© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722478

Predictive Maintenance of Airport Critical Systems Using Artificial Intelligence and IoT: A Framework for Saudi Vision 2030

TAIMOOR SHAHID MALIK
Consultant – Airport Special Systems, Jeddah, Saudi Arabia

Abstract- Saudi Arabia's aviation transformation under Vision 2030 requires airport infrastructure to support rapid growth while preserving safety, security, service continuity, and lifecycle value. Airport critical systems—including baggage handling systems, passenger boarding bridges, security screening equipment, closed-circuit television, access control, fire detection, power supplies, building management systems, communications networks, and airfield support assets—are tightly coupled. Failure in one subsystem can create cascading delays, congestion, security exposure, and reputational or financial loss. Traditional corrective and time-based preventive maintenance remain necessary but are insufficient for complex, sensor-rich environments in which degradation can be detected before functional failure. This review examines how artificial intelligence (AI), the Internet of Things (IoT), edge computing, digital twins, and enterprise asset-management platforms can enable predictive maintenance in Saudi airports. It synthesizes recent research on condition monitoring, anomaly detection, fault diagnosis, remaining useful life estimation, and maintenance decision support, while interpreting these capabilities within the operational and strategic context of the Saudi Aviation Strategy. The paper proposes a layered framework that links criticality analysis, secure IoT sensing, data governance, AI analytics, human validation, computerized maintenance management systems, and performance assurance. It also presents a phased implementation roadmap and a set of technical, operational, safety, cybersecurity, and economic indicators. The central argument is that predictive maintenance should not be implemented as an isolated algorithmic project. It should be treated as a safety-conscious, cyber-secure, human-governed asset-management transformation that supports airport reliability, capacity, workforce localization, and sustainable infrastructure under Vision 2030.

Keywords: predictive maintenance; artificial intelligence; Internet of Things; smart airports; airport critical systems; digital twins; condition monitoring; Saudi Vision 2030; aviation infrastructure; asset management

I. INTRODUCTION

Saudi Arabia is investing in a large-scale transformation of aviation, tourism, logistics, and transport infrastructure. The Saudi Aviation Strategy seeks to position the Kingdom as a global aviation hub, expand connectivity to more than 250 destinations, accommodate 330 million passengers annually, and increase air-cargo capacity to 4.5 million tonnes by 2030. These ambitions require not only new terminals, runways, airlines, and digital passenger services but also reliable operation of the technical systems that make airports safe, secure, and efficient. As passenger volumes and operational complexity rise, maintenance becomes a strategic capacity function rather than a back-office engineering activity.

An airport is a system of systems. Baggage handling, security screening, passenger processing, surveillance, access control, public address, fire alarm, radio, data networks, power, cooling, building automation, airfield lighting, boarding bridges, and ground-support facilities interact continuously. A failure in a conveyor motor may delay bags and aircraft; a degraded uninterruptible power supply may affect security devices; a network switch fault can interrupt cameras or access-control readers; and a passenger boarding bridge failure can disrupt gate utilization. The consequences may include reduced throughput, missed connections, flight delays, crowding, safety risk, contractual penalties, and loss of passenger confidence.

Conventional maintenance strategies are commonly divided into corrective, preventive, condition-based, and predictive approaches. Corrective maintenance restores an asset after failure. Preventive maintenance performs tasks at fixed calendar or usage intervals. Condition-based maintenance triggers action when measured condition exceeds a defined limit. Predictive maintenance extends condition-based practice by using historical and real-time data to estimate the probability, mode, or timing of failure and to recommend an intervention before service is lost. AI and IoT make this transition increasingly feasible because sensors can observe vibration, current, temperature, pressure, image quality, network performance, error logs, environmental conditions, and operational cycles at high frequency.

The technical promise, however, should not be overstated. Airport systems are safety- and security-relevant; failure data are rare and imbalanced; equipment is sourced from multiple vendors; operational technology may be old or proprietary; and changes to maintenance decisions require governance, validation, cybersecurity, and competent human oversight. A model that performs well in a laboratory may deteriorate when deployed under heat, dust, humidity, irregular loading, or changing passenger patterns. Predictive maintenance therefore requires an integrated architecture and a disciplined implementation process.

This paper reviews the technologies, applications, benefits, risks, and governance requirements of AI- and IoT-enabled predictive maintenance for airport critical systems. It focuses on Saudi Arabia and proposes a framework aligned with Vision 2030 outcomes: safe growth, resilient infrastructure, operational efficiency, digital transformation, local capability development, and sustainable lifecycle management. The paper addresses four questions: Which airport systems provide the strongest predictive-maintenance use cases? How should IoT, data platforms, AI, digital twins, and maintenance workflows be integrated? What controls are required for trustworthy implementation? And how can Saudi airport operators scale pilots into an assured national capability?

