International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 09, Issue 4, (December 2023), www.ijtmh.com

Securing the Brownfield: A Retrofit-First Framework for OT Cybersecurity in Legacy Process Plants

Kelly Okogbenin*, Tedun Awi Daniel
Independent Researcher
Email: okogbeninkelly@gmail.com

Abstract

This review examines cybersecurity modernization in legacy process plants through a retrofit-first perspective that prioritizes risk reduction without assuming wholesale replacement of operational technology. It synthesizes literature on industrial control systems, supervisory control and data acquisition environments, legacy architectures, industrial protocols, asset visibility, segmentation, access control, monitoring, patch governance, standards alignment, workforce capability, vendor dependence, and cyber resilience. The analysis adopts a structured narrative review approach, integrating international scholarship with selected African and Nigerian evidence to evaluate both technical and organizational constraints affecting brownfield environments.

The findings show that legacy plants remain exposed because aging devices, insecure protocols, unsupported software, weak trust boundaries, remote connectivity, and heterogeneous architectures coexist with stringent requirements for safety, availability, deterministic performance, and long asset lifecycles. Effective modernization therefore depends on staged interventions built around asset discovery, risk prioritization, zoning, network segmentation, least-privilege access, compensating safeguards, passive monitoring, anomaly detection, disciplined incident response, and risk-informed patching. The review further demonstrates that security assurance requires alignment with recognized industrial standards, measurable maturity, cross-functional governance, workforce development, and stronger supplier accountability.

The study concludes that brownfield cybersecurity is fundamentally a resilience and lifecycle-management challenge rather than a conventional replacement exercise. Retrofit strategies are most defensible when they reduce exposure while preserving process continuity and engineering integrity. Future practice should emphasize evidence-based control selection, validated maintenance windows, scalable monitoring, digital-twin-assisted testing, and adaptive analytics. Future research should prioritize multi-site empirical studies, realistic datasets, lifecycle cost analysis, and measurable resilience outcomes that demonstrate sustained security improvement across heterogeneous legacy plants. These priorities can support safer, more proportionate modernization across critical industrial environments.

Keywords: Operational technology; Brownfield cybersecurity; Industrial control systems; Cyber resilience; Security retrofitting; Legacy process plants.

DOI: 10.21590/ijtmh20230904028

1. Introduction

1.1 Legacy Process Plants and Cybersecurity Exposure

Legacy process plants occupy a distinctive cybersecurity position because their operational technology was commonly engineered for continuity, deterministic control, equipment protection, and process safety rather than persistent exposure to hostile digital environments. Distributed control systems, supervisory control and data acquisition platforms, programmable logic controllers, remote terminal units, historians, engineering workstations, and field instrumentation frequently remain in service for decades, creating heterogeneous estates in which successive generations of proprietary and open technologies coexist. Industrial control networks also differ fundamentally from conventional information technology because timing, availability, and predictable physical response are central design requirements, while growing reliance on Ethernet and enterprise connectivity increases their exposure to external communications (Galloway & Hancke, 2013).

The brownfield condition intensifies this problem because plant owners rarely possess the operational freedom to replace complete control architectures simply because individual components are old. Capital intensity, production commitments, certification requirements, vendor dependencies, shutdown constraints, and the residual usefulness of installed equipment encourage restoration and life-extension strategies. Research on industrial equipment restoration shows that structured diagnosis, root-cause analysis, and controlled intervention can extend asset life while reducing avoidable downtime, illustrating why cybersecurity modernization in process plants must often coexist with aging physical infrastructure rather than assume wholesale replacement (Akanbi, Ganiu & Sunday, 2023).

Legacy exposure is also inseparable from the control logic through which physical processes are stabilized. Even comparatively bounded systems rely on sensors, controllers, actuators, feedback loops, supervisory interfaces, and increasingly intelligent control strategies to maintain efficiency and acceptable operating conditions. Nigerian engineering research on thermodynamic control demonstrates how operational performance depends upon coordinated control functions across connected equipment, reinforcing the broader importance of preserving functional integrity when introducing protective measures into established plants (Sunday et al., 2019).

The principal cybersecurity shift has therefore arisen not from the existence of automation itself, but from the erosion of the isolation assumptions under which many industrial systems developed. Contemporary ICS environments increasingly exchange information with corporate

networks, remote engineering services, business applications, maintenance platforms, and Internet-connected infrastructure. Such integration produces economic and operational advantages, yet simultaneously enlarges the attack surface and exposes systems designed around trusted communications to adversarial conditions for which they were not originally prepared (Knowles et al., 2015).

African industrial environments illustrate that this exposure is not confined to highly digitized economies. South African analysis of ICS and SCADA security identifies control systems as foundational to critical infrastructure while emphasizing the difficulty of securing technologies that evolved within comparatively trusted environments and later became interconnected. The problem is especially consequential in process industries because successful compromise can affect not merely information confidentiality but production continuity, environmental protection, equipment integrity, and public safety (Pretorius & van Niekerk, 2016).

The cyber-physical consequences distinguish brownfield OT risk from ordinary enterprise compromise. Attacks against SCADA environments can manipulate commands, interfere with availability, falsify process information, or influence control performance, creating pathways through which digital interference may produce physical disruption. Taxonomies of SCADA attacks accordingly stress that standardized connectivity and increasing network integration can transform otherwise localized weaknesses into system-level vulnerabilities affecting critical operational functions (Zhu, Joseph & Sastry, 2011).

Exposure is further complicated by weak security visibility and by the difficulty of translating conventional cyber-risk methods into environments governed by safety, availability, and process constraints. Reviews of SCADA risk assessment methods show substantial variation in how threats, impacts, probabilities, and controls are evaluated, indicating that brownfield plants require context-sensitive assessment rather than generic enterprise scoring. Risk must incorporate operational consequence, asset criticality, process dependencies, recoverability, and the feasibility of implementing controls without destabilizing production (Cherdantseva et al., 2016).

Finally, legacy plants should be understood as heterogeneous cyber-physical systems in which vulnerabilities emerge from interactions among computational, communication, and physical components. Security weaknesses can migrate across these layers, while defensive changes in one component may alter performance elsewhere. The diversity of technologies and tightly coupled cyber-physical relationships therefore make uniform protection difficult, particularly where obsolete devices coexist with modern analytics, remote connectivity, and digital services (Humayed et al., 2017). A retrofit-first perspective consequently begins by recognizing exposure as an architectural and lifecycle condition embedded within the operating plant itself. It therefore

treats installed complexity, operational dependence, and inherited design assumptions as starting conditions for practical cybersecurity modernization.

1.2 Evolving Threats Across Industrial OT Environments

Industrial operational technology (OT) is confronting a threat environment that has shifted from opportunistic intrusion toward deliberate campaigns capable of exploiting the interaction between digital control and physical process behavior. Legacy process plants are particularly exposed because contemporary connectivity has been layered onto systems originally engineered for deterministic operation, long service life, and trusted internal communications. The convergence of control networks with enterprise platforms, cloud services, remote maintenance, and industrial Internet of Things technologies has expanded attack surfaces and created pathways for reconnaissance, credential theft, malware delivery, lateral movement, and unauthorized command execution (Bhamare et al., 2020).

The evolution of SCADA architectures from isolated environments toward distributed, Internet-connected configurations has simultaneously increased flexibility and adversarial opportunity. Threat actors can exploit weak authentication, insecure protocols, exposed remote interfaces, misconfiguration, and poorly segmented networks to traverse from business systems toward process-control assets, while heterogeneous legacy devices can restrict deployment of contemporary defensive technologies (Yadav & Paul, 2021). Such pathways are especially consequential in brownfield plants because compromise can disrupt availability, distort operator visibility, or manipulate control actions rather than merely expose information.

State-linked operations have also demonstrated that industrial malware may be engineered around process knowledge. Stuxnet showed that a sophisticated campaign could combine multiple exploitation techniques with detailed understanding of control logic to influence physical equipment while concealing abnormal behavior from operators, fundamentally altering perceptions of cyber risk in industrial environments (Langner, 2011). More recent ransomware activity has broadened the threat spectrum by targeting availability and operational continuity. In ICS environments, outdated platforms, proprietary technologies, limited visibility, and operational constraints can impede detection and recovery, increasing the disruptive potential of extortion-driven attacks (Gazzan & Sheldon, 2023).

Threat evolution also complicates post-incident investigation. Modern SCADA environments generate evidence across distributed controllers, workstations, communications infrastructure, and proprietary devices, making attribution and reconstruction difficult when logging is inconsistent or forensic acquisition risks operational interruption (Elhoseny & Abbas, 2020). This visibility challenge is amplified as energy and industrial ecosystems adopt decentralized

digital coordination. Nigerian research on blockchain-enabled peer-to-peer microgrids illustrates the expanding use of interconnected transaction platforms and distributed energy technologies, highlighting the growing importance of trustworthy communications, access governance, interoperability, and cyber-resilience across digitally coordinated infrastructure (Shittu et al., 2021).

