Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i03.027

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Cybersecure Industrial IoT Architectures for Saudi Arabia's Digital Manufacturing Ecosystem

Muhammad Kamran Asad[1]*
[1]Independent Researcher

***Corresponding Author**
Muhammad Kamran Asad
Independent Researcher

Article History
Received: 28.04.2026
Accepted: 20.06.2026
Published: 25.06.2026

Abstract: Industrial Internet of Things (IIoT) architectures are becoming central to Saudi Arabia's digital manufacturing agenda because connected sensors, programmable logic controllers, robotics, manufacturing execution systems, digital twins and cloud analytics can raise productivity, quality and energy efficiency. The same connectivity, however, expands the cyber-physical attack surface of factories that were historically protected by isolation and proprietary protocols. This review develops a cybersecure IIoT architecture model for Saudi Arabia's digital manufacturing ecosystem under Vision 2030. It synthesizes recent literature and standards published between 2020 and 2025, with emphasis on predictive cybersecurity, zero-trust principles, operational technology segmentation, machine-learning-enabled anomaly detection, governance and incident response. A narrative review methodology is used to classify threats, architectural controls, implementation barriers and research gaps. The analysis shows that resilient digital factories require more than perimeter firewalls; they require asset visibility, identity-based access, secure conduits between IT and OT, edge-level monitoring, explainable detection models, supplier assurance and safety-aware recovery playbooks. The paper proposes a layered architecture and risk-scoring cycle that can be adapted by Saudi manufacturers, industrial cities and giga-project supply chains. It concludes that Saudi digital manufacturing can achieve high-trust automation when cybersecurity is designed as an operational capability, not added after deployment.

Keywords: Industrial Internet of Things, Cybersecurity, Industry 4.0, Saudi Arabia, Digital Manufacturing, Zero Trust, Predictive Analytics.

1. INTRODUCTION

Saudi Arabia's manufacturing base is being reshaped by national industrial diversification, smart infrastructure investment and the wider digital transformation agenda of Vision 2030. In this context, digital manufacturing is not simply the automation of existing production lines; it is the creation of connected production ecosystems in which sensors, controllers, machines, operators, enterprise systems and external suppliers exchange data continuously. Industrial Internet of Things devices make this integration possible by linking operational technology (OT) to analytics platforms, cloud services and decision dashboards. The expected benefits include predictive maintenance, shorter production cycles, safer shop-floor operations, traceable supply chains and evidence-based resource optimization. These outcomes are highly relevant to Saudi industrial cities, energy-intensive manufacturing clusters, food and pharmaceutical production,

mining, logistics and emerging advanced-manufacturing initiatives.

The strategic opportunity also creates a security problem. Traditional factory networks were often designed around availability and deterministic control, not exposure to large-scale digital connectivity. Once IIoT gateways, remote maintenance links, cloud historians and mobile engineering workstations are introduced, a compromise can move from a user identity or supplier account to a production asset. The cyber risk is therefore cyber-physical: malicious commands can interrupt a line, alter set points, distort quality data, damage equipment or create safety hazards. Recent cybersecurity reviews emphasize that Industry 4.0 attack surfaces are expanding because cloud computing, artificial intelligence, big data and connected devices are being embedded into production systems (Alqudhaibi *et al*., 2025). The reference paper used for this review also highlights the need to combine predictive analytics, proactive threat management and cybersecurity frameworks for manufacturing systems.

A cybersecure IIoT architecture must reconcile two requirements that are sometimes treated as opposites. The first is openness: data must flow across machines, lines, plants and enterprise systems so that digital manufacturing can deliver business value. The second is restriction: every connection must be governed, monitored and limited so that compromise of one element does not become compromise of the entire production environment. Zero-trust architecture is useful because it shifts security from broad network assumptions to continuous verification of users, devices, applications and transactions (Rose *et al*., 2020). Yet zero trust cannot be copied from office IT into OT without adaptation. Industrial devices may have long lifecycles, limited computing resources and strict timing constraints. Security controls must therefore be engineered around production safety, maintenance windows, system interoperability and the human realities of factory operations.

This paper addresses the question: what architecture can support cybersecure IIoT adoption in Saudi Arabia's digital manufacturing ecosystem? The aim is to design a review-based framework that connects academic findings with practical implementation. The objectives are to identify the main IIoT threat vectors affecting digital factories, classify architecture controls suitable for Saudi industrial settings, evaluate the role of predictive and machine-learning methods, align the architecture with governance and Vision 2030 priorities, and define research gaps for future Saudi manufacturing cybersecurity studies. The paper is structured in the style of a Scopus-indexed review article, moving from methodology to literature synthesis, proposed architecture, discussion, future research and conclusion.

2. REVIEW METHODOLOGY

A narrative review methodology was selected because cybersecure IIoT architecture is an interdisciplinary topic crossing cybersecurity, manufacturing engineering, industrial control systems, data governance and national digital transformation. Narrative reviews are suitable when the purpose is to synthesize concepts, classify patterns and build an integrative framework rather than calculate a statistical effect size. The methodological logic follows the uploaded Springer-style model, which organizes a review around scope definition, literature selection, synthesis of predictive methods and identification of research gaps in manufacturing cybersecurity (Alqudhaibi *et al*., 2025). This study adapts that logic to the Saudi digital manufacturing context and focuses on publications and standards from 2020 to 2025.

