the principal cost drivers typically include guard wages, overtime, supervisory personnel, patrol vehicles, fuel, marine logistics, communications equipment, surveillance technologies, accommodation, training, insurance, regulatory compliance and emergency mobilization. These expenditures vary considerably according to asset location,

threat level, deployment intensity and the technological sophistication required for protection. Financial stability is therefore essential because security expenditure must be sustained even during periods of revenue pressure or operational disruption (Agwuna, 2022).

Macroeconomic conditions can significantly alter the real cost of security contracts. Inflation, exchange-rate movements and monetary conditions influence labour costs, imported surveillance equipment, vehicle parts, communications systems and financing expenses. Evidence from emerging-market economies demonstrates that interest rates, inflation dynamics and exchange-rate movements remain closely interconnected, implying that long-duration service contracts should anticipate macroeconomic volatility rather than assume stable input prices (Agwuna, Irrshad & Mazorodze, 2022).

Fuel represents another important variable because many petroleum-security arrangements depend heavily on mobile patrols, escort vehicles, generators, boats and emergency-response fleets. Nigerian evidence following fuel-price increases demonstrates substantial pass-through into transport costs, illustrating how energy-price shocks can rapidly alter mobility expenditure (Ajayi, Alaka & Tiamiyu, 2023). Security budgets should therefore identify fuel exposure separately and apply transparent adjustment mechanisms rather than allowing uncontrolled variations to accumulate within contractor invoices.

Outsourcing also generates transaction costs beyond the contractor's quoted service price. These include tender preparation, vendor evaluation, contract negotiation, mobilization, supervision, performance monitoring, dispute management and eventual contract termination. Transaction-cost economics emphasizes that external contracting is efficient only where the costs of governing the market relationship do not outweigh the benefits of outsourcing (Williamson, 1979). For petroleum operators, low headline bids may consequently prove expensive if they require intensive supervision, repeated corrective action or frequent contract variation.

Cost escalation is particularly important in complex hydrocarbon environments. Research on oil and gas megaprojects demonstrates that cost overruns arise through interactions among technical complexity, organizational structures, people, uncertainty and changing project conditions (Olaniran *et al.*, 2015). Although security services differ from capital projects, comparable dynamics arise when threat escalation, emergency deployments, scope expansion or unplanned technology requirements alter agreed expenditure.

Evidence from Ghana similarly shows that financial difficulties, poor planning, procurement delays and changing conditions can produce high cost and schedule overruns in developing-country projects (Frimpong, Oluwoye & Crawford, 2003). Nigerian petroleum operators should therefore maintain contingency provisions for credible security risks while avoiding excessive reserves that conceal inefficient spending.

Budget management should finally combine annual financial limits with continuous variance analysis. Contemporary budgeting research indicates that budgets remain valuable management-control instruments when they are used flexibly for planning, coordination and performance evaluation rather than as rigid expenditure ceilings (Libby & Lindsay, 2010). Effective security budgeting should accordingly compare approved and actual costs by site, contractor and cost category; investigate material variances; distinguish legitimate threat-driven expenditure from inefficiency; and connect financial performance with service quality. This approach enables cost discipline without undermining the level of protection required for critical petroleum assets.

4.2 Value Assessment and Contract Optimization

Value assessment in outsourced petroleum security should move beyond identifying the lowest contract price toward determining whether expenditure produces proportionate improvements in protection, reliability and operational continuity. For Nigerian oil and gas operators, value-for-money analysis should therefore compare security expenditure with measurable outcomes such as reduced incidents, improved response times, dependable asset coverage, technology availability and avoidance of operational disruption. Performance-based contracting research demonstrates that linking supplier remuneration to defined outcomes can encourage innovation and cost-efficient service delivery where performance criteria are clearly specified (Straub, 2009).

