

From Analog to IP: Lessons from Large-Scale CCTV Migration and Electronic Access Control in Nigerian Corporate Headquarters

Chibuzor Amarahobu^{1*}, Festus-Michael Uwagboe², Francis Ojeakhen³

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

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

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

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

Abstract

This review examines the modernization of corporate physical-security infrastructure through the transition from legacy analog surveillance to Internet Protocol-based CCTV and integrated electronic access-control systems within Nigerian corporate headquarters. The study aims to identify the technological, operational, infrastructural, and governance lessons associated with large-scale migration and to determine the conditions required for resilient and sustainable security transformation. A structured review of relevant scholarly and professional literature published up to 2023 was undertaken, drawing on evidence concerning video surveillance, access-control technologies, cybersecurity, network infrastructure, power resilience, system integration, maintenance and organizational governance. The findings demonstrate that migration from analog to IP environments delivers substantial gains in image quality, scalability, centralized management, remote diagnostics, interoperability and analytical capability. However, these benefits are accompanied by heightened dependence on reliable electrical supply, network performance, storage capacity, cybersecurity controls and technically competent personnel. The integration of RFID, biometric authentication, electronic door controllers, alarms and CCTV further strengthens identity assurance, event verification and auditability, but also creates new vulnerabilities relating to credential compromise, firmware security, privacy, data governance and system-wide failure. The review concludes that successful modernization requires an enterprise-level approach rather than isolated equipment replacement. It recommends comprehensive legacy-system assessment, phased migration, resilient power and communications architecture, network segmentation, secure credential management, interoperable platforms, predictive maintenance, continuous workforce development and clearly defined governance responsibilities. Ultimately, long-term effectiveness depends on aligning technology, infrastructure, cybersecurity, maintenance and human capability within a continuously monitored and adaptable security-management framework capable of responding to evolving operational and digital risks.

Keywords: IP video surveillance; electronic access control; CCTV migration; cybersecurity; security resilience; Nigerian corporate security

DOI: 10.21590/ijtmh.09.04.34

1. Introduction

1.1 Evolution of Corporate Physical Security Systems

Corporate physical security has evolved from a predominantly mechanical and locally monitored function into an integrated, network-dependent discipline combining surveillance, access control, automation, analytics and cyber-physical protection. Early corporate systems relied heavily on guards, locks, keys, perimeter barriers and stand-alone analogue closed-circuit television (CCTV). Analogue cameras typically transmitted continuous video through coaxial cabling to dedicated monitors or recording devices, creating architectures that were comparatively simple but constrained by fixed cabling, limited resolution, local storage and weak interoperability. The later diffusion of digital video recorders, network video recorders and Internet Protocol (IP) cameras transformed surveillance from a closed visual-monitoring function into a scalable information system capable of remote administration, higher-resolution recording and integration with other security technologies (Damjanovski, 2014). This evolution has also increased expectations for image quality, storage continuity, auditability, rapid retrieval, centralized command, and seamless coordination between security personnel, facilities teams, information technology specialists, and risk managers.

The practical significance of CCTV also expanded as organisations increasingly used video not merely for post-incident evidence but for active monitoring, deterrence and operational oversight. Nigerian evidence demonstrates that surveillance technologies have become increasingly embedded in institutional monitoring environments, while conventional deployments may suffer effectiveness limitations when automation, system design and operational processes are inadequate (Agwi et al., 2021). Comparable African experience shows that CCTV growth has also depended upon organisational coordination, control-room capability, financing and institutional arrangements rather than camera installation alone (Minnaar, 2007). These developments are directly relevant to Nigerian corporate headquarters, where large estates may require coordinated surveillance across entrances, office floors, parking areas, perimeter zones and sensitive technical spaces.

A second major stage of evolution has been the convergence of video surveillance with electronic access control. Modern corporate security increasingly links cameras with card readers, biometric devices, electronic locks, alarms and central monitoring platforms, allowing

physical entry decisions to be associated with identities, authorisations and recorded events. Contemporary access-control architecture therefore extends beyond simple locking mechanisms toward policy-based management of ingress and egress, credential verification and remote supervisory monitoring (Brooks et al., 2018). Such integration improves situational awareness because an access event can be correlated with corresponding video evidence, thereby supporting investigation, exception handling and accountability.

The migration toward IP-based surveillance has, however, altered the security risk profile. Digital cameras, servers, switches, management software and network interfaces produce a wider attack surface than isolated analogue systems, making confidentiality, integrity and availability central to physical-security design. Research on CCTV and IP-camera vulnerabilities demonstrates that modern surveillance platforms can be exposed through insecure firmware, communications, credentials and device configurations (Costin, 2016). Likewise, large-scale IP surveillance should be understood as part of the Internet of Things, with connectivity enabling advanced functions while simultaneously introducing network-borne threats and privacy risks (Kalbo et al., 2020).

This transition also reflects the wider movement from isolated equipment toward integrated cyber-physical environments. Federated architectures can combine fixed CCTV, mobile imaging devices and other intelligent sensors, enabling distributed monitoring and richer situational intelligence (De Pascale et al., 2023). In corporate headquarters, this architectural logic supports the shift from separate security devices toward interoperable platforms in which surveillance, alarms, access events and operational data are centrally visualised.

Automation has reinforced this evolution. Integrated control environments demonstrate how formerly separate equipment can be unified through common platforms that improve interoperability, real-time data exchange and system intelligence (Sunday & Omoegun, 2022a). Similarly, sensor-based fault monitoring illustrates the value of continuous condition awareness for identifying abnormal equipment behaviour before it develops into disruptive failure (Sunday & Omoegun, 2022b). For security estates containing numerous cameras, switches, controllers and recording units, such principles encourage proactive system-health management rather than dependence on user-reported faults.

Finally, intelligent condition monitoring has strengthened the movement toward predictive security-system maintenance. Data-driven monitoring can convert equipment signals into actionable maintenance intelligence, improving reliability and reducing avoidable downtime (Omoegun et al., 2023). For Nigerian corporate headquarters migrating from analogue CCTV to IP surveillance and electronic access control, the historical trajectory is therefore not merely a replacement of cameras. It represents a deeper transformation from fragmented, locally operated security equipment into connected, software-managed and increasingly intelligent infrastructures

whose effectiveness depends on integration, network resilience, cybersecurity, maintenance discipline and informed human oversight.