The review scope covered four literature streams. The first stream examined IIoT and smart manufacturing security, including cyber-physical vulnerabilities, edge security, anomaly detection and secure industrial communications. The second stream examined predictive cybersecurity models, including machine learning, deep learning, threat intelligence, attack graphs and risk scoring. The third stream covered governance and standards, especially zero trust, cybersecurity risk management and OT security controls. The fourth stream addressed Saudi Arabia's digital transformation and industrial ecosystem, including the need to support Vision 2030 objectives through secure manufacturing modernization. Searches were conceptually framed around terms such as industrial internet of things, smart manufacturing cybersecurity, predictive cybersecurity, OT segmentation, digital manufacturing, zero trust, Saudi Arabia and Vision 2030.

The inclusion criteria prioritized peer-reviewed or authoritative sources published between 2020 and 2025, relevance to manufacturing or cyber-physical systems, discussion of architecture or implementation, and usefulness for building a practical framework. Sources were excluded when they addressed only general enterprise IT without industrial relevance, when they focused on purely theoretical cryptography without deployable architecture implications, or when they were older than the requested period unless required for contextual standards. Evidence was synthesized thematically rather than bibliometrically. Each source was assessed for its contribution to the

architecture: asset visibility, identity control, network segmentation, secure data exchange, monitoring, predictive analytics, incident response, governance or workforce readiness.

The review has three limitations. First, because Saudi manufacturing cybersecurity is an emerging topic, many lessons are inferred from broader Industry 4.0, energy, food, supply-chain and critical-infrastructure studies. Second, the paper does not test a live factory network or evaluate a proprietary dataset, so the architecture should be interpreted as a conceptual and implementation framework. Third, cybersecurity evolves quickly; therefore, the proposed model requires periodic updating as new threats, regulatory expectations and industrial technologies emerge. These limitations do not weaken the review's value; rather, they clarify that the contribution is a structured synthesis for researchers, industrial managers and cybersecurity practitioners who need a deployable starting point.

3. Threat Landscape in IIoT-Enabled Manufacturing

The IIoT threat landscape differs from conventional IT because the targeted environment is a production system. Attackers are not only seeking data; they may seek downtime, process manipulation, intellectual-property theft, reputational damage or leverage over critical supply chains. Typical IIoT components include sensors, actuators, programmable logic controllers, supervisory control and data acquisition systems, human-machine interfaces, robotic cells, industrial gateways, historians, manufacturing execution systems and cloud analytics platforms. Each layer introduces different vulnerabilities. Field devices may use insecure legacy protocols, engineering workstations may be patched slowly, remote vendors may hold privileged credentials, and cloud dashboards may expose sensitive production data if identity and configuration controls are weak.

Ransomware remains a major concern because production downtime converts cyber compromise into immediate operational loss. Manufacturing firms are attractive targets because continuous production, tight delivery commitments and safety requirements can pressure organizations to restore operations quickly. Malware and ransomware can enter through phishing, exposed remote desktop services, unsegmented corporate networks, compromised suppliers or infected maintenance media. Once inside, attackers may encrypt IT systems, disrupt scheduling applications, move laterally into OT support networks or disable monitoring tools. The literature on food security and industrial control systems, for example, shows that ransomware against production environments creates both business-continuity and public-supply risks (Alkahtani & Theyazn, 2022; Manning & Kowalska, 2023).

Data integrity attacks are equally important. A smart factory relies on trusted data for predictive maintenance, quality assurance, energy optimization and automated decision-making. If sensor readings, digital twin inputs or manufacturing execution records are manipulated, the system may continue operating while producing defective output or unsafe decisions. This risk is often harder to detect than a visible outage. Predictive models trained on compromised data may learn the wrong baseline, and dashboards may give managers a false sense of control. Cybersecure architecture must therefore protect confidentiality, integrity and availability, but in manufacturing the ordering often shifts: availability and safety are vital, while data integrity determines whether automation remains trustworthy.

Supply-chain exposure intensifies the risk. Saudi digital manufacturing ecosystems include equipment vendors, system integrators, cloud providers, logistics partners, industrial-city operators and contractors. A weak supplier may become the entry point into a larger production environment. Cyber supply-chain research stresses that organizations need predictive analytics and external intelligence to understand threats before they reach internal systems (Yeboah-Ofori *et al*., 2021). For IIoT architecture, this means supplier assurance cannot remain a procurement formality. It must be embedded into device onboarding, remote access approvals, firmware management, software bills of materials, vulnerability disclosure processes and incident reporting obligations.

Insider and human-factor risks also remain significant. Factory engineers, operators and maintenance teams often prioritize uptime and immediate problem solving. Shared accounts, temporary firewall openings, unmanaged laptops and informal vendor access can become normalized practices. The uploaded reference review identifies people, process and technology as interdependent factors in manufacturing cybersecurity, noting that awareness, leadership support and IT-OT collaboration are essential for preventing breaches (Alqudhaibi *et al*., 2025). In Saudi plants with multilingual workforces and contractor-heavy operations, security procedures must be simple, role-specific and aligned with production routines. Otherwise, controls will be bypassed during maintenance, commissioning or urgent troubleshooting.