1.3 Brownfield Constraints on Cybersecurity Modernization

Brownfield cybersecurity modernization is constrained by a mismatch between contemporary security expectations and industrial assets designed for long operational lifecycles, deterministic control, and limited connectivity. Process plants commonly contain controllers, instruments, operating systems, and proprietary interfaces that remain productive after vendor support declines. South African research on cyber-physical systems emphasizes that long lifecycles and legacy technologies complicate security classification, lifecycle governance, and the consistent application of safeguards across interconnected operational environments (Pool & Venter, 2022).

Modernization is further restricted by the economic and technical impracticality of wholesale equipment replacement. Legacy manufacturing systems often lack native digital interfaces, standardized data models, and connectivity capabilities, yet replacing functioning machinery can impose capital costs and production disruption. Digital retrofitting consequently offers a pragmatic route for adding sensors, gateways, and interoperable communication technologies while preserving usable installed assets, although integration processes remain technically heterogeneous and insufficiently standardized (Alqoud, Schaefer & Milisavljevic-Syed, 2022).

Interoperability introduces another difficulty. Retrofitting established machinery may require additional edge devices, protocol translation, data acquisition mechanisms, and changes to organizational workflows. A holistic retrofit therefore cannot be treated as a hardware attachment exercise; it must reconcile digital strategy, multidisciplinary engineering, change management, and existing production requirements to generate sustainable operational value (Tantscher & Mayer, 2022).

Cybersecurity controls face similarly rigid operational boundaries. Industrial Internet of Things environments combine large-scale connectivity with components whose replacement cycles may span decades, while safety and productivity requirements limit aggressive security interventions. Measures such as patching, authentication changes, or network reconfiguration must therefore be evaluated against real-time performance and availability, because security actions that interrupt critical processes may create operational risks comparable to those they seek to reduce (Serror et al., 2021).

Maintenance philosophy also shapes modernization feasibility. Nigerian research on reliability-centered maintenance demonstrates that asset availability, lifecycle cost, process stability, and risk-based maintenance planning are mutually dependent, indicating that cybersecurity upgrades should be coordinated with maintenance governance rather than imposed as isolated information-technology projects (Olutimehin & Ganiu, 2022). This coordination is important where shutdown windows are infrequent, and modifications require validation.

The transition from reactive toward predictive maintenance further illustrates how brownfield plants can modernize incrementally through condition monitoring, analytics, and data-driven decision-making without abandoning serviceable equipment. Such evolution depends on readiness, sensor integration, competence, and disciplined lifecycle management, all of which also influence the practicability of cybersecurity retrofits (Sunday et al., 2020). Within a retrofit-first framework, these constraints make secure modernization a staged engineering problem in which security improvement must coexist with interoperability, reliability, maintainability, and uninterrupted process operation.

1.4 Review Scope, Objectives, and Contributions

This review is jointly conceptualized to establish a rigorous scholarly foundation for understanding cybersecurity modernization in legacy process plants through a retrofit-first lens. Reflecting the combined intellectual contribution of both authors, the review integrates operational technology security, industrial asset management, cyber-physical risk, systems resilience, and implementation governance into a unified analytical framework. Its scope encompasses aging industrial control systems, supervisory control and data acquisition platforms, programmable logic controllers, engineering workstations, field devices, industrial communications, remote-access pathways, and the digital services increasingly connected to brownfield environments.

The review pursues four interrelated objectives. First, it evaluates the evolving threat landscape affecting legacy operational technology and the pathways through which cyber incidents can disrupt physical processes. Second, it examines the structural constraints that complicate cybersecurity modernization, including obsolete equipment, interoperability limitations, vendor dependence, restricted maintenance windows, safety obligations, production continuity, and extended asset lifecycles. Third, it develops a retrofit-first framework for prioritizing practical interventions such as asset visibility, segmentation, access control, monitoring, compensating safeguards, and risk-based vulnerability management. Fourth, it assesses the governance, workforce, standards, and change-management mechanisms required to sustain these interventions across complex industrial settings.

The principal scholarly contribution lies in reframing brownfield cybersecurity as a staged resilience and modernization challenge rather than a technology-replacement problem. Through this jointly developed perspective, the review connects legacy architecture, operational criticality, lifecycle management, and layered security controls within a coherent framework intended to support proportionate, technically feasible, and operationally sustainable cybersecurity improvement in legacy process plants.

2. Brownfield OT Risk Landscape

2.1 Legacy Architectures and Inherited Security Weaknesses

Legacy process plants embody architectural assumptions formed when industrial control systems were designed for deterministic operation, availability, and equipment safety rather than exposure to hostile networks. Their control environments commonly combine programmable logic controllers, distributed control systems, supervisory control and data acquisition platforms, remote terminal units, human-machine interfaces, engineering workstations, historians, and field devices installed across different technology generations. This layered inheritance creates heterogeneous estates in which legacy operating systems, proprietary interfaces, vendor-specific configurations, and modern Ethernet-based services coexist. Such environments are difficult to secure uniformly because security capabilities vary sharply between devices, while replacing functioning assets may be operationally or economically unacceptable (McLaughlin et al., 2016).

Many inherited weaknesses originate in the historical expectation that industrial networks would remain isolated, physically protected, and operated by trusted personnel. Consequently, several industrial protocols and devices were developed without strong authentication, encryption, integrity checking, or granular authorization. As plants later adopted standard networking technologies and interconnected formerly isolated control domains, assumptions of implicit trust persisted inside architectures that had become more reachable. Industrial security therefore cannot be reduced to conventional enterprise hardening, because deterministic timing, continuous availability, equipment certification, and long replacement cycles constrain the countermeasures that can be deployed without affecting production (Cheminod, Durante & Valenzano, 2013).

SCADA evolution illustrates this architectural transition clearly. Earlier closed or specialized arrangements increasingly incorporated Internet Protocol networking, commercial operating systems, remote connectivity, and interfaces with corporate applications. The resulting architecture improved information exchange and operational efficiency but also increased dependencies between supervisory, control, and business layers. Vulnerabilities in administration, platform configuration, or communication boundaries can therefore provide

routes into systems that were not originally engineered for adversarial connectivity, while weak segmentation can magnify the consequences of compromise across otherwise distinct plant functions (Nicholson et al., 2012).

Communication architecture constitutes another inherited exposure. Contemporary SCADA implementations may integrate field networks, control centers, databases, engineering stations, and external services using combinations of legacy and standardized protocols. Security protections are uneven because protocol families developed under different assumptions regarding trust, bandwidth, computational resources, and operational urgency. Where legacy communications lack native confidentiality or authentication, modernization depends on gateways, segmentation, monitoring, or overlay protections rather than replacement of every endpoint, making architectural context central to retrofit design (Gao et al., 2014).

These weaknesses are reinforced by asset lifecycles that exceed those typical of enterprise information technology. Security updates may require vendor validation, process shutdowns, regression testing, or re-certification, and some components may no longer receive vendor support. Guidance for industrial control environments consequently emphasizes that cybersecurity controls must preserve safety, reliability, and real-time performance while recognizing platform constraints and legacy dependencies that can make conventional patch-and-replace strategies impractical (Stouffer et al., 2015).

The Nigerian automation context demonstrates how modern engineering platforms can consolidate PLC programming, visualization, diagnostics, and network configuration within integrated process-control environments. Such integration can improve engineering efficiency and interoperability, yet it also highlights the architectural concentration that arises when multiple control functions depend on interconnected software and hardware ecosystems. Brownfield security must therefore account for configuration integrity, engineering access, compatibility, and the coexistence of newer automation functions with pre-existing plant assets (Sunday & Omoegun, 2022).

African experience also shows that inherited weaknesses are shaped by governance and operating conditions as much as by technology. South African ICS/SCADA research identifies unpatched systems, legacy characteristics, remote access, limited security mechanisms, and differences between corporate IT and control networks as persistent challenges. These conditions reinforce the need for controls tailored to industrial architectures instead of mechanically transferring enterprise cybersecurity practices into process environments (Pretorius & van Niekerk, 2015).

The security problem is therefore architectural before it is merely technological. A legacy plant may contain secure individual components yet remain exposed through weak trust boundaries, insecure remote pathways, unsupported software, flat network structures, or poorly governed interconnections. Effective retrofit-first security begins by understanding these inherited relationships and identifying where compensating controls can reduce exposure without destabilizing essential operations. Reviews of SCADA cybersecurity consistently show that architecture, communication design, access pathways, and protocol behavior must be considered together because weaknesses at one layer can propagate across the cyber-physical system (Upadhyay & Sampalli, 2020).