Contract optimization also requires continuous identification of waste and service inefficiency. Integrating Lean Six Sigma with reliability-centered approaches provides a framework for eliminating non-value-adding activities while preserving system reliability, thereby supporting disciplined expenditure without weakening operational resilience (Olutimehin & Ganiu, 2022). Related advances in Lean Six Sigma emphasize real-time data, root-cause analysis and process-failure reduction, principles that can be applied to excessive overtime, duplicated patrols, repeated equipment failures and avoidable contractor mobilization costs (Akanbi, Ganiu & Sunday, 2023).

Resource deployment should likewise reflect actual security demand. Optimization research demonstrates that integrated path-planning can reduce travel, congestion and inefficient resource movement through data-driven allocation mechanisms (Akanbi & Sunday, 2024). In petroleum security, analogous approaches can optimize patrol routes, vehicle utilization and response-team positioning across geographically dispersed assets.

Contract design remains central to sustaining such value. Evidence from Ghana shows that contracting-out performance depends not simply on formal agreements but on effective contract-management capacity and the ability to control opportunistic behaviour (Awortwi, 2012). Accordingly, Nigerian petroleum operators should periodically reassess staffing ratios, unit rates, technology costs, patrol frequencies and service outcomes, using performance evidence to renegotiate inefficient provisions, consolidate overlapping activities and introduce incentive mechanisms that reward demonstrable security outcomes rather than contractor inputs alone.

5. Outsourcing Governance and Future Priorities

5.1 Governance, Coordination and Operational Resilience

Governance of outsourced security in Nigeria's oil and gas sector requires a framework that clearly distributes authority, accountability and decision rights between petroleum operators, private security contractors, public security agencies, regulators and host-community structures. Because security failures can escalate rapidly across interconnected operational systems, governance should not be limited to contract administration. It should establish who owns particular risks, who is authorized to escalate incidents, how information is shared and how resources are coordinated during both routine operations and major disruptions. Research on critical-infrastructure governance demonstrates that resilience is shaped significantly by cross-sector relationships, risk ownership, information exchange and the ability of organizations to overcome institutional silos (Rydén Sonesson, Johansson & Cedergren, 2021).

Clear governance arrangements are especially important where outsourced contractors operate alongside the police, military, civil defence agencies, emergency services and company security departments. Ambiguous command structures can create duplication, delayed response and gaps in accountability. Evidence from critical-infrastructure governance indicates that institutionalized coordination and joint planning are more resilient than arrangements relying predominantly on unilateral communication or ad hoc consultation (Knodt, Fraune & Engel, 2022). Nigerian petroleum operators should therefore define command hierarchies, notification thresholds, escalation pathways, joint-operating procedures and emergency decision authorities before incidents occur.

Governance quality also depends upon leadership. Ethical leadership is particularly important where public and private actors must implement common policies across institutional boundaries, because weak accountability and inconsistent implementation can undermine formally sound governance structures (Enaifoghe, Dlamini & Agwuna, 2020). In outsourced petroleum security, leadership should reinforce integrity, lawful conduct, transparency in contractor dealings and consistent application of performance and disciplinary standards.

Operational resilience extends beyond preventing disruption. It concerns the capacity to anticipate threats, absorb shocks, adapt under pressure and restore acceptable operating conditions. Organizational resilience theory conceptualizes these capabilities through anticipation, coping and adaptation, emphasizing that organizations must learn from disturbances rather than merely return to previous operating routines (Duchek, 2020). For security contractors, this implies maintaining contingency staffing, alternative communications, backup mobility, emergency command arrangements and the ability to reconfigure deployments when threat conditions change.

Coordination becomes particularly important during system-wide crises. South Africa's experience during COVID-19 illustrates how large-scale disruption places pressure on institutional coordination, implementation capacity and continuity arrangements, reinforcing the need for adaptable governance systems during prolonged emergencies (Ikwegbue *et al.*, 2021). Petroleum operators should similarly test contractor continuity plans against scenarios involving community unrest, flooding, cyber disruption, infrastructure sabotage, fuel shortages or simultaneous incidents across multiple locations.