4. Architectural Principles for Cybersecure Saudi IIoT

A cybersecure IIoT architecture for Saudi manufacturing should be layered, identity-driven, risk-informed and operationally realistic. The first principle is comprehensive asset visibility. A factory cannot protect what it cannot identify. Asset inventory should include PLCs, sensors, gateways, servers, engineering stations, virtual machines, cloud integrations, wireless devices, firmware versions, protocols and ownership. Discovery must be passive where active scanning could disrupt production. Each asset should be mapped to its function, criticality, data flows, maintenance owner and permitted communication paths. This inventory becomes the foundation for segmentation, vulnerability management, incident response and investment prioritization.

The second principle is zone-and-conduit segmentation. Industrial networks should be divided into logical zones based on production function, safety impact and trust level. Conduits between zones should be explicitly authorized, monitored and restricted. For example, a robotic cell should not communicate freely with office devices, and a vendor remote-access session should not automatically reach all controllers. Segmentation supports both prevention and recovery because it limits lateral movement and enables a compromised zone to be isolated without shutting down the entire plant. In practice, segmentation should combine industrial firewalls, secure gateways, unidirectional patterns where appropriate, software-defined controls and strict change management.

The third principle is zero-trust access adapted for OT. Zero trust assumes that no user, device or network segment is automatically trusted. Each request is evaluated using identity, device posture, role, location, behavior, asset sensitivity and policy. For IIoT, this principle should be applied through multi-factor authentication, privileged access management, session recording for engineers and vendors, time-bound access approvals, device certificates and continuous monitoring of unusual commands. NIST describes zero trust as an architecture that protects resources through continuous evaluation rather than reliance on a trusted internal perimeter (Rose *et al*., 2020). In OT, the goal is not to interrupt deterministic control loops, but to ensure that human and system access to those loops is verified, limited and auditable.

The fourth principle is secure edge computing. IIoT gateways often translate industrial protocols, preprocess telemetry and connect equipment to cloud platforms. Because these gateways sit between production assets and external analytics, they are high-value security points. They should enforce authentication, encryption, protocol filtering, secure boot, signed updates, local logging and fail-safe behavior. Edge monitoring is also useful because it can detect abnormal traffic near the source without sending all raw industrial data to the cloud. Research on IIoT edge cybersecurity emphasizes the importance of local detection, resilient communication and lightweight controls for cyber-physical systems (Zhukabayeva *et al*., 2025).

The fifth principle is predictive and explainable monitoring. Signature-based detection alone is insufficient for industrial environments where new attack paths, novel devices and plant-specific behavior are common. Machine-learning methods can support anomaly detection, attack prediction, vulnerability prioritization and incident triage. However, models must be explainable enough for engineers to trust them. A black-box alarm that cannot explain whether a pressure sensor, PLC command, user session or network pattern created the alert may be ignored. Therefore, predictive models should combine process knowledge, threat intelligence, operational baselines and explainable outputs. They should also be tested for false positives, detection latency and model drift, not only for offline accuracy.

The sixth principle is governance-by-design. Architecture decisions must align with cybersecurity policy, risk appetite, regulatory obligations and business objectives. NIST Cybersecurity Framework 2.0 emphasizes governance as a core function for managing cybersecurity risk across organizations (NIST, 2024). For Saudi manufacturers, governance should also reflect national cybersecurity expectations, supplier accountability, executive reporting and the strategic importance of resilient industrial transformation. Security architecture should be reviewed at project gates: before procurement, before commissioning, before connecting to cloud services, before allowing vendor remote access and after major process changes. This transforms cybersecurity from a late-stage audit into a lifecycle requirement.

5. Proposed Architecture and Operational Model

The proposed architecture is organized into six layers: physical production assets, edge security fabric, industrial data zone, enterprise integration, cloud analytics and governance overlay. The physical layer contains sensors, PLCs, robots, drives, safety systems and machines. The edge security layer contains industrial gateways, local intrusion detection sensors, protocol brokers and secure remote-access appliances. The industrial data zone contains historians, manufacturing execution systems, quality databases and digital twin services.

The enterprise layer connects planning, procurement, maintenance, finance and reporting. The cloud layer supports scalable analytics, artificial intelligence and cross-site benchmarking. The governance overlay defines identity rules, segmentation policy, supplier assurance, incident response, audit logging and executive risk reporting.

Data movement in this architecture is intentionally controlled. Production telemetry should travel from assets to the edge layer, then to the industrial data zone, and only then to enterprise or cloud analytics through approved conduits. Commands should be more restricted than telemetry. Cloud platforms may receive data for analysis, but direct cloud-to-controller command paths should be avoided unless justified by a formal risk assessment, safety analysis and compensating controls. Vendor access should terminate in a controlled access zone with session monitoring and approval workflows. Portable media and engineering laptops should pass through scanning and validation processes before touching production equipment.