2.2 Industrial Protocols and Persistent Attack Surfaces

Industrial communication protocols remain a persistent source of cyber exposure in brownfield operational technology (OT) because many were designed to support reliable process communication rather than operation within hostile or highly interconnected networks. Modbus is a prominent example. Its long-standing emphasis on simplicity, interoperability, and deterministic exchange has historically provided limited native protection against unauthorised reads and writes, replay, spoofing, and malicious command injection once an adversary obtains network access. Attack taxonomies demonstrate that exploitation can target programmable logic controllers (PLCs), field devices, and supervisory systems, producing effects that range from corrupted process data to direct disruption of physical operations (Huitsing et al., 2008).

Risk persists because industrial traffic often follows predictable relationships between human-machine interfaces, controllers, and remote devices. In Modbus/TCP environments, deterministic request-response patterns are operationally beneficial, yet they may also reveal device functions, register usage, polling intervals, and control semantics to an observer. Goldenberg and Wool (2013) show that protocol-aware models can identify deviations from legitimate behaviour, but their work also underscores how tightly these communications are embedded within plant operations. Consequently, outright protocol replacement may introduce unacceptable downtime, compatibility problems, or production risk, making compensating security controls more realistic in many legacy environments.

Comparable constraints affect DNP3, particularly in electric utilities and geographically distributed control systems. Earlier implementations were not designed around contemporary authentication expectations, leaving some broadcast or multicast exchanges exposed to impersonation and message manipulation. Security enhancement must therefore balance stronger authentication and cryptographic protection against constrained field devices, timing sensitivity, interoperability requirements, and the practical limitations of installed infrastructure (Amoah, Camtepe & Foo, 2016).

Table 1. Persistent protocol attack surfaces and retrofit-oriented controls

Protocol/exposure	Principal attack surface	Potential operational consequence	Retrofit-oriented security control
Modbus/Modbus TCP	Unauthenticated commands, replay, spoofing and register manipulation	False measurements, unauthorised actuation and process disruption	Segmentation, protocol-aware gateways and passive monitoring
Predictable HMI–PLC traffic	Observable polling patterns and control semantics	Reconnaissance and targeted command manipulation	Behavioural baselining and anomaly detection
DNP3	Weakly protected legacy exchanges and broadcast functions	Impersonation, message modification and false control actions	Authentication gateways and selective cryptographic protection
Ethernet-connected SCADA	Expanded routability and lateral connectivity	Network infiltration and propagation across control zones	Zoning, access control and intrusion detection
Remote supervisory access	External connectivity and credential compromise	Unauthorised control-system access	Hardened remote access and strong authentication
Legacy–digital integration	Interoperability and trust-boundary weaknesses	Integrity loss and unreliable supervisory decisions	Secure gateways, logging and integrity verification

Source: Synthesised from Huitsing et al. (2008), Goldenberg & Wool (2013), Amoah, Camtepe & Foo (2016), Shittu et al. (2022) and Diaba et al. (2023).

The same trust challenge is increasingly relevant to digitalised African power systems. In Nigeria, blockchain-assisted supervisory communication has been proposed as a means of improving integrity, traceability, auditability, and non-repudiation, while recognising that latency, scalability, interoperability, and real-time control requirements limit where such mechanisms can be safely deployed (Shittu et al., 2022). Similarly, research involving Ghanaian and Nigerian scholars indicates that expanding Ethernet connectivity, remote access, and interconnected SCADA platforms enlarge the attack surface and increase the need for advanced detection methods capable of distinguishing malicious behaviour from legitimate operational variation (Diaba et al., 2023).

Within a retrofit-first security framework, the objective is therefore not to eliminate legacy protocols indiscriminately, but to reduce their exploitability through layered safeguards. Network segmentation can restrict lateral movement; authenticated gateways can mediate insecure protocol exchanges; passive monitoring can detect suspicious traffic without interfering with control loops; anomaly detection can identify deviations from established operating patterns; and hardened remote-access mechanisms can reduce exposure from external connectivity. These controls should be engineered around production realities, preserving deterministic performance, device compatibility, and plant availability while progressively strengthening trust across heterogeneous legacy infrastructures. Protocol security in brownfield OT is thus best treated as an architectural containment problem in which vulnerabilities are isolated, monitored, and compensated for without destabilising the physical processes they support during continuous industrial operation.

2.3 Safety, Availability, and Lifecycle Constraints

Safety, availability, and lifecycle constraints define the practical boundaries within which cybersecurity modernization must occur in brownfield process plants. Unlike conventional information technology, operational technology directly governs physical processes whose interruption can endanger personnel, damage equipment, breach environmental limits, or halt production. Cybersecurity controls must therefore be evaluated not only for threat reduction but also for their effects on process safety, deterministic performance, fault tolerance, and recoverability. Research integrating safety and security engineering shows that increasingly digital control environments create interdependencies in which cyber failures can initiate or aggravate hazardous physical events, making coordinated risk assessment essential across the system lifecycle (Kriaa et al., 2015).

This interdependence is particularly significant where basic process control systems and safety instrumented systems coexist. Malicious interference with either layer can compromise protective functions, trigger unsafe operating states, or produce production outages; consequently, cyber-risk identification must account for accident scenarios, safety barriers, and the potential degradation of independent protection layers rather than treating cybersecurity as an isolated information-security function (Iaiani, Tugnoli & Cozzani, 2023).

Availability imposes an equally stringent constraint. Legacy SCADA and distributed control systems often support continuous operations in which unscheduled downtime carries economic and safety consequences. Risk assessment must therefore balance the probability and impact of cyber compromise against the operational consequences of security interventions, particularly when patching, configuration changes, or device replacement require shutdowns, validation, or vendor involvement (Ralston, Graham & Hieb, 2007).

The Nigerian power context further illustrates how physical reliability remains inseparable from secure modernization. Grounding design influences fault-current paths, protection-system performance, equipment integrity, and personnel safety, while emerging-market constraints require solutions that reconcile engineering performance with cost and lifecycle realities. Such considerations reinforce the need to sequence cybersecurity retrofits around established protection, maintenance, and reliability requirements rather than disrupt critical electrical functions (Adeniji et al., 2020).

Operational continuity also depends on organizational capability. Evidence from Egypt's downstream oil and gas sector indicates that cybersecurity governance, awareness, structured controls, and protection of critical information assets are important as industrial operations become more digitally connected and remotely managed (Shohoud, 2023). For retrofit-first cybersecurity, lifecycle planning must consequently integrate cyber risk with safety assurance, maintenance windows, obsolescence management, spare-part availability, vendor support, and recovery requirements. This approach allows legacy plants to strengthen resilience progressively while preserving the process integrity and availability on which safe production depends.

3. Retrofit-First Cybersecurity Architecture

3.1 Asset Discovery, Zoning, and Risk Prioritization

Asset discovery is foundational to a retrofit-first cybersecurity architecture because brownfield plants cannot protect assets that are unknown, misclassified, or absent from engineering records. Legacy process environments accumulate undocumented programmable logic controllers, remote terminal units, switches, engineering laptops, protocol converters, virtual machines, and vendor-installed appliances through successive maintenance cycles. The security problem is not merely to enumerate devices, but to establish visibility of device identity, function, communication relationships, firmware, ownership, and process criticality. Automated discovery research has shown that incomplete inventories weaken defensive planning, while intrusive scanning can itself threaten fragile operational equipment, making discovery methods sensitive to the availability requirements of industrial control systems (Wedgbury & Jones, 2015).

For brownfield facilities, passive discovery is especially suitable because it observes network traffic without deliberately interrogating field devices. By examining addresses, protocols, ports, communication patterns, and topology, passive monitoring can construct inventories while reducing the possibility of destabilising legacy controllers. Experimental work on passive scanning demonstrates its value for identifying industrial assets and reconstructing network relationships, although recognition accuracy depends on protocol visibility, traffic diversity, and device fingerprints (Thomas, Marali & Reddy, 2022). Asset records should consequently be

treated as living operational datasets, reconciled against engineering drawings, maintenance systems, configuration repositories, and physical verification rather than as one-time audit outputs.

Visibility becomes useful when assets are differentiated by operational importance. Critical-asset identification requires more than vulnerability counts because two technically similar devices may have different consequences if compromised. Situational-awareness research emphasises the need to connect asset information with functional roles, dependencies, failure consequences, and system state so that operators can distinguish ordinary components from assets whose loss would impair control, safety, or service continuity (Alrowaili, Saxena & Srivastava, 2023). This is important in brownfield plants, where obscure gateways or engineering stations may constitute high-value attack paths despite appearing peripheral in conventional inventories.

Risk prioritisation should translate asset visibility into an ordered programme of protection. Asset-focused risk management provides a basis by considering vulnerabilities, threats, interdependencies, and cascading effects rather than evaluating components in isolation. Such methods permit scarce security resources to be concentrated on assets whose compromise could propagate operational disruption or affect business continuity (Kure & Islam, 2019). Prioritisation should incorporate process consequence, exploitability, exposure, recovery difficulty, safety significance, connectivity, and dependency, producing a risk register revised as plant configurations and threat conditions change.