II. REVIEW METHODOLOGY

The study uses a structured narrative-review method. Peer-reviewed literature published mainly from 2020 onward was considered across predictive maintenance, industrial IoT, aviation maintenance, airport digitalization, anomaly detection, remaining useful life estimation, digital twins, cybersecurity, and asset management. Foundational standards and official Saudi aviation sources were also considered to connect the technical literature with national strategic objectives. Search concepts included combinations of "airport predictive maintenance," "aviation maintenance artificial intelligence," "IoT condition monitoring," "digital twin airport," "remaining useful life," "smart airport asset management," and "Saudi Aviation Strategy."

The evidence was synthesized into six analytical domains: asset criticality and failure consequences; sensing and connectivity; data engineering and governance; AI models and decision outputs; work-management integration; and safety, cybersecurity, and organizational assurance. The review deliberately distinguishes aircraft maintenance from airport infrastructure maintenance. Aircraft-focused research is valuable because it addresses safety-critical prognostics, heterogeneous sensors, and rigorous validation, but airport assets have different duty cycles, ownership structures, environmental conditions, and interfaces. Accordingly, aircraft findings are used as transferable methodological evidence rather than direct proof of effectiveness for every airport system.

The paper is conceptual and does not report a field experiment at a Saudi airport. Performance improvements described in the framework are proposed outcomes that must be demonstrated through controlled pilots and operational data. This limitation is important because predictive-maintenance value depends on local failure modes, data quality, maintenance maturity, spare-parts constraints, service-level agreements, and the cost of false alarms or missed failures.

III. STRATEGIC CONTEXT: SAUDI VISION 2030 AND AVIATION RELIABILITY

Vision 2030 treats transport and logistics as enablers of economic diversification, tourism, pilgrimage, trade, and quality of life. The aviation programme translates these objectives into increased passenger capacity, international connectivity, cargo growth, airport development, service improvement, and stronger sector competitiveness. GACA has also emphasized digital transformation, smart gates, automated baggage handling, artificial intelligence, advanced air mobility, safety, efficiency, and environmental sustainability. These priorities create a direct rationale for intelligent asset management: high-capacity airports cannot deliver reliable passenger and aircraft flows if critical technical assets are maintained only after failure.

Reliability contributes to Vision 2030 in several ways. First, it protects capacity. Equipment availability determines how many security lanes, baggage routes, gates, check-in positions, and operational workstations can be used during peaks. Second, it supports safety and security by reducing hidden degradation in alarms, detectors, cameras, power systems, and communications. Third, it improves passenger experience by limiting queue growth, baggage disruption, gate changes, and uncomfortable terminal conditions. Fourth, it protects investment by extending asset life and helping operators replace components according to condition rather than conservative schedules. Fifth, it supports sustainability by reducing unnecessary replacement, emergency travel, wasted energy, and premature disposal.

Saudi airports have distinctive operating conditions that should shape system design. High ambient temperature, airborne dust, large daily temperature ranges, coastal humidity at some locations, heavy seasonal peaks associated with Hajj and Umrah, and geographically distributed airport networks affect sensors and assets. Equipment models trained in a temperate environment may not represent local thermal loading or dust ingress. Predictive analytics should therefore learn from Saudi operational data and include environmental variables. The Kingdom's mix of major hubs, pilgrimage gateways, regional airports, and emerging mega-projects also suggests a tiered architecture: large airports may operate local edge analytics and digital twins, while smaller airports may use secure shared platforms and centralized specialist support.

A further strategic issue is localization. Predictive maintenance creates opportunities for Saudi engineers, technicians, data scientists, cybersecurity specialists, and universities to develop domain-specific models, failure libraries, Arabic-enabled maintenance knowledge systems, and national benchmarks. Vendor partnerships should therefore transfer skills and data access rather than create permanent dependence on opaque proprietary services. In this sense, predictive maintenance can be both an operational programme and a capability-building programme.

IV. AIRPORT CRITICAL SYSTEMS AND FAILURE MODES

Criticality should be assessed before selecting technology. An airport asset is not critical merely because it is expensive; criticality depends on the consequences of failure, redundancy, detectability, repair time, passenger or flight impact, and security or safety significance. A structured failure mode and effects analysis can rank assets by severity, occurrence, and detectability, while business-impact analysis can include throughput loss, delay minutes, queue growth, and regulatory consequences.