The operational model uses a continuous risk-scoring cycle. Each asset receives a criticality score based on safety impact, production dependency, quality impact and recovery complexity. Exposure is scored using connectivity, remote access, protocol security, patch status and supplier dependency. Threat likelihood is adjusted using intelligence about active campaigns, known vulnerabilities and sector-specific incidents. Detection confidence is based on telemetry coverage, baseline maturity, alert quality and staff readiness. Residual risk is then used to prioritize segmentation, compensating controls, patch windows, monitoring improvements and recovery exercises. This approach avoids treating all assets equally; a safety-linked controller in a bottleneck process receives more attention than a noncritical sensor with no external connectivity.

Incident response must be engineered for safe production recovery. Standard IT playbooks often focus on containment, eradication and restoration, but factory response also requires process safety, product quality verification, equipment calibration and coordination with operations leaders. For this reason, playbooks should define safe-state logic, manual fallback procedures, isolation points, communication responsibilities, evidence collection and criteria for restarting equipment. Exercises should include plant managers, OT engineers, IT security teams, health and safety personnel, legal staff and key vendors. A response plan that has not been rehearsed with operations teams is unlikely to work under production pressure.

The architecture also requires workforce integration. Cybersecurity roles should be translated into operational responsibilities. Operators should know how to report unusual HMI behavior, engineers should understand privileged-access rules, procurement teams should request security evidence from vendors, and executives should receive risk metrics that connect cybersecurity to downtime, safety, compliance and investment. Training should avoid generic awareness slides and focus instead on realistic factory scenarios: unauthorized remote sessions, suspicious firmware updates, abnormal robot behavior, phishing targeting maintenance teams, and emergency network changes. This helps build a security culture without slowing production unnecessarily.

6. Tables and Graphical Representations

Table 1 summarizes major threat categories, affected IIoT layers and recommended architecture controls. Table 2 converts the proposed architecture into implementation actions suitable for Saudi manufacturing entities. Figure 1 presents the layered reference architecture, while Figure 2 presents the operational risk-scoring cycle. Together, the tables and figures show that cybersecure IIoT is not a single product; it is a coordinated system of technology, governance, workforce practice and continuous improvement.

Table 1: IIoT threat categories and architecture controls

Threat category	Affected IIoT layer	Likely impact	Architecture response
Ransomware and malware	Enterprise, industrial data zone, engineering workstations	Downtime, encrypted systems, delayed orders	Immutable backups, segmentation, EDR where safe, rehearsed recovery
Insecure remote access	Vendor access, gateways, engineering laptops	Unauthorized commands, credential theft, lateral movement	MFA, PAM, jump hosts, session recording, time-bound approvals
Protocol abuse and lateral movement	OT networks, PLCs, HMI, gateways	Process manipulation and hidden persistence	Industrial firewalls, allow-listed conduits, passive IDS, zone isolation
Data integrity manipulation	Sensors, historians, MES, digital twins	Wrong analytics, defective output, unsafe decisions	Signed data flows, anomaly detection, validation rules, audit trails

Threat category	Affected IIoT layer	Likely impact	Architecture response
Supplier compromise	Firmware, software updates, contractors, cloud services	Backdoor entry and ecosystem spread	Supplier assurance, SBOMs, vulnerability disclosure, contract security clauses