1.2 Security Modernization in Nigerian Corporate Environments

Security modernization in Nigerian corporate environments reflects a shift from stand-alone protective devices toward integrated, digitally governed security ecosystems. In headquarters, modernization is shaped not only by surveillance requirements but also by the quality of institutional governance, power reliability, network infrastructure, and the capacity to maintain interconnected technologies. Nigerian evidence on IT governance shows that frameworks such as COBIT and ITIL can strengthen accountability, regulatory compliance, service continuity and control ownership, all of which are pertinent when CCTV, access-control servers and security databases become enterprise information assets (Fadero et al., 2018).

Power reliability remains a critical constraint. Corporate security platforms depend on uninterrupted electricity for cameras, network switches, storage arrays, access controllers and monitoring workstations. Research on Nigerian industrial energy systems demonstrates that decentralized solar integration can mitigate unstable grid supply and improve operational continuity, suggesting a basis for resilient power design around security infrastructure (Sunday & Omoegun, 2018). Similarly, optimized load distribution within hybrid-energy configurations illustrates how intelligent allocation and coordinated control can improve reliability under variable supply conditions, an important consideration where security devices must remain operational during utility disruptions (Sunday & Omoegun, 2019).

Modernization also requires risk-based access architecture. South African research on critical-infrastructure protection demonstrates that effective access-control design should evaluate unauthorized-entry probabilities, anomaly detection, and the suitability of biometric or digital credentials within an integrated security system (Goncalves, 2023). For Nigerian corporate headquarters, these lessons indicate that modernization should proceed as an enterprise transformation rather than a camera-replacement exercise. Successful migration therefore depends on aligning IP surveillance and electronic access control with cybersecurity policies, resilient energy provision, network segmentation, lifecycle maintenance, identity governance, and centralized monitoring. Such alignment enables physical-security investments to deliver dependable situational awareness, auditable access decisions, and continuity across complex corporate facilities.

1.3 Review Scope, Objectives, and Significance

This review examines the transition from legacy analog surveillance systems to Internet Protocol-based CCTV and electronically managed access-control environments within Nigerian corporate headquarters. Its scope encompasses the technological, operational, infrastructural, and

governance dimensions of large-scale security modernization, with particular attention to system architecture, migration planning, integration, network dependency, power resilience, cybersecurity, maintenance, user management, and lifecycle performance. The discussion is intentionally centred on complex corporate facilities where surveillance and access-control systems must operate continuously across multiple entrances, office zones, parking areas, technical rooms and restricted spaces.

The principal objective is to identify the practical lessons that emerge when organizations replace fragmented analog security infrastructure with interconnected digital platforms. Particular emphasis is placed on the factors that determine whether such migrations achieve improved visibility, reliability, scalability and control rather than merely introducing newer equipment. The review therefore evaluates the importance of phased implementation, interoperability, centralized monitoring, resilient supporting infrastructure, clearly defined access privileges, competent technical personnel and disciplined post-deployment maintenance.

The significance of this review lies in its focus on the realities of security transformation within Nigerian corporate environments, where modernization frequently occurs under conditions of uneven power reliability, legacy infrastructure, constrained technical capacity and growing cybersecurity exposure. By synthesizing these issues within a single analytical framework, the review provides a structured basis for understanding how large corporate organizations can approach CCTV migration and electronic access control as an integrated security-management programme. It also establishes a foundation for identifying transferable lessons relevant to future upgrades across similarly complex institutional and commercial facilities.

2. CCTV Migration and Access Control Integration

2.1 Legacy Analog Surveillance Infrastructure

Legacy analog surveillance infrastructure formed the technological foundation of corporate CCTV for decades and remains embedded within facilities where security estates evolved incrementally rather than through coordinated modernization. Conventional systems typically use analog cameras linked by coaxial cabling to monitors and digital video recorders. This architecture is comparatively straightforward, but its dependence on fixed cabling, localized recording and hardware-specific configurations limits scalability, flexibility and centralized management. Reviews of surveillance technology show that first-generation CCTV systems were adequate for basic monitoring but constrained recording, distribution and integration as security requirements expanded (Tsakanikas & Dagiuklas, 2018).

In Nigerian corporate headquarters, legacy surveillance systems often reflect successive procurement cycles in which cameras, recorders, power supplies and monitors were added according to immediate requirements. Such development can produce heterogeneous estates containing equipment from different manufacturers, inconsistent image standards and uneven maintenance histories. Nigerian CCTV research indicates that surveillance technologies may be hindered by infrastructural, operational and management limitations, reinforcing the need to treat legacy estates as socio-technical systems rather than collections of cameras (Nte, Gande& Uzorka, 2020). The challenge is that piecemeal expansion can create fragmented architectures whose documentation and performance are difficult to establish before migration.

Image quality represents another important limitation. Analog systems transmit continuously varying electrical signals susceptible to degradation over distance, electromagnetic interference, connector deterioration, and poor termination. When footage must support incident reconstruction, identity verification, or evidential review, degraded images can significantly reduce investigative value. Contemporary surveillance scholarship demonstrates that modern video systems increasingly depend on higher-resolution imaging, automated interpretation, and networked processing capabilities that exceed conventional analog environments (Elharrouss, Almaadeed& Al-Maadeed, 2021). These differences are consequential in large headquarters where security teams require rapid retrieval and dependable visual coverage across numerous internal and external zones.

Legacy CCTV also places substantial operational dependence on human observation. Where analytics, event correlation and automated alerting are absent, security officers must identify significant activity from multiple live feeds and manually search recorded footage after incidents. Although CCTV can contribute to deterrence and investigative effectiveness, outcomes depend strongly on monitoring, positioning and integration with broader security practices rather than camera presence alone (Piza et al., 2019). In large Nigerian facilities, this dependency may be amplified by control-room workload, inconsistent operator training and limited correlation between surveillance and access-control events.

The governance burden of aging infrastructure is equally significant. Surveillance footage contains identifiable information, and poorly controlled storage, retrieval or retention processes create privacy and accountability risks. South African experience illustrates that private CCTV operation increasingly intersects with data-protection obligations governing how recorded information is processed and managed (Ismail, 2023). Similar considerations arise when Nigerian corporations determine what legacy footage is retained, who can access recordings, and how migration affects historical archives.