Multidisciplinary collaboration also improves decision quality where problems require several professional perspectives. Nigerian evidence from emergency environments demonstrates that coordinated multidisciplinary working can improve operational outcomes in complex, time-sensitive settings (Ohunyon, Ayinde & Ojukwu, 2023). In petroleum security, equivalent collaboration should connect security professionals with operations, HSE, legal, community-relations, intelligence, logistics and information-technology teams.

Resilience nevertheless requires more than detailed contingency plans. Critical-infrastructure research warns that conventional crisis-management arrangements may prove inadequate during catastrophic breakdowns, when adaptive action by frontline personnel and middle managers becomes essential (Boin & McConnell, 2007). Outsourced security governance should therefore combine disciplined procedures with sufficient delegated authority for rapid localized action. Such an approach enables Nigerian oil and gas operators to retain strategic control while ensuring that contractors, public agencies and operational teams can coordinate effectively, adapt to disruption and sustain protection of critical petroleum assets.

5.2 Technology and Future Security Strategies

Technology is progressively redefining outsourced security in petroleum operations from manpower-intensive guarding toward integrated, intelligence-led protection. For Nigeria's oil and gas sector, this transition is particularly important because pipelines, flow stations, terminals and logistics corridors extend across geographically dispersed and sometimes difficult-to-access environments. Future security strategies should therefore combine human surveillance with sensors, analytics, automated alarms, digital twins and resilient communications rather than treat technology as an isolated substitute for contractor personnel.

Wireless sensor networks offer a practical foundation for continuous pipeline surveillance. Nigerian research demonstrates that distributed sensor nodes can identify abnormal flow conditions associated with leakage and communicate observations through cloud-based monitoring architectures, thereby supporting earlier intervention than periodic physical inspection alone (Ezeja & Nwobi, 2024). Such systems could complement contractor patrols by directing mobile teams toward anomalies rather than requiring uniform surveillance intensity across extensive pipeline networks.

Digital twins represent another significant development. Real-time digital representations of infrastructure can integrate operating data with fault-detection functions, enabling abnormal conditions to be identified and investigated more systematically (Shittu *et al.*, 2023). When combined with artificial intelligence, digital twins can move monitoring toward predictive intervention, allowing operators to identify developing equipment or operational problems before they create vulnerabilities that compromise security coverage (Shittu & Shittu, 2024).

Sensor-based monitoring similarly provides an important model for automated anomaly detection. Smart fault-detection systems demonstrate how continuous sensor information can distinguish abnormal system behaviour and trigger targeted intervention, reducing dependence on reactive inspection (Sunday & Omoegun, 2022). Condition-monitoring research further illustrates how continuous acquisition and interpretation of equipment signals can identify deterioration that may otherwise remain undetected until failure occurs (Omoegun *et al.*, 2023).

Automation should also strengthen security command-and-control functions. Industrial process-control systems demonstrate the potential for programmable automation to standardize responses, coordinate alarms and reduce manual intervention in repetitive monitoring tasks (Sunday & Omoegun, 2022). SCADA-enabled automation extends this capability by integrating remote data acquisition, process visualization and centralized operational control, offering a technological basis for consolidated security and infrastructure monitoring across dispersed facilities (Omoegun *et al.*, 2024).

However, increased connectivity creates new vulnerabilities. IoT-enabled protection can improve adaptive monitoring and response but simultaneously expands the cyber-physical attack surface, requiring resilience measures that protect both field devices and communications architecture (Shittu, Olagunju & Shittu, 2024). South African research on critical-infrastructure resilience similarly emphasizes integrated cybersecurity capabilities spanning industrial control systems, IoT, cloud environments and established security frameworks rather than fragmented technical controls (Malatji, Marnewick & Von Solms, 2022).