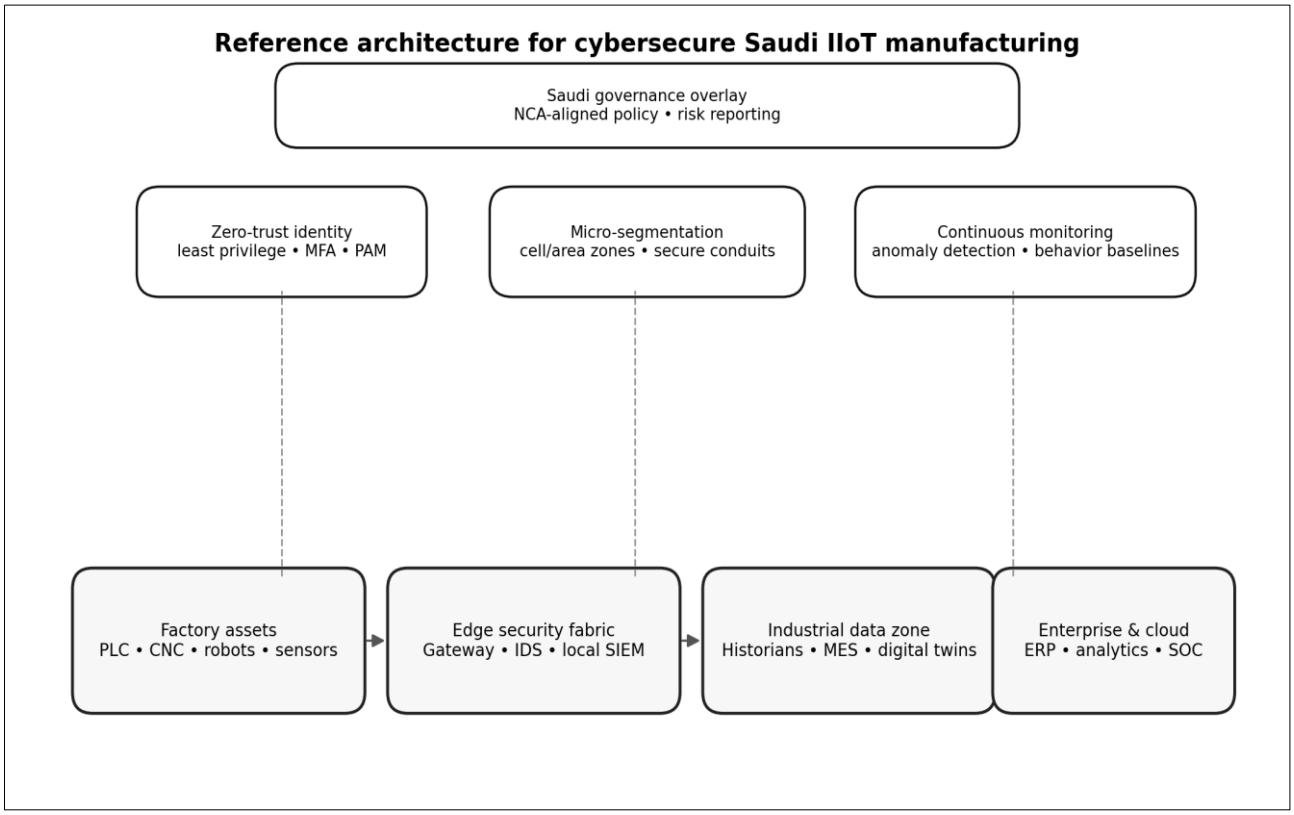

Figure 1: Layered reference architecture for cybersecure Saudi IIoT manufacturing.

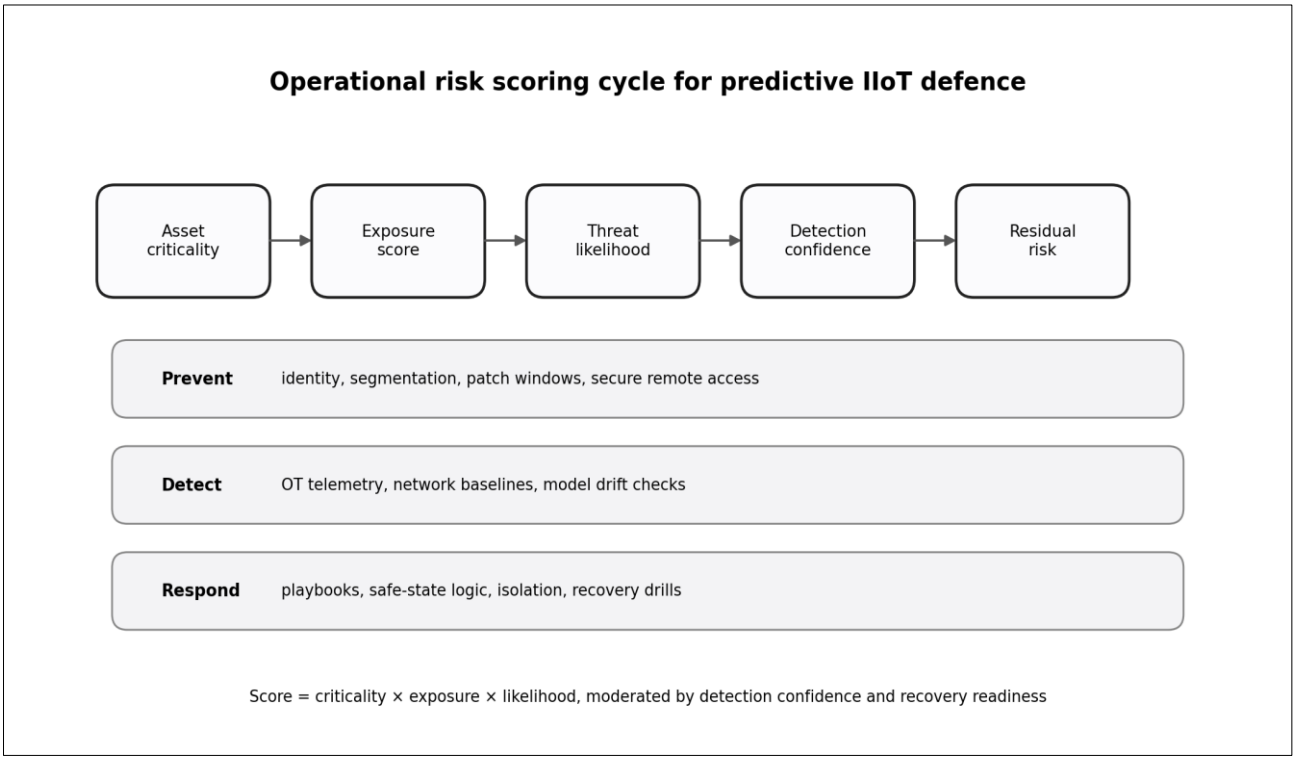

Figure 2: Operational risk-scoring cycle for predictive IIoT defence.