Legacy architectures also reveal the difficulty of integrating isolated control systems into secure digital environments. Research on African technological transformation emphasizes that modernization requires institutional capacity, infrastructure, and effective governance alongside

technological investment (Enaifoghe, Dlamini& Agwuna, 2020). As surveillance platforms become interconnected, secure data exchange, traceability and resilience become increasingly important; research on SCADA-controlled infrastructure similarly demonstrates the limitations of centralized legacy architectures under expanding interoperability and cybersecurity requirements (Opara et al., 2022).

2.2 Transition to IP-Based Video Surveillance

The transition from analog closed-circuit television to Internet Protocol (IP)-based video surveillance represents a reconfiguration of corporate security architecture. Rather than transmitting video through dedicated point-to-point coaxial links, IP surveillance converts visual information into networked data that can be routed, stored, retrieved, and managed across shared digital infrastructure. For large Nigerian corporate headquarters, this shift enables higher-resolution imaging, centralized administration, remote diagnostics, and more flexible expansion, but it also increasingly transfers surveillance reliability to the underlying data network. Research on IP video environments shows that multiple camera streams can impose substantial bandwidth, latency and packet-loss demands, making network design and traffic management integral to surveillance performance (Go et al., 2019).

Interoperability is equally important in large-scale migration. IP surveillance estates frequently combine cameras, recorders, analytics engines and management platforms from different vendors; consequently, open standards can reduce proprietary dependence and facilitate phased modernization. ONVIF-based architectures demonstrate how standardized discovery, streaming and metadata exchange can support distributed surveillance devices while preserving extensibility across wide-area deployments (Sens et al., 2011). Within African institutional environments, CCTV design experience in Ghana further illustrates the operational value of technologically supported monitoring where camera placement, visualization and system configuration are planned around surveillance objectives rather than treated as isolated equipment decisions (Gyamfi et al., 2022).

For Nigerian organizations, the transition also creates opportunities for more intelligent infrastructure management. Digital-twin research developed partly within Nigerian engineering institutions demonstrates how connected physical assets, communication layers and analytical models can support real-time monitoring, fault detection and predictive intervention (Shittu et al., 2023). Applied to enterprise surveillance, this logic encourages continuous visibility of camera availability, storage health, switch performance and communication faults instead of dependence on periodic manual inspection.

The increased volume of digital information generated by IP systems also makes analytical coordination increasingly valuable. Data-driven frameworks can support forecasting, bottleneck identification and proactive resource allocation, principles applicable to storage planning,

bandwidth utilization, maintenance scheduling and capacity expansion in large surveillance estates (Akin-Oluyomi & Akhigbe, 2023a). Likewise, multi-site performance frameworks demonstrate the value of standardized indicators for comparing distributed operational assets and identifying inconsistencies requiring intervention (Akin-Oluyomi & Akhigbe, 2023b). Accordingly, effective analog-to-IP migration in Nigerian corporate headquarters requires more than camera replacement: it demands deliberate network architecture, interoperability standards, scalable storage, performance monitoring, cybersecurity controls, and structured lifecycle management capable of sustaining surveillance availability as the digital estate expands.

2.3 Electronic Access Control System Integration

Electronic access control integration transforms corporate security from mechanical restriction into an identity-driven architecture in which credentials, authorization rules, door hardware, alarms, and surveillance platforms operate as a coordinated system. In Nigerian corporate headquarters, this integration is valuable where large workforces, contractors, visitors and sensitive zones require differentiated access privileges. RFID provides a practical foundation because unique tags can be associated with users and read electronically, enabling automated identification, transaction logging and faster credential processing than manual registers or conventional keys (Yusuf et al., 2023).

Modern access control increasingly requires stronger authentication than possession of a single card. Multi-factor designs can combine RFID credentials with biometric verification, reducing risks associated with lost, borrowed, or cloned cards. Smart-building research demonstrates that facial recognition and RFID can be combined within a unified access framework, allowing identity verification to support broader building automation functions (Maciel et al., 2017). In South Africa, biometric deployment research similarly emphasizes that environmental conditions, user interaction, system configuration, and operational context influence whether biometric access solutions perform reliably after implementation (Lang & van der Haar, 2020).

Integration must extend beyond the reader and credential. Effective physical access control requires an architecture connecting enrollment, identity records, authorization policies, controllers, electronic locks, and audit logs while selecting authentication strength according to facility risk. Risk-based guidance for physical access control systems stresses interoperable credentials and graduated authentication mechanisms rather than identical controls for every location (Ferraiolo et al., 2018). For Nigerian corporate headquarters, this supports differentiated protection between reception areas, employee workspaces, data rooms, executive zones, and restricted facilities.

As access-control systems become networked, authorization itself becomes a cybersecurity concern. Attribute-based encryption demonstrates how access decisions can be linked to user attributes so that protected information is available only to entities possessing appropriate

permissions (Shittu & Nabil, 2023). This principle aligns with enterprise access governance, where roles, departments, clearance levels and operational responsibilities determine entitlement.

Integration with wider smart-building platforms also creates opportunities for decentralization and automation. Smart-contract architectures can provide flexible authorization management across connected building environments while reducing dependence on a single centralized decision point (Bindra et al., 2022). In large Nigerian headquarters, electronic access control should therefore be engineered as part of the broader security ecosystem, enabling credential governance, event logging, alarm escalation and CCTV correlation to function together effectively under clearly defined cybersecurity, privacy and lifecycle-management controls.

3. Migration Planning and Implementation Lessons

Electronic access control integration is a critical dimension of security modernization because it transforms entry management from isolated locks and credentials into an auditable, networked control environment. Within Nigerian corporate headquarters, an integrated architecture can connect employee credentials, RFID readers, biometric terminals, door controllers, electromagnetic locks, visitor-management systems, alarms and CCTV platforms. Nigerian experimental evidence demonstrates that RFID credentials can operate with electromagnetic locking and automatic intrusion alerts, illustrating how identification, physical locking and event notification can function within a unified access pathway (Makanjuola et al., 2022).