Artificial intelligence will increasingly influence surveillance through automated anomaly detection, threat classification and prioritization of large volumes of sensor data. International critical-infrastructure research indicates that AI can strengthen cyber-threat detection and intelligent decision-making, although privacy, algorithmic bias, data security and human oversight remain material governance concerns (Raval *et al.*, 2024). For outsourced petroleum security, technology adoption should consequently be accompanied by contractual standards governing system availability, data ownership, cybersecurity, maintenance responsibility and contractor access privileges.

Future security strategy should therefore integrate people, technology and governance into a unified operating model. Contractors should increasingly be evaluated not merely by guard

numbers but by their capacity to operate interoperable surveillance technologies, maintain secure digital systems, interpret real-time information and translate automated alerts into disciplined field responses.

Conclusion

This study examined the management of outsourced security within Nigeria's oil and gas sector through the interrelated lenses of contractor selection, performance monitoring, cost control, governance, and technological modernization. The review established that effective outsourcing depends fundamentally on rigorous prequalification, evidence-based due diligence, and risk-sensitive contract design. Contractors must therefore be assessed not merely on price, but on competence, financial resilience, regulatory compliance, workforce integrity, safety performance, technological capability, and proven capacity to operate across complex petroleum environments.

The study further demonstrated that contractor effectiveness cannot be sustained without measurable performance standards. Security scorecards, audit systems, incident reporting, response-time monitoring, compliance checks, and corrective-action mechanisms are essential for converting contractual obligations into verifiable outcomes. Cost control was likewise shown to require more than expenditure reduction. Sustainable value emerges when operators distinguish legitimate security costs from inefficiency, optimize patrols and staffing, manage contract variations, and link remuneration to measurable service performance.

Governance emerged as a central condition for resilience. Clear allocation of responsibilities among operators, contractors, regulators, public security agencies, and host-community structures strengthens coordination, accountability, and crisis response. At the same time, digital twins, SCADA systems, sensors, AI-enabled monitoring, and secure data platforms are reshaping the future of petroleum security by enabling earlier detection, predictive intervention, and more targeted deployment.

Accordingly, Nigerian oil and gas operators should institutionalize risk-based contractor selection, integrated performance dashboards, lifecycle cost analysis, periodic contract optimization, and joint resilience planning. Investment in interoperable technologies should be accompanied by robust cybersecurity, data-governance, and access-control standards. Ultimately, outsourced security is most effective when treated as a strategically governed capability rather than a transactional procurement function, with contractor accountability, operational intelligence, and financial discipline integrated into a single security-management framework. This approach can strengthen asset protection, improve procurement transparency, reduce avoidable expenditure, and preserve continuity amid evolving physical, environmental, and cyber threats.

References

1. Agwuna, L., Irrshad, K. and Mazorodze, B.T. (2022) 'Assessing monetary policy via the Taylor Rule in a selection of middle-income emerging market economies: Issues and evidence', *Management and Economics Research Journal*, 8(2), pp. 1–14. DOI: [10.18639/MERJ.2022.9900060](https://doi.org/10.18639/MERJ.2022.9900060).
2. Agwuna, L.U. (2022) 'Entrepreneurship financial stability and implications', in Eniola, A.A., Iwu, C.G. and Opute, A.P. (eds.) *The Future of Entrepreneurship in Africa: Challenges and Opportunities Post-Pandemic*. Abingdon: Routledge, pp. 116–142.
3. Ajayi, O., Alaka, O.B. and Tihamiyu, R. (2023) 'Willingness to pay for shared and digitally booked transport among low-income commuters after fuel price increases', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), pp. 3059–3070.
4. Akanbi, O. and Sunday, E.A. (2024) 'An integrated path-planning and slotting optimization model for AMR-enabled high-density warehousing', *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), pp. 3226–3243. DOI: [10.62225/2583049X.2024.4.6.6181](https://doi.org/10.62225/2583049X.2024.4.6.6181).
5. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'A workforce-centric line-balancing model for throughput maximization in multi-shift operations', *Shodhshauryam: International Scientific Refereed Research Journal*, 5(3).
6. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'Comprehensive review of statistical process control (SPC) for precision weight management in global food manufacturing', *Gyanshauryam: International Scientific Refereed Research Journal*, 5(3).
7. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2023) 'Technological advances in Lean Six Sigma methodologies for reducing process failures in high-speed packaging lines', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10).
8. Akhigbe, R., Falemi, A. and Akin-Oluyomi, O.T. (2023) 'A conceptual model for improving customer experience using workforce behavior and real-time operational data'.
9. Akin-Oluyomi, O.T. and Akhigbe, R. (2022). A supply chain governance model for enhancing compliance and operational quality across retail networks. *All Multidisciplinary Journal*.
10. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'A conceptual supply chain leadership model for aligning logistics decisions with enterprise strategy'.
11. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'A proposed supply chain analytics framework for improving forecasting accuracy and reducing bottlenecks'.
12. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'An advanced framework for improving multi-site operational efficiency using data-driven performance indicators'.
13. Alaka, O.B., Bolaji, O. and Tihamiyu, 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: [10.56201/ijgem.v8.no2.2022.pg117.143](https://doi.org/10.56201/ijgem.v8.no2.2022.pg117.143).