Table 2: Implementation roadmap for Saudi digital manufacturing entities

Phase	Priority action	Owner groups	Evidence of completion
1. Discover	Passive OT asset inventory and data-flow mapping	OT, IT, production engineering	Asset register with criticality and approved conduits
2. Control access	MFA, PAM and governed vendor remote access	Cybersecurity, procurement, vendors	Recorded sessions, privileged account list and access approvals
3. Segment	Cell/area zones, industrial firewalls and secure gateways	Network, OT engineering	Segmentation diagrams, firewall rules and isolation tests
4. Monitor	Edge IDS, SIEM integration and anomaly baselines	SOC, OT analysts	Alert catalogue, baseline reports and triage playbooks
5. Recover	Safe-state playbooks, backups and restart validation	Operations, safety, IT/OT	Exercise reports, backup restore tests and restart criteria

7. DISCUSSION: SAUDI VISION 2030 ALIGNMENT

The proposed architecture aligns closely with Saudi Vision 2030 because secure digital manufacturing supports industrial diversification, local content development, private-sector growth and high-value employment. Smart factories can improve resource efficiency, support resilient supply chains and strengthen the Kingdom's competitiveness in advanced production. However, these gains depend on trust. If manufacturers fear that connected systems will introduce unacceptable cyber risk, they may delay digital adoption or restrict integration. A clear cybersecurity architecture therefore becomes an enabler of transformation rather than a compliance burden.

Saudi industrial cities and giga-project supply chains provide a strong setting for architecture-based cybersecurity because many facilities are being modernized or built with digital systems from the beginning. Greenfield projects can design segmentation, monitoring and identity controls into the network before production starts. Brownfield factories need a phased approach because legacy systems cannot always be replaced quickly. A practical roadmap may begin with asset discovery and remote-access control, then move to segmentation, edge monitoring, backup validation, supplier governance and predictive analytics. This staged approach allows progress without requiring an unrealistic shutdown of production.

The Saudi context also highlights the importance of governance localization. International standards provide excellent foundations, but implementation must reflect local regulatory expectations, Arabic and English operating environments, contractor ecosystems and sector-specific requirements. Cybersecurity dashboards should be designed for both technical and executive audiences. Technical teams need alerts, asset lists and protocol visibility. Executives need risk heat maps, downtime exposure, compliance status and investment priorities. This dual reporting helps cybersecurity compete for resources in manufacturing organizations where capital is often directed first toward production capacity.

Another Saudi-specific issue is talent development. Advanced manufacturing cybersecurity requires hybrid professionals who understand networking, industrial control, safety, data analytics and operations. Such talent is globally scarce. The architecture should therefore be accompanied by workforce pathways: OT security analyst roles, plant cyber champions, vendor-security coordinators, digital manufacturing risk managers and incident-response teams trained for industrial environments. Partnerships among universities, technical institutes, manufacturers and government bodies can help build this capability. Research papers, applied case studies and industry sandboxes can also support the Premium Residency objective of demonstrating specialized contribution to the Kingdom's knowledge economy.

Predictive cybersecurity is especially relevant for Saudi manufacturing because large industrial ecosystems generate significant operational data. When properly governed, this data can support early warning systems, anomaly detection and risk forecasting. Yet prediction must not be oversold. Models require high-quality data, contextual labels, expert validation and continuous tuning. The uploaded reference paper notes that predictive model effectiveness depends on data quality, system complexity and implementation resources (Alqudhaibi *et al.,* 2025). Saudi manufacturers should therefore pilot models in defined production areas, validate them with engineers, measure operational outcomes and scale only after demonstrating value.

8. Research Gaps and Future Directions

Several research gaps remain. First, there is a need for Saudi manufacturing datasets that can support realistic evaluation of IIoT cybersecurity models while protecting sensitive plant information. Public datasets often fail to capture the timing, protocol diversity and production logic of real

factories. Synthetic datasets can help, but they must be validated against operational expertise. Future studies should explore privacy-preserving data sharing, federated learning and anonymized industrial telemetry so that Saudi manufacturers can improve detection models without exposing proprietary processes.

Second, more work is needed on explainable artificial intelligence for OT security. High offline accuracy is insufficient if engineers cannot understand why a model produced an alert. Research should examine explanations that connect cyber indicators with process context, such as abnormal command sequences, unusual maintenance timing, sensor drift, unexpected protocol use or divergence between a digital twin and physical behavior. Explainability should be evaluated by whether it improves response decisions, reduces false-positive fatigue and supports safe containment.

Third, cyber-physical resilience metrics require development. Many studies report precision, recall and F-measure, but plant leaders need metrics such as avoided downtime, time to isolate a compromised cell, recovery-time confidence, safety impact, product-quality assurance and supplier-response maturity. Future Saudi studies should integrate cybersecurity metrics with manufacturing performance indicators so that investment decisions can be justified in language understood by operations and finance leaders.