Modern systems increasingly combine possession-based credentials with biometric verification. RFID authentication supplemented by biometric characteristics can strengthen identity assurance because access no longer depends exclusively upon possession of a card or knowledge of a password (Huang et al., 2022). South African research similarly demonstrates the feasibility of fingerprint authentication combined with remote GSM notification, highlighting the importance of both identity confirmation and immediate security communication when abnormal entry conditions arise (Govender & Umenne, 2021). More advanced behavioural biometrics further demonstrate how physical access can potentially be authenticated using unobtrusive characteristics such as footsteps and hand movements, extending security beyond conventional cards and static physiological traits (Gupta, Kacimi & Crispo, 2022).

For corporate headquarters, however, credential sophistication alone does not create effective integration. Access events should be correlated with CCTV footage so that a card transaction, rejected credential, forced door, or biometric mismatch can automatically direct operators toward corresponding video. Secure biometric authentication models for IoT-enabled video surveillance demonstrate the value of connecting identity verification, authentication, and protected access to surveillance information within a common security architecture (Bagga et al., 2022).

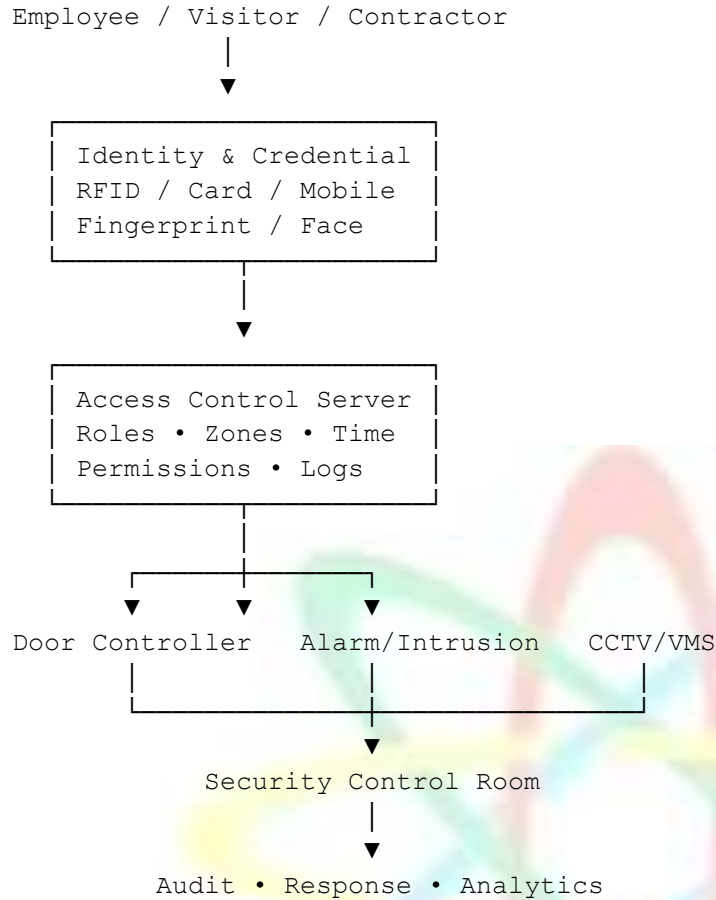


Figure 1. Illustrative integrated electronic access-control architecture

Source: Author's conceptualisation.

The integrity of this architecture depends on credential security. Studies of operational smart-card systems have shown that insecure card technology, poor configuration and inadequately maintained supporting applications can expose personal information or permit credential manipulation (Teule et al., 2020). RFID installations must likewise consider physical resilience and contingency arrangements because electronic access systems remain dependent on electrical power and functional control hardware (Đurica & Lenko, 2021). Contactless technologies have consequently gained additional relevance where organisations seek secure access while minimizing unnecessary physical interaction (Singh et al., 2022).

Table 1. Core components of integrated electronic access control. Source: Author's conceptualisation

Integration element	Primary function	Corporate security value
RFID/smart credentials	Identifies authorised users	Rapid, traceable entry
Biometrics	Verifies individual identity	Reduces credential sharing

Door controllers	Executes access decisions	Enforces zoning policies
CCTV/VMS linkage	Associates access with video	Strengthens verification
Alarm integration	Flags abnormal conditions	Accelerates intervention
Central server	Manages permissions and logs	Enables unified governance
Analytics	Detects unusual behaviour	Supports proactive investigation

Integration also generates behavioural data capable of strengthening security intelligence. Building-access records can reveal anomalous spatial and temporal patterns associated with credential impersonation, enabling access logs to become analytical inputs rather than passive records (Silva & Sichman, 2022). Governance therefore becomes central: defined ownership, permission-review cycles, audit trails and compliance controls are needed to maintain consistent access decisions across organisational units (Akin-Oluyomi & Akhigbe, 2022). Equally, lifecycle reliability should incorporate preventive maintenance, failure analysis and performance measurement so that readers, locks, controllers and supporting infrastructure remain available when required (Olutimehin & Ganiu, 2022). For Nigerian corporate headquarters, effective integration therefore rests on coordinated identity governance, CCTV correlation, cybersecurity, resilient power, reliable hardware and disciplined lifecycle management.

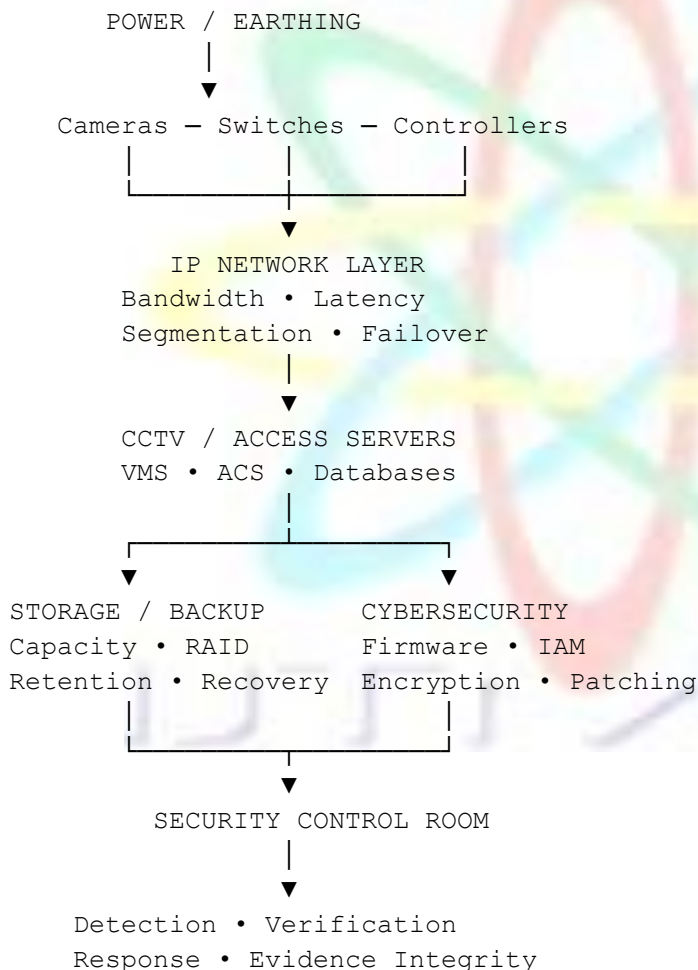
4. Operational, Cybersecurity, and Infrastructure Challenges