Zoning provides the architectural bridge between discovery and protection. Instead of treating a brownfield network as a homogeneous perimeter, assets can be grouped according to function, trust requirement, process consequence, access need, and criticality, with communications between groups constrained through controlled pathways. In process plants, risk-informed segmentation can reduce the possibility that compromise of one control area propagates into other operational units; modelling of cyber-induced domino effects demonstrates that selected ICS segmentation can increase plant robustness by limiting escalation across interconnected units (Arief, Khakzad & Pieters, 2020).

Regional operating conditions reinforce disciplined mapping. South African SCADA research documented vulnerable communication pathways, Internet exposure, weak administration, and legacy practices across critical infrastructure, illustrating why plant-specific discovery must identify not only devices but also electronic access points and inherited trust relationships (Chileshe & van Heerden, 2012). In Nigeria, emerging approaches to zero-trust protection of industrial energy networks similarly emphasise continuous verification, least privilege, behavioural visibility, and policy enforcement, principles that depend on knowing which assets

and communication relationships are legitimate before access decisions can be meaningfully enforced (James, Idika & Enyejo, 2023).

Risk prioritisation must remain tied to organisational decision-making. Cyber risks should be ranked in terms that allow engineering, operations, safety, and management functions to compare response options, allocate resources, and determine which exposures require mitigation, transfer, acceptance, or monitoring. Structured prioritisation helps distinguish urgent risks from tolerable weaknesses and prevents vulnerability severity scores from becoming substitutes for operational consequence analysis (Quinn et al., 2022). Within a retrofit-first framework, asset discovery, zoning, and risk prioritisation operate as a continuous cycle: visibility reveals dependencies, dependencies shape zones, and risk determines where limited retrofit effort should be applied first without disrupting essential production in practice today.

3.2 Segmentation, Access Control, and Compensating Safeguards

Segmentation, access control, and compensating safeguards form the operational core of a retrofit-first cybersecurity architecture because legacy plants often cannot replace vulnerable devices or introduce disruptive controls without affecting production. Effective segmentation begins by grouping assets according to process function, criticality, trust requirement, and communication dependency, then restricting traffic between zones through controlled conduits. For resource-constrained manufacturing environments, security segmentation offers a practical means of reducing lateral movement and limiting compromise while preserving essential industrial communications (Powell et al., 2023).

Access control should complement segmentation by enforcing least privilege at user, device, application, and service levels. Traditional role-based models can become inflexible where contractors, vendors, operators, engineers, and automated processes require different permissions under changing conditions. Attribute-based approaches can provide finer authorization decisions using identity, role, device state, location, time, and operational context, thereby supporting centrally governed access without assuming every legacy endpoint can enforce modern controls natively (Yalcinkaya, Maffei & Onori, 2017).

The same logic extends to cryptographically protected authorization. Attribute-based encryption can bind access to defined user or system characteristics, allowing sensitive operational information to remain protected across distributed environments. Nigerian-led research demonstrates how attribute-driven encryption can strengthen confidentiality and access governance in interconnected systems, offering principles adaptable to industrial data exchanges where centralized trust is undesirable or impractical (Shittu & Nabil, 2023).

Brownfield plants must also accommodate legitimate emergency access. Strict authorization can become unsafe if it prevents timely intervention during abnormal conditions. Break-glass mechanisms provide controlled exceptions while preserving logging, accountability, and policy enforcement, enabling emergency users to obtain necessary access without permanently weakening normal restrictions (Tu et al., 2021).

Remote access represents another critical trust boundary. Zero-trust architecture rejects implicit confidence based solely on network location and instead requires continuous authentication, authorization, device validation, and policy-based access. For legacy OT, these principles can be implemented through jump hosts, multifactor authentication, brokered vendor sessions, session recording, and tightly scoped privileges rather than wholesale platform replacement (Rose et a., 2020).

Where direct remediation remains impossible, compensating safeguards become essential. Egyptian research using ICS and SCADA honeypots illustrates how layered defenses can improve visibility into hostile behavior and support detection without altering core control logic (Mesbah et al., 2023). Combined with allowlisting, protocol-aware firewalls, passive monitoring, secure gateways, and controlled remote-access paths, these measures enable incremental risk reduction while maintaining deterministic performance and availability in legacy process operations and reliability.

4. Operationalizing Retrofit Security Controls

4.1 Monitoring, Detection, and Incident Response

Monitoring in brownfield operational technology must reconcile two imperatives: sufficient visibility to recognize malicious behavior and minimal intrusion into fragile controllers or time-sensitive processes. A retrofit-first architecture favors passive telemetry, network-flow observation, event collection, and process-variable monitoring. Digital twins strengthen this model by maintaining synchronized representations of assets, enabling deviations between expected and observed states to be examined without directly manipulating production equipment. For industrial control systems, this creates an analytical layer for identifying anomalous behavior while preserving plant availability (Dietz & Pernul, 2020).

Real-time monitoring becomes more valuable when cyber indicators are correlated with equipment condition and process behavior. In smart substations, digital-twin models can combine operational measurements, equipment states, and fault signatures to identify deviations that conventional alarms may miss. Within legacy process plants, a suspicious command, network session, or configuration change should therefore be interpreted alongside process-state

changes, engineering activity, and asset health rather than as an isolated IT event. This cross-domain observability improves discrimination between maintenance and harmful intervention (Shittu et a., 2023).

Sensor-based diagnostics likewise demonstrate why trustworthy telemetry is fundamental to OT detection. Monitoring frameworks that evaluate temperature, pressure, vibration, flow, and related variables can establish behavioral baselines and identify abnormal operating conditions. Although developed for HVAC environments, sensor-driven fault detection illustrates the value of combining multiple measurements, trend analysis, and automated diagnostics, capabilities transferable to cyber-physical monitoring where malicious actions may resemble equipment degradation or control instability (Sunday & Omoegun, 2022).

Condition monitoring provides another detection layer because cyber incidents may manifest through physical consequences rather than obvious malware signatures. Vibration-based monitoring of rotating machinery demonstrates how continuous measurement can reveal changes in equipment behavior that warrant investigation. In a retrofit-first security model, such operational data can complement packet inspection and security logs, allowing analysts to correlate abnormal network activity with physical deviations and reduce dependence on purely signature-based detection (Omoegun et al., 2023).

Advanced anomaly detection can improve coverage where static signatures are ineffective against previously unseen attacks. Federated learning offers a means of developing detection models across distributed industrial sites without centralizing all operational data, while explainability can help operators understand why traffic or process activity has been classified as anomalous. This is important in safety-critical OT, where opaque alerts may be difficult to trust and excessive false positives can generate alarm fatigue (Huong et al., 2022).

Detection architecture should combine rather than privilege individual analytical techniques. Signature-based methods remain effective for known malicious patterns, anomaly-based methods can identify deviations from established behavior, and hybrid systems can improve coverage across changing threats. A systematic assessment of intrusion-detection research shows that each approach presents trade-offs involving false alarms, computational cost, training-data quality, and generalizability, reinforcing the need for layered monitoring matched to operational characteristics (Abdulganiyu, Ait Tchakoucht & Saheed, 2023).

Incident response begins before an incident occurs. OT organizations require escalation paths, communication responsibilities, evidence-preservation procedures, containment options, and recovery criteria that account for safety and production continuity. Cyber-defense research emphasizes that industrial response must integrate technical controls with situational awareness

and coordinated action, because indiscriminate isolation or shutdown decisions may create additional operational hazards. Monitoring should therefore generate decision-quality evidence rather than merely increase alert volume (Rubio et al., 2019).

Forensics must also accommodate legacy constraints. Replication-based digital twins can preserve and reproduce aspects of system state for post-incident analysis, reducing the need for invasive forensic activity on operational assets. Such capabilities support timeline reconstruction, hypothesis testing, and evidence analysis while minimizing interference with production systems (Dietz, Englbrecht & Pernul, 2021). Within retrofit-first practice, monitoring, detection, and incident response should therefore operate as a continuous loop in which passive visibility establishes baselines, analytics identify deviations, human judgment validates significance, and prepared response procedures contain threats while preserving safe plant operation.

4.2 Patch Governance and Vulnerability Mitigation

Patch governance in brownfield operational technology requires a different logic from conventional enterprise patching because remediation itself can introduce production, safety, and compatibility risks. Legacy controllers, engineering workstations, historians, and vendor-specific applications may depend on obsolete operating systems or validated software combinations that cannot be altered without retesting the surrounding process. Accordingly, effective governance should begin with an asset inventory, vulnerability intelligence, ownership assignments, and criteria that distinguish exploitable weaknesses from lower-priority exposures whose remediation can be deferred safely (Souppaya & Scarfone, 2022).