Fourth, architecture research should address small and medium-sized manufacturers. Large industrial firms may have dedicated security teams, but smaller suppliers often lack OT cybersecurity resources. Because these suppliers may connect to larger ecosystems, their weakness can become a shared risk. Scalable reference designs, managed security services, simplified procurement requirements and sector-specific templates can help raise the baseline. Saudi industrial clusters could benefit from shared cyber ranges, supplier assurance programs and maturity models adapted to different sizes of manufacturers.

Finally, future research should test architecture maturity through longitudinal case studies. A model may appear strong on paper but fail when confronted with maintenance pressure, legacy systems, vendor constraints or budget limitations. Case studies should track implementation over time, including barriers, cost, training needs, production impact and measurable reduction in risk. Such studies would support evidence-based policy and help Saudi Arabia develop globally relevant knowledge in secure digital manufacturing.

A final research need concerns validation governance. Before a predictive IIoT security model is used in a production plant, manufacturers should define acceptance criteria with operations teams rather than with data scientists alone. Validation should ask whether the alert arrives early enough to prevent unsafe conditions, whether the explanation is understandable to control engineers, whether the suggested containment step is compatible with the process, and whether the response can be executed during a shift handover. These questions make evaluation more realistic than isolated accuracy scores and ensure that cybersecurity tools support production decisions.

Another priority is secure-by-design procurement. Saudi manufacturers purchasing robots, sensors, drives, gateways or analytics platforms should request evidence of secure development, patch support, vulnerability disclosure, authentication capability, logging functions and integration with monitoring tools. Procurement teams rarely control cyber risk after installation, so security requirements must be included before contracts are signed. Future research can compare supplier security maturity across industrial sectors and develop procurement checklists tailored to Saudi industrial cities.

The growth of digital twins also deserves focused study. Digital twins can improve maintenance and planning, but they become risky if they mirror sensitive production processes without strong access control and integrity protection. Researchers should examine how to verify twin inputs, detect divergence between simulated and physical behavior, and prevent unauthorized use of twin models for reconnaissance. In high-value Saudi industries, twin security should be treated as protection of both operational knowledge and intellectual property.

Wireless industrial connectivity creates another gap. Private 5G, Wi-Fi 6 and low-power sensor networks can support flexible factories, mobile robots and real-time tracking, but they also introduce spectrum, authentication, roaming and device-management issues. Security studies should evaluate how wireless IIoT can be segmented, monitored and recovered when devices move across production zones. This is especially relevant for logistics-heavy plants, warehouses, ports and modular manufacturing facilities.

Finally, governance research should examine board-level accountability for OT risk. Many manufacturers still report cybersecurity through IT metrics that do not show production consequences. Future frameworks should translate cyber findings

into board language: maximum credible downtime, safety exposure, quality hold risk, supplier concentration, regulatory exposure and recovery confidence. When decision makers understand these indicators, cybersecure IIoT investment becomes easier to prioritize and sustain.

Human factors should also be examined through field research. Operators may bypass controls when controls conflict with urgent repairs, and engineers may create informal workarounds when remote access is slow. Studies based on interviews, simulations and incident exercises can reveal where security procedures create friction. The findings can then guide simpler workflows, role-based training and control designs that protect the plant without ignoring production realities. This human-centred approach is essential because cybersecure architecture ultimately depends on everyday decisions made by people on the factory floor.

Economic evaluation is another underdeveloped area. Researchers should model the cost of segmentation, monitoring, training and recovery against avoided downtime, reduced insurance exposure and improved customer confidence. Such analysis would help Saudi manufacturers move from fear-based cybersecurity spending to evidence-based investment planning.

Together, these directions would create a stronger empirical base for Saudi Arabia and could position the Kingdom as a contributor to global best practice in secure, resilient and competitive digital manufacturing. They would also support local talent pipelines by linking academic research with practical plant-level cybersecurity challenges. This connection is essential for sustainable industrial transformation across the Kingdom.

9. CONCLUSION

Cybersecure IIoT architecture is a foundation for Saudi Arabia's digital manufacturing ecosystem. Connected factories can improve productivity, quality, safety and sustainability, but their value depends on whether manufacturers can trust the data, systems and partners that support automation. This review has shown that the main risks arise from expanded connectivity, insecure legacy protocols, ransomware, data integrity attacks, supplier exposure, weak remote access and human-factor challenges. The answer is not a single technology; it is a layered architecture that integrates asset visibility, segmentation, zero-trust access, secure edge computing, predictive monitoring, governance and safe incident response.

The proposed model is practical for Saudi manufacturers because it recognizes both national ambition and operational constraints. It supports Vision 2030 by enabling industrial modernization while protecting production continuity and cyber-physical safety. Its strongest contribution is the integration of architecture and operations: controls are mapped not only to networks and devices, but also to risk scoring, supplier management, workforce behavior and recovery. The review also identifies future research needs in Saudi datasets, explainable AI, resilience metrics, SME adoption and longitudinal case studies. Overall, Saudi digital manufacturing can move from connected production to trusted production when cybersecurity is designed into every layer of the IIoT lifecycle.