Large-scale migration from analog CCTV to IP-based surveillance and electronic access control creates an operational environment in which physical security becomes dependent on electricity, data networks, servers, storage, software and cyber hygiene. In Nigerian corporate headquarters, this dependency can magnify ordinary infrastructure weaknesses because a single failure in switching, power conditioning or authentication may affect multiple cameras, access points and monitoring functions simultaneously. Grounding is therefore fundamental: optimized earthing limits hazardous voltages, protects sensitive electronic equipment and improves fault performance in environments where electrical quality may be inconsistent (Adeniji et al., 2020).

Power continuity is only one layer of resilience. Network reach and stability determine whether IP cameras can transmit reliably, controllers can communicate with central servers and operators can obtain live video without interruption. Nigerian evidence on digitally mediated services shows that connectivity outside major urban centres can remain uneven, illustrating how network availability becomes an operational constraint once service delivery depends on communications infrastructure (Alaka et al., 2022). Corporate deployments consequently require capacity planning, redundant uplinks, segmented switches, UPS-backed PoE infrastructure and tested failover paths.

Cybersecurity introduces a second class of challenges. IP cameras are networked computing devices and may contain exploitable services, insecure credentials or firmware weaknesses. Penetration testing has demonstrated risks including denial-of-service, video eavesdropping and unauthorized manipulation, underscoring the need for firmware governance, credential hardening and vulnerability management (Biondi et al., 2021). More broadly, IoT security requires confidentiality, authentication, access control, privacy and trust to be engineered across heterogeneous devices rather than added after deployment (Sicari et al., 2015). South African research similarly shows that connected-device adoption raises intertwined concerns about data security, privacy and stakeholder trust, which are particularly important where corporate surveillance captures identifiable employees and visitors (Ngwenya, 2020).

Figure 2. Illustrative challenge pathways in integrated corporate security infrastructure



Source: Author's conceptualisation.

Bandwidth and storage pressures can also undermine operational performance. High-definition cameras generate continuous streams whose simultaneous transmission competes for finite

network capacity; event-driven bandwidth allocation can reduce congestion by prioritizing surveillance traffic according to operational significance (Seetanadi et al., 2021). At the storage layer, increasing camera counts, resolution and retention periods rapidly enlarge data volumes, requiring scalable architectures, efficient indexing, backup and recovery rather than simple disk expansion (Ma et al., 2018). Artificial-intelligence processing may reduce unnecessary transmission and storage by identifying relevant activity closer to the camera or processing layer, although analytical workloads themselves introduce computing and governance requirements (Nguyen et al., 2020).

Table 2. Principal operational, cybersecurity and infrastructure challenges. Source: Author's conceptualisation

Challenge domain	Typical risk	Operational consequence	Priority control
Electrical infrastructure	Outages, surges, weak grounding	Camera/controller downtime	UPS, generators, surge protection, grounding
Network capacity	Congestion and packet loss	Delayed or degraded video	VLANs, QoS, redundant switching
Cybersecurity	Weak credentials or firmware	Unauthorized access or disruption	Hardening, MFA, patching, segmentation
Storage	Capacity exhaustion	Lost retention or recording gaps	Scalable storage, RAID, monitoring
Interoperability	Vendor incompatibility	Fragmented monitoring	Standards-based integration
Access systems	Controller/server failure	Doors unavailable or uncontrolled	Local fallback and redundancy
Operations	Weak monitoring and ownership	Slow incident response	Central dashboards and escalation procedures

System availability is further threatened by single points of failure. Fault-tolerant ONVIF architectures demonstrate that NVR failure, network interruption and stream disruption can be mitigated through active backup, camera-side caching and resilient service discovery (Lin et al., 2018). Such resilience is especially important during phased migration, when legacy DVRs, IP cameras, network video recorders and access-control platforms may coexist.

Distributed infrastructure also requires trustworthy transaction and control mechanisms. Research on blockchain-enabled microgrids illustrates how decentralised systems must address scalability, interoperability, privacy and secure coordination between multiple actors and devices

(Shittu et al., 2021). In corporate security environments, comparable principles apply to audit integrity, event exchange and authorization across interconnected platforms.

Operationally, these challenges converge in the control room. Security teams must distinguish camera faults from network faults, cybersecurity incidents from configuration errors, and storage failures from power disruptions. Effective modernization therefore requires integrated monitoring, configuration baselines, asset inventories, patch schedules, redundancy testing and clear escalation ownership. The objective is not merely to keep cameras online, but to preserve trustworthy surveillance, controlled physical access and evidential continuity under foreseeable technical and cyber disruptions. Routine resilience testing should also verify generator transfer, UPS autonomy, switch recovery, controller fail-safe behaviour, timestamp synchronization and restoration procedures before faults occur during critical security operations unexpectedly.

5. Resilience, Governance, and Future Security Modernization

Resilience and governance are central to sustaining the value of large-scale CCTV migration and electronic access-control investments after commissioning. In Nigerian corporate headquarters, modernization should therefore progress beyond equipment replacement toward an enterprise security model that preserves service continuity, assigns accountability and anticipates technological obsolescence. Effective risk governance requires clear ownership of cyber and physical-security risks, defined escalation pathways, board-level oversight and continuous evaluation of control effectiveness; evidence from Nigerian financial institutions indicates that structured risk-governance mechanisms can reduce exposure to cybercrime and strengthen organizational control (Erin et al., 2020).