14. Alaka, O.B., Tihamiyu, 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: [10.54660/IJMRGE.2021.2.6.1086-1101](https://doi.org/10.54660/IJMRGE.2021.2.6.1086-1101).
15. Alaka, O.B., Tihamiyu, R., Ajayi, O. and Bolaji, O. (2023) 'Multi-criteria prioritization of rural road rehabilitation using surface condition, population, and market-access indicators', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), pp. 3047–3058.
16. Ameyaw, E.E. and Chan, A.P.C. (2015) 'Risk allocation in public-private partnership water supply projects in Ghana', *Construction Management and Economics*, 33(3), pp. 187–208. DOI: [10.1080/01446193.2015.1031148](https://doi.org/10.1080/01446193.2015.1031148).
17. Awortwi, N. (2012) 'Contracting out local government services to private agents: An analysis of contract design and service delivery performance in Ghana', *International Journal of Public Administration*, 35(13), pp. 886–900. DOI: [10.1080/01900692.2012.686033](https://doi.org/10.1080/01900692.2012.686033).
18. Bayramova, A., Edwards, D.J., Roberts, C. and Rillie, I. (2024) 'Unravelling the Gordian knot of leading indicators', *Safety Science*, 177, 106603. DOI: [10.1016/j.ssci.2024.106603](https://doi.org/10.1016/j.ssci.2024.106603).
19. Berg, J. (2008) 'Holding South Africa's private security industry accountable: Mechanisms of control and challenges to oversight', *Acta Criminologica*, 21(1), pp. 87–103.
20. Bing, L., Akintoye, A., Edwards, P.J. and Hardcastle, C. (2005) 'The allocation of risk in PPP/PFI construction projects in the UK', *International Journal of Project Management*, 23(1), pp. 25–35. DOI: [10.1016/j.ijproman.2004.04.006](https://doi.org/10.1016/j.ijproman.2004.04.006).
21. 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: [10.1111/j.1468-5973.2007.00504.x](https://doi.org/10.1111/j.1468-5973.2007.00504.x).
22. 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: [10.1016/j.jclepro.2020.123583](https://doi.org/10.1016/j.jclepro.2020.123583).
23. Chinwokwu, E.C. (2018) 'An assessment of the relationship between private security companies and the police in crime prevention in Lagos Metropolis, Nigeria', *Police Journal: Theory, Practice and Principles*, 91(4), pp. 338–353. DOI: [10.1177/1461355718756413](https://doi.org/10.1177/1461355718756413).
24. Comyns, B. (2015) 'Greenhouse gas reporting quality in the oil and gas industry: A longitudinal study using the typology of “search”, “experience” and “credence” information', *Accounting, Auditing & Accountability Journal*, 28(3), pp. 403–433. DOI: [10.1108/AAAJ-10-2013-1498](https://doi.org/10.1108/AAAJ-10-2013-1498).
25. De Toni, A.F., Fornasier, A., Montagner, M. and Nonino, F. (2007) 'A performance measurement system for facility management: The case study of a medical service