REFERENCES

- Al-Ansari, A. O., & Alsubait, T. M. (2022). Predicting cyber threats using machine learning for improving cyber supply chain security. In 2022 Fifth National Conference of Saudi Computers Colleges (NCCC) (pp. 123-130). IEEE. https://doi.org/10.1109/NCCC57165.2022.10067692
- Al-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2). https://doi.org/10.14569/IJACSA.2023.0140292
- Alkahtani, H., & Theyazn, H. H. A. (2022). Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: Industrial control systems. Electronics, 11(11), 1717. https://doi.org/10.3390/electronics11111717
- Alqudhaibi, A., Aloseel, A., Jagtap, S., & Salonitis, K. (2022). Identifying and predicting cybersecurity threats in Industry 4.0 based on motivations towards a critical infrastructure. Advances in Manufacturing Technology XXXV, 10-16. https://doi.org/10.3233/ATDE220599
- Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for Industry 4.0: A proactive approach based on attacker motivations. Sensors, 23(9), 4539. https://doi.org/10.3390/s23094539
- Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: Developing a cybersecurity framework for manufacturing. Technology and Sustainability, 2(4), 372-387. https://doi.org/10.1108/TECHS-05-2023-0022
- Alqudhaibi, A., Krishna, A., Jagtap, S., Afy-Shararah, M., & Salonitis, K. (2023). Safeguarding food industry: Understanding cyber threats and ensuring cybersecurity. Engineering Proceedings, 40(1), 11. https://doi.org/10.3390/engproc2023040011

- Alqudhaibi, A., Krishna, A., Jagtap, S., et al. (2024). Cybersecurity 4.0: Safeguarding trust and production in the digital food industry era. Discover Food, 4, 2. https://doi.org/10.1007/s44187-023-00071-7
- Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., & Salonitis, K. (2024). Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. Cyber Security and Applications. https://doi.org/10.1016/j.csa.2024.100067
- Alqudhaibi, A., Albarrak, M., Aloseel, A., Munshi, A., Alsharif, T., Jagtap, S., & Salonitis, K. (2025). Proactive cybersecurity in Industry 4.0: A survey of cybersecurity threat prediction approaches in manufacturing systems. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01188-9
- Akwetey, H. M., & Danquah, P. (2022). Predicting cyber-attack using cyber situational awareness: The case of independent power producers. arXiv. https://doi.org/10.48550/arXiv.2202.01778
- da Silveira Dib, M., Ribeiro, B., & Prates, P. (2021). Federated learning as a privacy-providing machine learning for defect predictions in smart manufacturing. Smart and Sustainable Manufacturing Systems. https://doi.org/10.1520/SSMS20200029
- Dandamudi, S. R. P., Sajja, J., & Khanna, A. (2025). Advancing cybersecurity and data networking through machine learning-driven prediction models. International Journal of Innovative Research in Computer Science and Technology, 13(1), 26-33. https://doi.org/10.55524/ijircst.2025.13.1.4
- Langlois-Berthelot, J., Gaie, C., & Lebraty, J. F. (2021). Epidemiology inspired cybersecurity threats forecasting models applied to e-government. In Transforming Public Services (pp. 117-139). Springer. https://doi.org/10.1007/978-3-031-55575-6_6
- Liu, C. (2021). Risk prediction of digital transformation of manufacturing supply chain based on principal component analysis and backpropagation artificial neural network. Alexandria Engineering Journal. https://doi.org/10.1016/j.aej.2021.06.010
- Manning, L., & Kowalska, A. (2023). The threat of ransomware in the food supply chain: A challenge for food defence. Trends in Organized Crime. https://doi.org/10.1007/s12117-023-09516-y
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29
- Rahman, M. A., Al-Saggaf, Y., & Zia, T. (2020). A data mining framework to predict cyber attack for cyber security. In 2020 15th IEEE Conference on Industrial Electronics and Applications (pp. 207-212). IEEE. https://doi.org/10.1109/ICIEA48937.2020.9248225
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207
- Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., Quwaider, M., & Saldamli, G. (2020). Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model. In MCNA 2020 (pp. 113-118). IEEE. https://doi.org/10.1109/MCNA50957.2020.9264301
- Weinberg, A. I. (2024). Zero trust implementation in the emerging technologies era. Cybersecurity and Emerging Systems. https://doi.org/10.20517/ces.2024.41
- Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. IEEE Access, 9, 94318-94337. https://doi.org/10.1109/ACCESS.2021.3087109
- Zhukabayeva, T., et al. (2025). Cybersecurity solutions for Industrial Internet of Things-edge systems: A review. Sensors. https://pmc.ncbi.nlm.nih.gov/articles/PMC11723252/
- Saudi Vision 2030. (2024). Vision 2030 overview and transformation programs. https://www.vision2030.gov.sa/
- Digital Government Authority. (2024). Digital Transformation Strategies Across Saudi Arabia. https://dga.gov.sa/
- ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/
- MITRE. (2024). MITRE ATT&CK for ICS knowledge base. https://attack.mitre.org/matrices/ics/
- National Cybersecurity Authority. (2024). Saudi cybersecurity controls and national guidance. https://nca.gov.sa/
- U.S. Department of Commerce. (2025). Saudi Arabia digital economy: Country commercial guide. International Trade Administration. https://www.trade.gov/