Future-ready security architecture must also recognize that surveillance, access control and building-management technologies increasingly operate as interconnected cyber-physical systems. Contemporary building automation research shows that expanding IP connectivity improves integration and remote management but simultaneously enlarges the attack surface, making segmentation, authentication, anomaly detection and secure protocol management essential components of resilient design (Graveto, Cruz& Simões, 2022). Cyber-resilience should consequently be engineered across management, automation and field layers, with redundancy, fail-safe operation and recovery mechanisms capable of maintaining acceptable service during cyber disruption or component failure (Li et al., 2023).

Governance is equally important at institutional level. South African cybersecurity experience demonstrates that legal frameworks, coordination, skilled personnel, privacy safeguards and sustained implementation capacity are necessary if digital-security policies are to translate into operational protection (Sutherland, 2017). For Nigerian corporate headquarters, this implies that

CCTV footage, biometric records, access logs and identity data should be governed through explicit retention schedules, access privileges, audit trails, vendor obligations and incident-response procedures rather than left solely to technical administrators.

Modernization should also become increasingly data-driven. Real-time operational information can support faster recognition of performance deviations and more responsive managerial intervention, providing a useful basis for security dashboards that track camera uptime, access-controller health, alarm frequency, storage utilization and unresolved faults (Akhigbe, Falemi& Akin-Oluyomi, 2023). Workforce continuity must accompany this technological sophistication because resilient security operations depend on trained operators, engineers and administrators who understand system dependencies, escalation procedures and cybersecurity responsibilities; integrated workforce and productivity frameworks reinforce the importance of aligning human-resource stability with operational performance (Falemi, Akhigbe& Akin-Oluyomi, 2023).

Continuous improvement should further shape lifecycle governance. Lean Six Sigma approaches augmented by real-time monitoring, predictive analytics and intelligent automation illustrate how organizations can move from reactive fault correction toward earlier detection, root-cause analysis and predictive intervention (Akanbi, Ganiu& Sunday, 2023). Applied to corporate security estates, this means analysing recurring camera outages, credential failures, false alarms, storage anomalies and maintenance delays as measurable process weaknesses.

Conclusion

This review examined the technological and organizational transition from legacy analog surveillance toward integrated IP-based CCTV and electronic access-control environments within Nigerian corporate headquarters. The study's objectives were achieved by evaluating the evolution of corporate physical-security systems, the drivers of modernization, the limitations of legacy surveillance infrastructure, the operational implications of IP migration, the integration of electronic access control, and the resilience and governance requirements necessary for sustainable modernization. Collectively, the analysis demonstrates that successful migration is not fundamentally a camera-replacement exercise, but a complex transformation of physical security into a networked, data-driven and cyber-physical capability.

The review identified several critical findings. Legacy analog environments are constrained by fragmented architectures, limited scalability, inconsistent image quality, weak interoperability and reactive maintenance practices. IP-based systems provide significant improvements in image resolution, centralized management, remote diagnostics, scalability and analytical capability, but these benefits introduce greater dependence on bandwidth, storage, electrical resilience, cybersecurity and technical competence. Electronic access-control integration further strengthens

security by connecting identity verification, credentials, door controllers, alarms and CCTV evidence within unified monitoring environments. However, such convergence also increases exposure to credential compromise, network intrusion, firmware vulnerabilities, privacy risks and system-wide failure.

The evidence therefore supports a resilience-led modernization strategy. Nigerian corporate organizations should undertake comprehensive legacy-system audits before migration, adopt phased implementation plans, strengthen network segmentation and cybersecurity controls, provide redundant power and communications infrastructure, and prioritize interoperable technologies. Governance frameworks should establish clear system ownership, access privileges, data-retention requirements, maintenance responsibilities and incident-escalation procedures. Organizations should additionally invest in continuous workforce development, predictive maintenance, real-time performance monitoring and periodic technology-refresh assessments. Ultimately, sustainable security modernization depends on integrating technology, infrastructure, governance and human capability into a continuously managed enterprise-security architecture capable of adapting to evolving operational risks, digital threats and organizational requirements.

References

1. Adeniji, I.O., Shittu, H., Elumilade, R.A., 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. 547–565. DOI: <https://doi.org/10.64388/IREV3I11-1714040>.
2. Agwi, U.C., Irhebhude, M.E. and Ogwueleka, F.N. (2021) ‘Video surveillance in examination monitoring’, *Security and Privacy*, 4(2), e144. DOI: <https://doi.org/10.1002/spy2.144>.
3. 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), pp. 463–492. No verifiable article-specific DOI identified.
4. 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’, *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(6), pp. 1322–1338. DOI: <https://doi.org/10.54660/IJMRGE.2023.4.6.1322-1338>.
5. Akin-Oluyomi, O.T. and Akhigbe, R. (2022) ‘A supply chain governance model for enhancing compliance and operational quality across retail networks’, *International*

- Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 860–878. DOI: <https://doi.org/10.54660/IJMRGE.2022.3.6.860-878>.
6. Akin-Oluyomi, O.T. and Akhigbe, R. (2023a) ‘A proposed supply chain analytics framework for improving forecasting accuracy and reducing bottlenecks’, *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1686–1703. DOI: <https://doi.org/10.62225/2583049X.2023.3.1.5338>.
 7. Akin-Oluyomi, O.T. and Akhigbe, R. (2023b) ‘An advanced framework for improving multi-site operational efficiency using data-driven performance indicators’, *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1763–1781. DOI: <https://doi.org/10.62225/2583049X.2023.3.1.5343>.
 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. Bagga, P., Mitra, A., Das, A.K., Vijayakumar, P., Park, Y. and Karuppiah, M. (2022) ‘Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system’, *Computer Communications*, 195, pp. 27–39. DOI: <https://doi.org/10.1016/j.comcom.2022.08.003>.
 10. Bindra, L., Eng, K., Ardakanian, O. and Stroulia, E. (2022) ‘Flexible, decentralised access control for smart buildings with smart contracts’, *Cyber-Physical Systems*, 8(4), pp. 286–320. DOI: <https://doi.org/10.1080/23335777.2021.1922502>.
 11. Biondi, P., Bognanni, S. and Bella, G. (2021) ‘Vulnerability assessment and penetration testing on IP camera’, in 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 1–8. IEEE. DOI: <https://doi.org/10.1109/IOTSMS53705.2021.9704890>.
 12. Brooks, C.J., Grow, C., Craig, P. and Short, D. (2018) ‘Understanding access-control and monitoring systems’, in Brooks, C.J., Grow, C., Craig, P. and Short, D. (eds.) *Cybersecurity Essentials*. Hoboken, NJ: John Wiley & Sons. DOI: <https://doi.org/10.1002/9781119369141.ch2>.
 13. Costin, A. (2016) ‘Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations’, *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, pp. 45–54. DOI: <https://doi.org/10.1145/2995289.2995290>.
 14. Damjanovski, V. (2014) *Digital Video Surveillance and Security*. 2nd edn. Oxford: Butterworth-Heinemann. DOI: <https://doi.org/10.1016/C2013-0-00650-0>.
 15. De Pascale, D., Cascavilla, G., Sangiovanni, M., Tamburri, D.A. and van den Heuvel, W.-J. (2023) ‘Internet-of-things architectures for secure cyber-physical spaces: The VISOR experience report’, *Journal of Software: Evolution and Process*, 35(7), e2511. DOI: <https://doi.org/10.1002/smr.2511>.

16. Āurica, J. and Lenko, F. (2021) ‘Comparison of the difficulty overcoming of RFID electronic access control systems and overcoming of pin tumbler locks’, *Transportation Research Procedia*, 55, pp. 1620–1626. DOI: <https://doi.org/10.1016/j.trpro.2021.07.192>.
17. Elharrouss, O., Almaadeed, N. and Al-Maadeed, S. (2021) ‘A review of video surveillance systems’, *Journal of Visual Communication and Image Representation*, 77, 103116. DOI: <https://doi.org/10.1016/j.jvcir.2021.103116>.
18. 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: [https://doi.org/10.22610/jebis.v12i6\(J\).3102](https://doi.org/10.22610/jebis.v12i6(J).3102).
19. Erin, O.A., Kolawole, A.D. and Noah, A.O. (2020) ‘Risk governance and cybercrime: The hierarchical regression approach’, *Future Business Journal*, 6, Article 12. DOI: <https://doi.org/10.1186/s43093-020-00020-1>.
20. 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>.
21. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2023) ‘A proposed framework for integrating employee retention systems with operational productivity metrics’, *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), pp. 1704–1724. DOI: <https://doi.org/10.62225/2583049X.2023.3.1.5339>.
22. Ferraiolo, H., Mehta, K.L., Ghadiali, N., Mohler, J., Johnson, V. and Brady, S. (2018) *Guidelines for the Use of PIV Credentials in Facility Access*. NIST Special Publication 800-116 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: <https://doi.org/10.6028/NIST.SP.800-116r1>.
23. Go, S.J.Y., Festin, C.A.M. and Tan, W.M. (2019) ‘An SDN-based framework for improving the performance of underprovisioned IP video surveillance networks’, *Journal of Network and Computer Applications*, 132, pp. 49–74. DOI: <https://doi.org/10.1016/j.jnca.2019.01.026>.
24. Goncalves, D.P. (2023) ‘Security access control effectiveness design’, *South African Journal of Industrial Engineering*, 34(3), pp. 84–96. DOI: <https://doi.org/10.7166/34-3-2954>.
25. Govender, T. and Umenne, P. (2021) ‘Design of a fingerprint biometric access control system with GSM functionality’, in *2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*. IEEE. DOI: <https://doi.org/10.1109/icABCD51485.2021.9519320>.
26. Graveto, V., Cruz, T. and Simões, P. (2022) ‘Security of building automation and control systems: Survey and future research directions’, *Computers & Security*, 112, 102527. DOI: <https://doi.org/10.1016/j.cose.2021.102527>.

27. Gupta, S., Kacimi, M. and Crispo, B. (2022) ‘Step & turn—A novel bimodal behavioral biometric-based user verification scheme for physical access control’, *Computers & Security*, 118, 102722. DOI: <https://doi.org/10.1016/j.cose.2022.102722>.
28. Gyamfi, E.O., Danso, J.M., Opoku-Mensah, N., Botchey, F.E., Gyamerah, S., Adom, D.K. and Awewonu, G.A. (2022) ‘Using 3D tools to design CCTV monitoring system for Ghanaian university: A case of C.K. Tedam University of Technology and Applied Sciences (CKT-UTAS)’, *Asian Journal of Research in Computer Science*, 14(4), pp. 130–146. DOI: <https://doi.org/10.9734/ajrcos/2022/v14i4298>.
29. Huang, Y., Fu, B., Peng, N., Ba, Y. and Liu, X. (2022) ‘RFID authentication system based on user biometric information’, *Applied Sciences*, 12(24), 12865. DOI: <https://doi.org/10.3390/app122412865>.
30. Ismail, N. (2023) ‘Private closed-circuit television surveillance under the Protection of Personal Information Act 4 of 2013’, *Tydskrif vir die Suid-Afrikaanse Reg*, 2023(1), pp. 20–37. DOI: <https://doi.org/10.47348/TSAR/2023/11a2>.
31. Kalbo, N., Mirsky, Y., Shabtai, A. and Elovici, Y. (2020) ‘The security of IP-based video surveillance systems’, *Sensors*, 20(17), 4806. DOI: <https://doi.org/10.3390/s20174806>.
32. Lang, D. and van der Haar, D. (2020) ‘Recommendations for biometric access control system deployment in a vehicle context in South Africa’, in Kim, K.J. and Kim, H.-Y. (eds.) *Information Science and Applications, ICISA 2019. Lecture Notes in Electrical Engineering*, 621. Singapore: Springer, pp. 305–317. DOI: https://doi.org/10.1007/978-981-15-1465-4_32.
33. Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K.S. and O’Neill, Z. (2023) ‘A critical review of cyber-physical security for building automation systems’, *Annual Reviews in Control*, 55, pp. 237–254. DOI: <https://doi.org/10.1016/j.arcontrol.2023.02.004>.
34. Lin, C.-F., Chiao, H.-T., Sheu, R.-K., Chang, Y.-S. and Yuan, S.-M. (2018) ‘A fault-tolerant ONVIF protocol extension for seamless surveillance video stream recording’, *Computer Standards & Interfaces*, 55, pp. 55–72. DOI: <https://doi.org/10.1016/j.csi.2017.04.005>.
35. Ma, S., Chen, X., Li, Z. and Yang, Y. (2018) ‘A retrieval optimized surveillance video storage system for campus application scenarios’, *Journal of Electrical and Computer Engineering*, 2018, Article 3839104. DOI: <https://doi.org/10.1155/2018/3839104>.
36. Maciel, H.S., Cardoso, I., Ramos, H.S., Rodrigues, J.J.P.C. and Aquino, A.L.L. (2017) ‘An integrated access control and lighting configuration system for smart buildings’, *Journal of Communications Software and Systems*, 13(2), pp. 101–108. DOI: <https://doi.org/10.24138/jcomss.v13i2.378>.
37. Makanjuola, P.O., Shokenu, E.S., Araromi, H.O., Idowu, P.O. and Babatunde, J.D. (2022) ‘An RFID-based access control system using electromagnetic door lock and an intruder alert system’, *Journal of Engineering Research and Reports*, 22(11), pp. 7–17. DOI: <https://doi.org/10.9734/jerr/2022/v22i1117574>.