- authority', *International Journal of Productivity and Performance Management*, 56(5/6), pp. 417–435. DOI: [10.1108/17410400710757123](https://doi.org/10.1108/17410400710757123).
26. Diphoorn, T.G. (2016) 'Twilight policing: Private security practices in South Africa', *The British Journal of Criminology*, 56(2), pp. 313–331. DOI: [10.1093/bjc/azv057](https://doi.org/10.1093/bjc/azv057).
27. Duchek, S. (2020) 'Organizational resilience: A capability-based conceptualization', *Business Research*, 13, pp. 215–246. DOI: [10.1007/s40685-019-0085-7](https://doi.org/10.1007/s40685-019-0085-7).
28. Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Assessing the importance of ethical leadership for policy implementation in SADC', *Journal of Economics and Behavioral Studies*, 12(6), pp. 11–20. DOI: [10.22610/jebs.v12i6\(J\).3102](https://doi.org/10.22610/jebs.v12i6(J).3102).
29. Ezeja, O.M. and Nwobi, C.G. (2024) 'A fuel pipeline monitoring and security system using wireless sensor networks (WSN)', *Nigerian Journal of Technology*, 43(3), pp. 518–525. DOI: [10.4314/njt.v43i3.14](https://doi.org/10.4314/njt.v43i3.14).
30. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations'.
31. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2023) 'A supply chain workforce optimization framework for addressing staffing volatility during rapid expansion cycles'.
32. Frimpong, Y., Oluwoye, J. and Crawford, L. (2003) 'Causes of delay and cost overruns in construction of groundwater projects in a developing country: Ghana as a case study', *International Journal of Project Management*, 21(5), pp. 321–326. DOI: [10.1016/S0263-7863\(02\)00055-8](https://doi.org/10.1016/S0263-7863(02)00055-8).
33. Ikwegbue, P.C., Enaifoghe, A.O., Maduku, H. and Agwuna, L.U. (2021) 'The challenges of COVID-19 pandemic and South Africa's response', *African Renaissance*, 18(1), pp. 271–292. DOI: [10.31920/2516-5305/2021/18n1a13](https://doi.org/10.31920/2516-5305/2021/18n1a13).
34. Jatto, A.L.A. (2024) *Oil and Gas Pipeline Infrastructure Insecurity: Vandalism, Threats, and Conflicts in the Niger Delta and the Global South*. Cham: Palgrave Macmillan. DOI: [10.1007/978-3-031-56932-6](https://doi.org/10.1007/978-3-031-56932-6).
35. Kakabadse, A. and Kakabadse, N. (2005) 'Outsourcing: Current and future trends', *Thunderbird International Business Review*, 47(2), pp. 183–204. DOI: [10.1002/tie.20048](https://doi.org/10.1002/tie.20048).
36. Knodt, M., Fraune, C. and Engel, A. (2022) 'Local governance of critical infrastructure resilience: Types of coordination in German cities', *Journal of Contingencies and Crisis Management*, 30(3), pp. 307–316. DOI: [10.1111/1468-5973.12386](https://doi.org/10.1111/1468-5973.12386).
37. Koleoso, H.A., Omirin, M.M. and Adewunmi, Y.A. (2017) 'Performance measurement scale for facilities management service in Lagos-Nigeria', *Journal of Facilities Management*, 15(2), pp. 128–152. DOI: [10.1108/JFM-04-2016-0015](https://doi.org/10.1108/JFM-04-2016-0015).
38. Lambrechts, D. and Blomquist, L.B. (2017) 'Political–security risk in the oil and gas industry: The impact of terrorism on risk management and mitigation', *Journal of Risk Research*, 20(10), pp. 1320–1337. DOI: [10.1080/13669877.2016.1153502](https://doi.org/10.1080/13669877.2016.1153502).