Patch prioritization should be consequence-driven rather than based solely on nominal severity scores. In industrial environments, vulnerability criticality is shaped by asset function, network position, exploit availability, process dependency, compensating controls, and the operational cost of downtime. SmartPatch demonstrates the value of combining architectural dependencies, attacker behavior, patch interdependencies, and residual impact when selecting remediation order, thereby supporting defensible decisions in resource-constrained ICS environments (Yadav et al., 2022).

Execution must then be synchronized with maintenance governance. International practice for complex ICS stresses staged validation, vendor consultation, rollback planning, test environments, and scheduled deployment windows because a technically correct patch can still disrupt deterministic behavior, invalidate configurations, or create new incompatibilities (Gentile & Serio, 2019). Where production shutdowns are infrequent, organizations should bundle approved changes into planned outages while retaining emergency procedures for actively exploited vulnerabilities.

Vulnerability assessment must also account for the peculiarities of SCADA environments. Comparative research shows that patch management is often underemphasized because availability requirements make uncontrolled remediation hazardous, reinforcing the need to combine vulnerability identification with prioritization, verification, and alternative safeguards when patching cannot proceed immediately (Qassim et al., 2019).

For Nigerian manufacturing environments, process-improvement research demonstrates how structured failure analysis, real-time monitoring, predictive techniques, and disciplined change control can reduce process disruption and support intervention decisions in high-speed production systems (Akanbi, Ganiu & Sunday, 2023). These principles complement cybersecurity remediation by emphasizing evidence-based change rather than indiscriminate modification.

At the organizational level, South African critical-infrastructure research highlights the importance of governance capabilities, resilience planning, coordinated responsibilities, and cyber readiness across interconnected IT and ICS environments (Malatji, Marnewick & Von Solms, 2022). Within a retrofit-first framework, unpatchable or deferred vulnerabilities should therefore trigger compensating safeguards such as segmentation, allowlisting, protocol filtering, restricted remote access, enhanced monitoring, and configuration hardening. Patch governance thus becomes a continuous risk-management discipline aligned with operational windows, safety assurance, vendor support, and lifecycle realities.

5. Governance and Implementation Strategy

5.1 Standards Alignment and Security Assurance

Standards alignment in brownfield operational technology should be treated as a mechanism for translating cybersecurity intent into engineering practice rather than as a documentary compliance exercise. Legacy process plants contain heterogeneous controllers, safety systems, supervisory platforms, vendor appliances, and unsupported operating environments, so assurance depends on selecting controls that remain technically feasible without compromising availability. The NIST Cybersecurity Framework provides a risk-oriented structure for organizing activities across Identify, Protect, Detect, Respond, and Recover, allowing asset owners to map existing practices, identify gaps, and define target profiles that reflect operational priorities rather than impose uniform remediation across dissimilar assets (National Institute of Standards and Technology, 2018).

For industrial environments, ISA/IEC 62443 provides a more specific basis for structuring security requirements around zones, conduits, security levels, component capabilities, secure

development practices, and lifecycle responsibilities. Comparative analysis shows substantial overlap between ISA/IEC 62443, ISO/IEC 27001, and other cybersecurity standards, but also important differences in scope and control granularity; consequently, organizations can reduce duplicated effort by cross-mapping requirements and maintaining a unified evidence model for audits and engineering assurance (Djebbar & Nordström, 2023).

Risk assessment is central to this alignment. IEC 62443-3-2 emphasizes defining systems under consideration, establishing zones and conduits, evaluating cyber risk, and assigning target security levels according to tolerable risk. In chemical and process industries, such an approach is valuable because security decisions must account for physical consequence, process safety, operational dependency, and threat exposure rather than rely solely on generic vulnerability severity (Cusimano, 2022). A retrofit-first program should therefore convert standards into prioritized engineering requirements tied to asset criticality and plant-specific risk scenarios.

Security assurance must also demonstrate that controls continue to operate as intended after implementation. Maturity assessment provides a practical bridge between formal standards and operational evidence by examining whether practices are institutionalized, measured, reviewed, and improved. Smart-grid research shows that cyber-hygiene maturity models can quantify organizational, infrastructure, and personnel capabilities, helping operators identify gaps between current and desired security states and track progressive improvement over time (Skarga-Bandurova, Kotsiuba & Velasco, 2021).

African research similarly underscores the importance of measuring resilience rather than assuming that policy adoption equals effective protection. A cybersecurity resilience maturity framework developed with Nigerian participation proposes evaluating the existence, effectiveness, and efficiency of security controls against defined resilience objectives, thereby supporting evidence-based decisions about where capability improvement is most urgent (Mbanaso, Abrahams & Apene, 2019). Such measurement is especially relevant to brownfield plants, where full conformity may require phased implementation supported by compensating safeguards.

Governance determines whether standards remain embedded in routine operations. Nigerian research on supply-chain governance emphasizes accountability, compliance structures, performance monitoring, and coordinated oversight across distributed operations, principles that translate well to OT environments involving asset owners, system integrators, maintenance contractors, and equipment vendors (Akin-Oluyomi & Akhigbe, 2022). In parallel, Southern African scholarship highlights the role of ethical leadership and policy implementation in converting formal institutional commitments into consistent practice, reinforcing the need for

clear authority, accountability, and implementation discipline in technology governance (Enaifoghe, Dlamini & Agwuna, 2020).

Sector-specific policy alignment is equally important. Analysis of South Africa's water and wastewater cybersecurity environment shows that critical infrastructure protection requires coordination between national policy, sector responsibilities, organizational governance, and operational implementation rather than isolated technical controls (Malatji, Marnewick & von Solms, 2020). For legacy process plants, security assurance should therefore combine standards mapping, risk-based control selection, documented exceptions, evidence of testing, maturity measurement, supplier obligations, and periodic reassessment. This creates an auditable assurance chain in which every retrofit decision can be traced to risk, control intent, implementation evidence, and operational performance, enabling cybersecurity improvement without treating certification alone as proof of resilience.

5.2 Workforce, Vendors, and Change Management

Workforce capability is a decisive condition for sustainable cybersecurity modernization in brownfield process plants because technical controls depend on people who understand both cyber risk and the operational consequences of intervention. Legacy environments frequently rely on tacit knowledge held by experienced operators, maintenance engineers, automation specialists, and contractors; losing that knowledge can weaken troubleshooting, configuration control, and safe recovery. Structured capability development therefore requires role-specific training, cross-functional learning, succession planning, and competency pathways that connect workforce development with distributed operational requirements (Falemi, Akhigbe & Akin-Oluyomi, 2020).

Retention is equally important because OT cybersecurity depends on continuity of plant-specific expertise. High turnover can fragment knowledge of obsolete platforms, undocumented interfaces, vendor workarounds, and historical configuration decisions. Linking retention systems with productivity and operational performance provides a basis for preserving institutional knowledge while strengthening accountability and workforce stability in complex environments (Falemi, Akhigbe & Akin-Oluyomi, 2023).

Leadership must convert technical modernization into coordinated organizational change. Retrofit programs require priorities that align engineering, cybersecurity, procurement, operations, and executive decision-making, particularly when interventions compete with production targets and maintenance budgets. Leadership models that connect operational decisions with enterprise strategy are therefore relevant to sequencing cybersecurity investments and resolving cross-functional trade-offs (Akin-Oluyomi & Akhigbe, 2023).

Vendors introduce another critical dependency. Original equipment manufacturers, integrators, software suppliers, and maintenance contractors may retain privileged access or control essential updates, creating supply-chain pathways that must be governed through due diligence, contractual security requirements, access restrictions, vulnerability disclosure, and lifecycle support obligations. Cybersecurity supply-chain risk management accordingly requires organizations to evaluate supplier practices and maintain visibility across externally sourced products and services (Boyens et al., 2022).

Organizational culture determines whether these controls become routine practice. South African research demonstrates that information-security culture can be assessed through employee attitudes, awareness, behavior, and organizational practices, reinforcing the importance of embedding secure conduct within daily work rather than relying exclusively on policy documents (Da Veiga & Eloff, 2010).

Change management should therefore combine communication, training, leadership reinforcement, feedback, and measurable behavioral expectations. Cybersecurity culture research shows that employee behavior is shaped by management commitment, awareness activities, communication, and organizational norms, making sustained behavioral change essential to effective security implementation (Alshaikh, 2020). In retrofit-first OT environments, workforce development, vendor governance, and cultural change should proceed together so that new controls are understood, accepted, maintained, and safely integrated into established operating routines throughout the remaining lifecycle of critical plant assets.

6. Research Gaps and Future Priorities

6.1 Evidence Gaps in Brownfield Cybersecurity

Evidence gaps in brownfield cybersecurity arise less from the absence of proposed controls than from the limited empirical basis for determining which controls remain effective under constraints of ageing industrial plants. Much literature concentrates on technical countermeasures, while implementation evidence from long-lived plants are sparse. Nigerian-led scholarship has argued that industrial control system protection is frequently treated as a predominantly technological problem, leaving people, processes, governance, and evolving operational conditions insufficiently integrated into security design and evaluation (Ani et al., 2018).