38. Minnaar, A. (2007) 'The implementation and impact of crime prevention/crime control open street closed-circuit television surveillance in South African Central Business Districts', *Surveillance & Society*, 4(3), pp. 174–207. DOI: <https://doi.org/10.24908/ss.v4i3.3447>.
39. Nguyen, M.T., Truong, L.H. and Le, T.T.H. (2020) 'Artificial intelligence based data processing algorithm for video surveillance to empower Industry 3.5', *Computers & Industrial Engineering*, 148, 106671. DOI: <https://doi.org/10.1016/j.cie.2020.106671>.
40. Ngwenya, M. (2020) 'A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa', *Security and Privacy*, 3(5), e122. DOI: <https://doi.org/10.1002/spy2.122>.
41. Nte, N.D., Gande, G. and Uzorka, M. (2020) 'The challenges and prospects of ICTs in crime prevention and management in Nigeria: A review of CCTV cameras in Abuja', *Indonesian Journal of Criminal Law Studies*, 5(1), pp. 75–100. DOI: <https://doi.org/10.15294/ijcls.v5i1.36372>.
42. 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>.
43. 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: <https://doi.org/10.32628/IJSRCE237529>.
44. Opara, I.S., Shittu, M.A., Adeniji, I.O. and Shittu, H. (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. Piza, E.L., Welsh, B.C., Farrington, D.P. and Thomas, A.L. (2019) 'CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis', *Criminology & Public Policy*, 18(1), pp. 135–159. DOI: <https://doi.org/10.1111/1745-9133.12419>.
46. Seetanadi, G.N., Årzén, K.-E. and Maggio, M. (2021) 'Control-based event-driven bandwidth allocation scheme for video-surveillance systems', *Cyber-Physical Systems*, 7(2), pp. 111–137. DOI: <https://doi.org/10.1080/23335777.2021.1887364>.
47. Senst, T., Pätzold, M., Heras Evangelio, R., Eiselein, V., Keller, I. and Sikora, T. (2011) 'On building decentralized wide-area surveillance networks based on ONVIF', in 2011 8th IEEE International Conference on Advanced Video and Signal-Based Surveillance. IEEE. DOI: <https://doi.org/10.1109/AVSS.2011.6027365>.
48. Shittu, H. and Nabil, M. (2023) 'Smart supply chain management with attribute-based encryption access control', in 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 198–204. IEEE. DOI: <https://doi.org/10.1109/CCWC57344.2023.10099268>.

49. Shittu, H., Shittu, M., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain-based energy trading models for peer-to-peer renewable microgrids', *International Journal of Research in Electrical and Electronics Engineering*, 4(3), pp. 1–19. DOI: https://doi.org/10.34218/IJREEE_04_03_001.
50. 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 Research and Development*, 14(2), pp. 25–44. DOI: https://doi.org/10.34218/IJIERD_14_02_003.
51. Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks*, 76, pp. 146–164. DOI: <https://doi.org/10.1016/j.comnet.2014.11.008>.
52. Silva, G. and Sichman, J.S. (2022) 'Impersonation fraud detection on building access control systems: An approach based on anomalous social and spatio-temporal behaviors', *Applied Soft Computing*, 118, 108310. DOI: <https://doi.org/10.1016/j.asoc.2021.108310>.
53. Singh, D., Singh, A., Kaur, G., Chauhan, M. and Sumit (2022) 'Challenges for electronic access control systems amid pandemic: A survey', in 2022 IEEE World Conference on Applied Intelligence and Computing (AIC). IEEE, pp. 462–466. DOI: <https://doi.org/10.1109/AIC55036.2022.9848961>.
54. 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.
55. 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.
56. Sunday, E.A. and Omoegun, G.O. (2022a) '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.
57. Sunday, E.A. and Omoegun, G.O. (2022b) 'Smart fault detection in HVAC systems using sensor-based monitoring', *International Journal of Scientific Research in Science, Engineering and Technology*, 7(4), pp. 380–403. DOI: <https://doi.org/10.32628/IJSRSET229473>.
58. Sutherland, E. (2017) 'Governance of cybersecurity: The case of South Africa', *The African Journal of Information and Communication*, 20, pp. 83–112. DOI: <https://doi.org/10.23962/10539/23574>.
59. Teule, J.J., Hensel, M.F., Büttner, V., Sørensen, J.V., Melgaard, M. and Olsen, R.L. (2020) 'Examining the cyber security of a real world access control implementation', in 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, Article 9139617. DOI: <https://doi.org/10.1109/CyberSA49311.2020.9139617>.

60. Tsakanikas, V. and Dagiuklas, T. (2018) ‘Video surveillance systems-current status and future trends’, *Computers & Electrical Engineering*, 70, pp. 736–753. DOI: <https://doi.org/10.1016/j.compeleceng.2017.11.011>.
61. 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: <https://doi.org/10.47604/ijts.2041>.