39. Lambright, K.T. (2008) 'Getting what you ask for: Barriers to proper use of service monitoring tools', *American Review of Public Administration*, 38(3), pp. 362–379. DOI: [10.1177/0275074007309150](https://doi.org/10.1177/0275074007309150).
40. Libby, T. and Lindsay, R.M. (2010) 'Beyond budgeting or budgeting reconsidered? A survey of North-American budgeting practice', *Management Accounting Research*, 21(1), pp. 56–75. DOI: [10.1016/j.mar.2009.10.003](https://doi.org/10.1016/j.mar.2009.10.003).
41. Malatji, M., Marnewick, A.L. and Von Solms, S. (2022) 'Cybersecurity capabilities for critical infrastructure resilience', *Information and Computer Security*, 30(2), pp. 255–279. DOI: [10.1108/ICS-06-2021-0091](https://doi.org/10.1108/ICS-06-2021-0091).
42. Ngulube, L.S.J., Nkwana, M.J. and Buthelezi, M. (2024) 'Analysis of private security companies' compliance to the private security industry's regulatory framework in Gauteng: A South African case study', *International Journal of Research in Business and Social Science*, 13(4), pp. 515–525. DOI: [10.20525/ijrbs.v13i4.3280](https://doi.org/10.20525/ijrbs.v13i4.3280).
43. Ohunyon, G., Ayinde, M. and Ojukwu, P.U. (2023) 'The impact of multidisciplinary collaboration on patient outcomes in emergency departments', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), pp. 2727–2741. DOI: [10.62225/2583049X.2023.3.6.6029](https://doi.org/10.62225/2583049X.2023.3.6.6029).
44. Olaniran, O.J., Love, P.E.D., Edwards, D., Olatunji, O.A. and Matthews, J. (2015) 'Cost overruns in hydrocarbon megaprojects: A critical review and implications for research', *Project Management Journal*, 46(6), pp. 126–138. DOI: [10.1002/pmj.21556](https://doi.org/10.1002/pmj.21556).
45. 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: [10.54660/IJMRGE.2022.3.6.983-996](https://doi.org/10.54660/IJMRGE.2022.3.6.983-996).
46. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2023) 'Vibration-based condition monitoring of rotating machinery using LabVIEW', *International Journal of Scientific Research in Civil Engineering*, 7(6), pp. 82–108. DOI: [10.32628/IJSRCE237529](https://doi.org/10.32628/IJSRCE237529).
47. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2024) 'Implementing smart automation solutions in medium-scale industries using SCADA systems', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(5), pp. 1207–1231. DOI: [10.32628/CSEIT241061242](https://doi.org/10.32628/CSEIT241061242).
48. Opara, I.S., Shittu, M.A., Adeniji, I.O. and Shittu, H. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', *IRE Journals*, 6(3), pp. 359–380. DOI: [10.64388/IREV6I3-1714041](https://doi.org/10.64388/IREV6I3-1714041).
49. Pashchenko, O., Khomenko, V., Ratov, B., Koroviaka, Y. and Rastsvietaiev, V. (2024) 'Main security threats to oil and gas infrastructure', in Ercetin, U. et al. (eds.) *Critical Infrastructure Protection in Response to Terrorist Attacks*. Amsterdam: IOS Press, pp. 109–116. DOI: [10.3233/NHSDP240009](https://doi.org/10.3233/NHSDP240009).