A second gap concerns the representativeness of experimental evidence. Security mechanisms are commonly evaluated using laboratory platforms, simulated traffic, or datasets because direct experimentation on plants can introduce unacceptable safety and continuity risks. Yet testbeds

differ in physical fidelity, protocol coverage, device diversity, scalability, and process realism, which limits comparability of reported results. Surveys of ICS testbeds and datasets show that many benchmark environments represent narrow configurations and attack classes, making it difficult to infer whether reported performance would persist across brownfield estates (Conti, Donadel & Turrin, 2021).

Dataset limitations compound this problem. SCADA research continues to depend heavily on datasets generated in controlled conditions, while traces from production systems remain scarce because asset owners are reluctant to expose sensitive architectures and incident records. Reviews of SCADA security research identify inadequate dataset diversity, limited coverage of evolving attack vectors, and insufficient validation across different operating conditions as barriers to robust comparative evaluation (Alanazi, Mahmood & Chowdhury, 2023).

Testbed research has improved experimental accessibility, but representational gaps remain. Physical, virtual, simulated, and hybrid environments offer different compromises between cost, reproducibility, safety, and realism, and many cannot reproduce complete plant hierarchies, legacy device interactions, or long-duration operating variability. Consequently, cybersecurity results obtained within controlled facilities require cautious interpretation before being translated into brownfield deployment decisions (Pospisil et al., 2021).

The shortage of adaptable, high-fidelity evaluation environments has prompted development of configurable frameworks that emulate industrial components, network architectures, physical processes, and multiple attack types. Such platforms improve reproducibility and reduce experimentation risk, but their emergence also demonstrates that scalable validation across realistic industrial configurations remains unresolved when proprietary protocols and obsolete technologies must be represented accurately (Dehlaghi-Ghadim et al., 2023).

A related weakness is the imbalance between academic security research and recurrent weaknesses observed in operational environments. Reviews of industrial cyber-physical systems indicate that research attention often concentrates on intrusion detection and machine-learning techniques even though real-world vulnerability reports repeatedly identify weak boundary protection, deficient policies, outdated mechanisms, and insufficiently adaptive controls. Technical novelty is therefore not always matched by evidence that proposed mechanisms address persistent operational weaknesses (Kayan et al., 2022).

Implementation evidence from African industrial environments is also limited. Egyptian work demonstrating secured cloud-SCADA integration provides applied evidence, yet it illustrates how published implementations are often architecture-specific and difficult to generalize to plants containing unsupported controllers, proprietary communications, and mixed-generation

automation assets (Osman, Hashem & Eltokhy, 2022). Broader multi-site studies are needed across diverse regulatory, technological, and resource settings.

Finally, contemporary methodological reviews identify open problems involving dataset quality, model generalization, adversarial adaptation, process-aware detection, and validation of countermeasures under realistic operating conditions (Canonico & Sperlì, 2023). Brownfield cybersecurity research consequently needs stronger field-based evidence linking retrofit controls to measurable reductions in risk, downtime, recovery time, safety exposure, and lifecycle cost. Comparative studies should test segmentation, access controls, monitoring, compensating safeguards, and patch deferral strategies across representative legacy architectures, while reporting implementation burden, false-positive rates, maintainability, and operational side effects. Such evidence would allow retrofit-first cybersecurity to progress from conceptually sound guidance toward empirically validated practice.

6.2 Adaptive, Resilient, and Scalable Retrofits

Adaptive, resilient, and scalable retrofits represent the next stage of brownfield OT cybersecurity because static controls cannot adequately address changing threats, evolving process configurations, and heterogeneous legacy estates. A retrofit-first architecture should therefore incorporate mechanisms that can adjust protection according to operational context while preserving deterministic performance. Adaptive anomaly detection offers one pathway by learning behavioural patterns within industrial control environments and recalibrating detection as system conditions change, reducing dependence on fixed signatures that may become ineffective against novel attacks (Vávra et al., 2021).

Resilience extends beyond prevention to the capacity to anticipate, withstand, recover from, and adapt after cyber disruption. Industrial-network research shows that resilient architectures require coordinated defense, anomaly detection, failure management, survivability, and measurable recovery capabilities rather than isolated security products. For brownfield plants, this implies designing retrofit controls around graceful degradation, rapid restoration, redundancy, and continued operation of essential functions when some components are compromised (Alrumaih et al., 2023).

Digital twins can strengthen this adaptive model by providing virtual representations in which configuration changes, attacks, and recovery actions can be evaluated before deployment to production assets. Their integration with cybersecurity supports situational awareness, experimentation, and resilience planning without exposing fragile legacy equipment to unnecessary intervention (Faleiro et al., 2022).

Scalability also requires consistent analytics across multiple plants without eliminating local operational context. Nigerian research on predictive and prescriptive analytics demonstrates how real-time data, forecasting, and machine-learning methods can support proactive decisions and identify emerging bottlenecks, principles applicable to risk-informed cyber monitoring and resource allocation across distributed industrial estates (Akin-Oluyomi & Akhigbe, 2023a). Multi-site performance architectures further show the value of common indicators, integrated dashboards, and data-driven comparison for coordinating geographically dispersed operations while retaining site-level accountability (Akin-Oluyomi & Akhigbe, 2023b).

Resilient retrofits must nevertheless be treated as socio-technical systems. Moroccan research modelling cyber resilience in manufacturing emphasizes interactions among technology, organizational preparedness, recovery capacity, learning, and interconnected operational factors, demonstrating that resilience emerges from reinforcing capabilities rather than single defensive measures (Said, Bouloiz & Gallab, 2023). Accordingly, future retrofit architectures should combine adaptive analytics, digital twins, automated policy enforcement, resilient control, distributed monitoring, and standardized performance metrics. Such designs can allow security controls to evolve incrementally with threat conditions and plant modernization, supporting repeatable deployment across sites without imposing disruptive greenfield replacement on functioning legacy assets. This enables progressive modernization while preserving safety, continuity, interoperability, and lifecycle sustainability across operations.

Conclusion

This review examined the challenge of strengthening cybersecurity in legacy process plants where operational continuity, safety, aging assets, and inherited architectures constrain conventional modernization. The study met its objectives by first clarifying the distinctive exposure of brownfield operational technology, including obsolete platforms, insecure industrial protocols, expanding connectivity, remote access, and the growing convergence of cyber and physical risk. It then demonstrated that effective protection cannot depend on wholesale replacement, but must instead prioritize carefully sequenced, risk-based interventions compatible with existing plant conditions.

The analysis showed that retrofit-first cybersecurity is most effective when built on accurate asset discovery, criticality assessment, network zoning, segmentation, controlled access, compensating safeguards, continuous monitoring, anomaly detection, and disciplined incident response. Equally important, patch governance must account for maintenance windows, vendor support, test requirements, operational risk, and the possibility that some vulnerabilities cannot be remediated immediately. Standards alignment, particularly through risk-oriented industrial cybersecurity frameworks, further strengthens assurance when technical controls are supported

by governance, measurable maturity, workforce capability, vendor accountability, and structured change management.

A central finding is that brownfield cybersecurity is fundamentally a resilience problem. The most sustainable approach is one that preserves essential operations while progressively reducing exposure, improving visibility, and increasing recovery capacity. However, important evidence gaps remain, especially regarding long-term field validation, representative datasets, retrofit economics, control effectiveness across heterogeneous plants, and the scalability of adaptive security mechanisms.

Accordingly, plant operators should adopt phased retrofit programs linked to asset criticality, safety consequence, and operational feasibility; establish cross-functional governance between engineering, cybersecurity, maintenance, and management; strengthen vendor and workforce controls; and validate interventions through measurable performance indicators. Future research should prioritize multi-site empirical studies, realistic test environments, lifecycle cost analysis, adaptive monitoring, digital-twin-assisted validation, and resilience metrics capable of demonstrating whether retrofit investments measurably improve security without undermining process safety, availability, maintainability, or production continuity across extended operating lifecycles.

References

1. Abdulganiyu, O.H., Ait Tchakoucht, T. and Saheed, Y.K. (2023) ‘A systematic literature review for network intrusion detection system (IDS)’, International Journal of Information Security, 22(5), pp. 1125–1162. DOI: 10.1007/s10207-023-00682-2.
2. 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’, Iconic Research and Engineering Journals, 3(11), pp. 547–565. DOI: 10.64388/IREV3I11-1714040.
3. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2023) ‘A review of industrial equipment restoration strategies: Integrating design of experiments (DOE) and root-cause analysis’, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), pp. 444–462.
4. 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.
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: 10.54660/.IJMRGE.2022.3.6.860-878.