50. Raval, K.J., Jadav, N.K., Rathod, T., Tanwar, S., Vimal, V. and Yamsani, N. (2024) 'A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions', *International Journal of Critical Infrastructure Protection*, 44, 100647. DOI: [10.1016/j.ijcip.2023.100647](https://doi.org/10.1016/j.ijcip.2023.100647).
51. Rezazadeh, A., Talarico, L., Reniers, G., Cozzani, V. and Zhang, L. (2019) 'Applying game theory for securing oil and gas pipelines against terrorism', *Reliability Engineering & System Safety*, 191. DOI: [10.1016/j.ress.2018.04.021](https://doi.org/10.1016/j.ress.2018.04.021).
52. Rydén Sonesson, T., Johansson, J. and Cedergren, A. (2021) 'Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience', *Safety Science*, 142, 105383. DOI: [10.1016/j.ssci.2021.105383](https://doi.org/10.1016/j.ssci.2021.105383).
53. Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). DOI: [10.1109/CCWC57344.2023.10099268](https://doi.org/10.1109/CCWC57344.2023.10099268).
54. Shittu, H. and Shittu, M. (2024) 'AI-powered digital twins for predictive maintenance and operational optimization of renewable energy systems', *International Journal of Science, Architecture, Technology and Environment*, 1.
55. Shittu, H., Olagunju, F. and Shittu, M. (2024) 'Cyber physical resilience in digital substations: IoT-enabled adaptive protection for secure DER integration', *International Journal of Science, Architecture, Technology and Environment*, 1(3).
56. Shittu, M.A., Shittu, H., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real-time monitoring and fault detection in smart substations', *International Journal of Industrial Engineering*, 14(2), pp. 25–44.
57. Straub, A. (2009) 'Cost savings from performance-based maintenance contracting', *International Journal of Strategic Property Management*, 13(3), pp. 205–217. DOI: [10.3846/1648-715X.2009.13.205-217](https://doi.org/10.3846/1648-715X.2009.13.205-217).
58. 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.
59. Sunday, E.A. and Omoegun, G.O. (2022) 'Smart fault detection in HVAC systems using sensor-based monitoring', *International Journal of Scientific Research in Science, Engineering and Technology*.
60. Tihamiyu, 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: [10.54660/IJMRGE.2021.2.6.1102-1118](https://doi.org/10.54660/IJMRGE.2021.2.6.1102-1118).
61. Tihamiyu, R., Alaka, O.B., Bolaji, O. and Ajayi, O. (2023) 'Combining field survey and open geospatial data for transport infrastructure decision support in data-scarce regions', *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), pp. 3071–3084.

62. 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: [10.1080/23322039.2017.1353199](https://doi.org/10.1080/23322039.2017.1353199).
63. Williamson, O.E. (1979) 'Transaction-cost economics: The governance of contractual relations', *Journal of Law and Economics*, 22(2), pp. 233–261. DOI: [10.1086/466942](https://doi.org/10.1086/466942).
64. Yusuf, M., Akintunde, A., Habeeb, S. and Quadri, A. (2023) 'Radio Frequency Identification (RFID) based library management system', *International Journal of Technology and Systems*, 8(2), pp. 21–35. DOI: [10.47604/ijts.2041](https://doi.org/10.47604/ijts.2041).
65. Zabyelina, Y. and Kustova, I. (2015) 'Energy and conflict: Security outsourcing in the protection of critical energy infrastructures', *Cooperation and Conflict*, 50(4), pp. 531–549. DOI: [10.1177/0010836714558640](https://doi.org/10.1177/0010836714558640).
66. Zhang, S., Zhang, S., Gao, Y. and Ding, X. (2016) 'Contractual governance: Effects of risk allocation on contractors' cooperative behavior in construction projects', *Journal of Construction Engineering and Management*, 142(6), 04016005. DOI: [10.1061/\(ASCE\)CO.1943-7862.0001111](https://doi.org/10.1061/(ASCE)CO.1943-7862.0001111).
67. Zhen, X., Vinnem, J.E., Han, Y., Peng, C. and Huang, Y. (2022) 'Development and prospects of major accident indicators in the offshore petroleum sector', *Process Safety and Environmental Protection*, 160, pp. 551–562. DOI: [10.1016/j.psep.2022.02.050](https://doi.org/10.1016/j.psep.2022.02.050).