6. Akin-Oluyomi, O.T. and Akhigbe, R. (2023) 'A conceptual supply chain leadership model for aligning logistics decisions with enterprise strategy', International Journal of Advanced Multidisciplinary Research and Studies, 3(1), pp. 1725–1744. DOI: 10.62225/2583049X.2023.3.1.5340.
7. 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: 10.62225/2583049X.2023.3.1.5338.
8. 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: 10.62225/2583049X.2023.3.1.5343.
9. Alanazi, M., Mahmood, A. and Chowdhury, M.J.M. (2023) 'SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues', Computers & Security, 125, 103028. DOI: 10.1016/j.cose.2022.103028.
10. Alqoud, A., Schaefer, D. and Milisavljevic-Syed, J. (2022) 'Industry 4.0: A systematic review of legacy manufacturing system digital retrofitting', Manufacturing Review, 9, 32. DOI: 10.1051/mfreview/2022031.
11. Alrowaili, Y., Saxena, N. and Srivastava, A. (2023) 'A review: Monitoring situational awareness of smart grid cyber-physical systems and critical asset identification', IET Cyber-Physical Systems: Theory & Applications, 8(3), pp. 160–185. DOI: 10.1049/cps2.12059.
12. Alrumaih, T.N.I., Alenazi, M.J.F., AlSowaygh, N.A., Humayed, A.A. and Alablani, I.A. (2023) 'Cyber resilience in industrial networks: A state of the art, challenges, and future directions', Journal of King Saud University - Computer and Information Sciences, 35(9), 101781. DOI: 10.1016/j.jksuci.2023.101781.
13. Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: A practice perspective', Computers & Security, 98, 102003. DOI: 10.1016/j.cose.2020.102003.
14. Amoah, R., Camtepe, S. and Foo, E. (2016) 'Securing DNP3 broadcast communications in SCADA systems', IEEE Transactions on Industrial Informatics, 12(4), pp. 1474–1485. DOI: 10.1109/TII.2016.2587883.
15. Ani, U.D., Daniel, N., Oladipo, F. and Adewumi, S.E. (2018) 'Securing industrial control system environments: The missing piece', Journal of Cyber Security Technology, 2(3–4), pp. 131–163. DOI: 10.1080/23742917.2018.1554985.

16. Arief, R., Khakzad, N. and Pieters, W. (2020) 'Mitigating cyberattack-related domino effects in process plants via ICS segmentation', Journal of Information Security and Applications, 51, 102450. DOI: 10.1016/j.jisa.2020.102450.
17. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K. and Meskin, N. (2020) 'Cybersecurity for industrial control systems: A survey', Computers & Security, 89, 101677. DOI: 10.1016/j.cose.2019.101677.
18. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. and Fallon, M. (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-161r1.
19. Canonico, R. and Sperlì, G. (2023) 'Industrial cyber-physical systems protection: A methodological review', Computers & Security, 135, 103531. DOI: 10.1016/j.cose.2023.103531.
20. Cheminod, M., Durante, L. and Valenzano, A. (2013) 'Review of security issues in industrial networks', IEEE Transactions on Industrial Informatics, 9(1), pp. 277–293. DOI: 10.1109/TII.2012.2198666.
21. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems', Computers & Security, 56, pp. 1–27. DOI: 10.1016/j.cose.2015.09.009.
22. Chileshe, G. and van Heerden, R. (2012) 'SCADA systems in South Africa and their vulnerabilities', in Proceedings of the 7th International Conference on Information Warfare and Security, Seattle, USA, pp. 90–97. DOI: 10.13140/2.1.3988.3529.
23. Conti, M., Donadel, D. and Turrin, F. (2021) 'A survey on industrial control system testbeds and datasets for security research', IEEE Communications Surveys & Tutorials, 23(4), pp. 2248–2294. DOI: 10.1109/COMST.2021.3094360.
24. Cusimano, J. (2022) 'Industrial control system risk assessment standards and leading practices in the chemical industry', Process Safety Progress, 41(4), pp. 665–669. DOI: 10.1002/prs.12372.
25. Da Veiga, A. and Eloff, J.H.P. (2010) 'A framework and assessment instrument for information security culture', Computers & Security, 29(2), pp. 196–207. DOI: 10.1016/j.cose.2009.09.002.
26. Dehlaghi-Ghadim, A., Balador, A., Helali Moghadam, M., Hansson, H. and Conti, M. (2023) 'ICSSIM—A framework for building industrial control systems security testbeds', Computers in Industry, 148, 103906. DOI: 10.1016/j.compind.2023.103906.
27. Diaba, S.Y., Anafo, T., Tetteh, L.A., Oyibo, M.A., Alola, A.A., Shafie-khah, M. and Elmusrati, M. (2023) 'SCADA securing system using deep learning to prevent cyber infiltration', Neural Networks, 165, pp. 321–332. DOI: 10.1016/j.neunet.2023.05.047.
28. Dietz, M. and Pernul, G. (2020) 'Unleashing the digital twin's potential for ICS security', IEEE Security & Privacy, 18(4), pp. 20–27. DOI: 10.1109/MSEC.2019.2961650.

29. Dietz, M., Englbrecht, L. and Pernul, G. (2021) 'Enhancing industrial control system forensics using replication-based digital twins', in Advances in Digital Forensics XVII, IFIP Advances in Information and Communication Technology, pp. 21–38. DOI: 10.1007/978-3-030-88381-2_2.
30. Djebbar, F. and Nordström, K. (2023) 'A comparative analysis of industrial cybersecurity standards', IEEE Access, 11, pp. 85315–85332. DOI: 10.1109/ACCESS.2023.3303205.
31. Elhoseny, M. and Abbas, H. (2020) 'Towards automated SCADA forensic investigation: Challenges, opportunities and promising paradigms', International Journal of Information and Computer Security, 13(3/4), pp. 268–288. DOI: 10.1504/IJICS.2020.109477.
32. 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.
33. Faleiro, R., Pan, L., Pokhrel, S.R. and Doss, R. (2022) 'Digital twin for cybersecurity: Towards enhancing cyber resilience', in Broadband Communications, Networks, and Systems, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 57–76. DOI: 10.1007/978-3-030-93479-8_4.
34. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp. 439–456. DOI: 10.54660/.IJMRGE.2020.1.5.439-456.
35. 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: 10.62225/2583049X.2023.3.1.5339.
36. Galloway, B. and Hancke, G.P. (2013) 'Introduction to industrial control networks', IEEE Communications Surveys & Tutorials, 15(2), pp. 860–880. DOI: 10.1109/SURV.2012.071812.00124.
37. Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W. and Chen, C.L.P. (2014) 'SCADA communication and security issues', Security and Communication Networks, 7(1), pp. 175–194. DOI: 10.1002/sec.698.
38. Gazzan, M. and Sheldon, F.T. (2023) 'Opportunities for early detection and prediction of ransomware attacks against industrial control systems', Future Internet, 15(4), 144. DOI: 10.3390/fi15040144.
39. Gentile, U. and Serio, L. (2019) 'Survey on international standards and best practices for patch management of complex industrial control systems: The critical infrastructure of particle accelerators case study', International Journal of Critical Computer-Based Systems, 9(1/2), pp. 115–132. DOI: 10.1504/IJCCBS.2019.098812.Goldenberg, N. and Wool, A. (2013) 'Accurate modeling of Modbus/TCP for intrusion detection in SCADA

systems', International Journal of Critical Infrastructure Protection, 6(2), pp. 63–75. DOI: 10.1016/j.ijcip.2013.05.001.

40. Huitsing, P., Chandia, R., Papa, M. and Shenoi, S. (2008) 'Attack taxonomies for the Modbus protocols', International Journal of Critical Infrastructure Protection, 1, pp. 37–44. DOI: 10.1016/j.ijcip.2008.08.003.
41. Humayed, A., Lin, J., Li, F. and Luo, B. (2017) 'Cyber-physical systems security—A survey', IEEE Internet of Things Journal, 4(6), pp. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.
42. Huong, T.T., Bac, T.P., Ha, K.N., Hoang, N.V., Hoang, N.X., Hung, N.T. and Tran, K.P. (2022) 'Federated learning-based explainable anomaly detection for industrial control systems', IEEE Access, 10, pp. 53854–53872. DOI: 10.1109/ACCESS.2022.3173288.
43. Iaiani, M., Tugnoli, A. and Cozzani, V. (2023) 'Identification of cyber-risks for the control and safety instrumented systems: A synergic framework for the process industry', Process Safety and Environmental Protection, 172, pp. 69–82. DOI: 10.1016/j.psep.2023.01.078.
44. James, U.U., Idika, C.N. and Enyejo, L.A. (2023) 'Zero Trust Architecture leveraging AI-driven behavior analytics for Industrial Control Systems in energy distribution networks', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(4), pp. 685–709. DOI: 10.32628/CSEIT23564522.
45. Kayan, H., Nunes, M., Rana, O., Burnap, P. and Perera, C. (2022) 'Cybersecurity of industrial cyber-physical systems: A review', ACM Computing Surveys, 54(11s), pp. 1–35. DOI: 10.1145/3510410.
46. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) 'A survey of cyber security management in industrial control systems', International Journal of Critical Infrastructure Protection, 9, pp. 52–80. DOI: 10.1016/j.ijcip.2015.02.002.
47. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. and Halgand, Y. (2015) 'A survey of approaches combining safety and security for industrial control systems', Reliability Engineering & System Safety, 139, pp. 156–178. DOI: 10.1016/j.ress.2015.02.008.
48. Kure, H.I. and Islam, S. (2019) 'Assets focus risk management framework for critical infrastructure cybersecurity risk management', IET Cyber-Physical Systems: Theory & Applications, 4(4), pp. 332–340. DOI: 10.1049/iet-cps.2018.5079.
49. Langner, R. (2011) 'Stuxnet: Dissecting a cyberwarfare weapon', IEEE Security & Privacy, 9(3), pp. 49–51. DOI: 10.1109/MSP.2011.67.
50. Malatji, M., Marnewick, A.L. and von Solms, S. (2020) 'Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa', Sustainability, 13(1), 291. DOI: 10.3390/su13010291.
51. 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.

52. Mbanaso, U.M., Abrahams, L. and Apene, O.Z. (2019) 'Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework', The African Journal of Information and Communication, 23, pp. 1–26. DOI: 10.23962/10539/27535.
53. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M. and Karri, R. (2016) 'The cybersecurity landscape in industrial control systems', Proceedings of the IEEE, 104(5), pp. 1039–1057. DOI: 10.1109/JPROC.2015.2512235.
54. Mesbah, M., Elsayed, M.S., Jurcut, A.D. and Azer, M. (2023) 'Analysis of ICS and SCADA systems attacks using honeypots', Future Internet, 15(7), 241. DOI: 10.3390/fi15070241.
55. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.04162018.
56. Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012) 'SCADA security in the light of cyber-warfare', Computers & Security, 31(4), pp. 418–436. DOI: 10.1016/j.cose.2012.02.009.
57. 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.
58. 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.
59. Osman, F.A., Hashem, M.Y.M. and Eltokhy, M.A.R. (2022) 'Secured cloud SCADA system implementation for industrial applications', Multimedia Tools and Applications, 81(7), pp. 9989–10005. DOI: 10.1007/s11042-022-12130-9.
60. Pool, J.H. and Venter, H. (2022) 'A harmonized information security taxonomy for cyber physical systems', Applied Sciences, 12(16), 8080. DOI: 10.3390/app12168080.
61. Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R. and Misurec, J. (2021) 'Application perspective on cybersecurity testbed for industrial control systems', Sensors, 21(23), 8119. DOI: 10.3390/s21238119.
62. Powell, M., Hoyt, J., Sherule, A. and Wilcox, L. (2023) Security Segmentation in a Small Manufacturing Environment. NIST Cybersecurity White Paper. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.CSWP.28.
63. Pretorius, B. and van Niekerk, B. (2015) 'Cyber-security and governance for ICS/SCADA in South Africa', in Zaaiman, J. and Leenen, L. (eds.) Proceedings of the 10th International Conference on Cyber Warfare and Security. Reading: Academic Conferences and Publishing International Limited, pp. 241–251.

64. Pretorius, B. and van Niekerk, B. (2016) 'Cyber-security for ICS/SCADA: A South African perspective', International Journal of Cyber Warfare and Terrorism, 6(3), pp. 1–16. DOI: 10.4018/IJCWT.2016070101.
65. Qassim, Q.S., Jamil, N., Daud, M., Patel, A. and Ja'affar, N. (2019) 'A review of security assessment methodologies in industrial control systems', Information and Computer Security, 27(1), pp. 47–61. DOI: 10.1108/ICS-04-2018-0048.
66. Quinn, S., Barrett, M., Witte, G., Gardner, R. and Ivy, N. (2022) Prioritizing Cybersecurity Risk for Enterprise Risk Management. NIST Interagency/Internal Report 8286B. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.8286B.
67. Ralston, P.A.S., Graham, J.H. and Hieb, J.L. (2007) 'Cyber security risk assessment for SCADA and DCS networks', ISA Transactions, 46(4), pp. 583–594. DOI: 10.1016/j.isatra.2007.04.003.
68. Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-207.
69. Rubio, J.E., Alcaraz, C., Roman, R. and Lopez, J. (2019) 'Current cyber-defense trends in industrial control systems', Computers & Security, 87, 101561. DOI: 10.1016/j.cose.2019.06.015.
70. Said, S., Bouloiz, H. and Gallab, M. (2023) 'Modeling a cyber-resilience-for-manufacturing ecosystem through causal loop diagram', in Proceedings of the 33rd European Safety and Reliability Conference, pp. 3160–3164. DOI: 10.3850/978-981-18-8071-1_P626-cd.
71. Serror, M., Hack, S., Henze, M., Schuba, M. and Wehrle, K. (2021) 'Challenges and opportunities in securing the Industrial Internet of Things', IEEE Transactions on Industrial Informatics, 17(5), pp. 2985–2996. DOI: 10.1109/TII.2020.3023507.
72. 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. DOI: 10.1109/CCWC57344.2023.10099268.
73. Shittu, H.A., Shittu, M.A., 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: 10.34218/IJREEE_04_03_001.
74. Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', Iconic Research and Engineering Journals, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.
75. 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: 10.34218/IJIERD_14_02_003.

76. Shohoud, M. (2023) 'Study the effectiveness of ISO 27001 to mitigate the cyber security threats in the Egyptian downstream oil and gas industry', Journal of Information Security, 14, pp. 152–180. DOI: 10.4236/jis.2023.142010.
77. Skarga-Bandurova, I., Kotsiuba, I. and Velasco, E.R. (2021) 'Cyber hygiene maturity assessment framework for smart grid scenarios', Frontiers in Computer Science, 3, 614337. DOI: 10.3389/fcomp.2021.614337.
78. Souppaya, M. and Scarfone, K. (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. NIST Special Publication 800-40 Revision 4. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-40r4.
79. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015) Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-82r2.
80. 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.
81. 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, 7(4), pp. 380–403.
82. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2019) 'Thermodynamic efficiency and control strategies in residential air conditioning systems', International Journal of Scientific Research in Civil Engineering, 3(3), pp. 52–76. DOI: 10.32628/IJSRCE19339.
83. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) 'Transitioning from reactive to predictive maintenance in mechanical systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), pp. 425–447.
84. Tantscher, D. and Mayer, B. (2022) 'Digital retrofitting of legacy machines: A holistic procedure model for industrial companies', CIRP Journal of Manufacturing Science and Technology, 36, pp. 35–44. DOI: 10.1016/j.cirpj.2021.10.011.
85. Thomas, A.M., Marali, M. and Reddy, L. (2022) 'Identification of assets in industrial control systems using passive scanning', in Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies, pp. 269–283. DOI: 10.1007/978-981-19-0898-9_21.
86. Tu, Y., Wang, J., Yang, G. and Liu, B. (2021) 'An efficient attribute-based access control system with break-glass capability for cloud-assisted industrial control system',

Mathematical Biosciences and Engineering, 18(4), pp. 3559–3577. DOI: 10.3934/mbe.2021179.

87. Upadhyay, D. and Sampalli, S. (2020) 'SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations', Computers & Security, 89, 101666. DOI: 10.1016/j.cose.2019.101666.
88. Vávra, J., Hromada, M., Lukáš, L. and Dworzecki, J. (2021) 'Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment', International Journal of Critical Infrastructure Protection, 34, 100446. DOI: 10.1016/j.ijcip.2021.100446.
89. Wedgbury, A. and Jones, K. (2015) 'Automated asset discovery in industrial control systems: Exploring the problem', in Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015, pp. 73–83. DOI: 10.14236/ewic/ICS2015.8.
90. Yadav, G. and Paul, K. (2021) 'Architecture and security of SCADA systems: A review', International Journal of Critical Infrastructure Protection, 34, 100433. DOI: 10.1016/j.ijcip.2021.100433.
91. Yadav, G., Gauravaram, P., Jindal, A.K. and Paul, K. (2022) 'SmartPatch: A patch prioritization framework', Computers in Industry, 137, 103595. DOI: 10.1016/j.compind.2021.103595.
92. Yalcinkaya, E., Maffei, A. and Onori, M. (2017) 'Application of attribute-based access control model for industrial control systems', International Journal of Computer Network and Information Security, 9(2), pp. 12–21. DOI: 10.5815/ijcnis.2017.02.02.
93. Zhu, B., Joseph, A.D. and Sastry, S. (2011) 'A taxonomy of cyber attacks on SCADA systems', in 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, pp. 380–388. DOI: 10.1109/iThings/CPSCom.2011.34.