Baggage handling systems are strong candidates because they contain motors, bearings, belts, drives, sensors, scanners, conveyors, diverters, and programmable controls. Useful data include vibration, motor current, temperature, belt speed, jam counts, fault codes, bag volume, and start-stop cycles. Models can identify bearing wear, belt misalignment, abnormal current signatures, sensor contamination, or control anomalies before a route becomes unavailable. Because baggage systems are interconnected, graph-based models or digital twins may also estimate how local degradation affects network throughput and identify alternative routing.

Passenger boarding bridges experience mechanical, hydraulic, electrical, control, and structural stress. Sensor data can include motor current, hydraulic pressure, wheel vibration, elevation cycles, docking time, emergency stops, and environmental exposure. Predictive maintenance may reduce gate outages by identifying slow movement, leakage, alignment drift, or component fatigue. For bridges, remaining useful life must be combined with inspection and safety rules; AI should prioritize inspection rather than override statutory requirements.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722478

Security screening assets include X-ray machines, explosive trace detectors, metal detectors, under-vehicle surveillance systems, and associated conveyors and networks. Their maintenance condition affects security and passenger flow. Data sources include self-test logs, image-quality metrics, tube current, detector calibration, conveyor speed, error codes, alarm frequency, and environmental conditions. Models can detect gradual image degradation or component instability, but access to vendor diagnostics and security-sensitive data requires strict governance.

CCTV and access-control systems are distributed digital assets. Cameras may suffer lens contamination, focus loss, obstruction, overheating, network instability, storage errors, or power degradation. Access-control readers, locks, controllers, and credentials may show intermittent faults before complete loss. Computer vision can evaluate camera image quality, while network analytics can identify packet loss, latency, or unusual resets. For such systems, predictive maintenance and cybersecurity monitoring should be integrated because some symptoms may result from either component degradation or malicious activity.

Power and environmental systems are foundational. Uninterruptible power supplies, batteries, generators, switchgear, cooling units, pumps, and building-management systems support almost every airport function. Battery impedance, temperature, discharge behavior, harmonics, vibration, refrigerant pressure, fan current, and energy consumption can reveal degradation. AI can identify inefficient operation and predict failures, but life-safety and electrical protection functions require conservative thresholds and certified procedures.

Communication and information systems include radio, public address, flight-information displays, master clocks, telephone systems, servers, storage, switches, and airport operational databases. Logs and performance counters support anomaly detection, but changes in software configuration can create data drift. Maintenance models should therefore integrate configuration management and distinguish planned changes from emerging faults. Airfield assets such as lighting, power regulators, weather sensors, and surface-monitoring systems are also suitable, although access and safety constraints make sensor reliability and remote diagnostics especially important.

Table 1. Priority airport systems, data sources, and predictive-maintenance outputs

Critical system	Typical data	Likely degradation	Decision output
Baggage handling	Vibration, current, speed, jam and fault logs	Bearing wear, belt misalignment, motor overload	Inspect component; reroute; schedule repair
Passenger boarding bridges	Pressure, current, cycles, vibration, docking time	Hydraulic leakage, drive wear, alignment drift	Condition inspection and gate maintenance window
Security screening	Self-tests, image quality, calibration and error codes	Detector drift, tube degradation, conveyor instability	Calibration, vendor service, controlled component replacement
CCTV/access control	Image quality, temperature, packet loss, device resets	Lens contamination, overheating, network/power degradation	Cleaning, network repair, camera/reader replacement
Power and HVAC	Temperature, harmonics, battery impedance, pressure, energy	Battery ageing, fan/pump wear, inefficient cooling	Load transfer, maintenance, energy optimization
Communications/IT	Logs, latency, storage, errors, configuration	Network instability, storage degradation, software faults	Failover, patching, component or configuration action

V. ENABLING TECHNOLOGIES

IoT provides the sensing and connectivity foundation. Sensors may be embedded by the original equipment manufacturer or retrofitted to measure vibration, acoustic emission, temperature, humidity, pressure, current, voltage, speed, position, image quality, and environmental conditions. Gateways translate industrial protocols, timestamp data, filter noise, and transmit selected features to edge or central platforms. In airport operational technology, connectivity should be purpose-built: segmentation, device identity, encryption, secure update mechanisms, and controlled data flows are more important than simply connecting every asset.

Edge computing is valuable where latency, bandwidth, resilience, or data sensitivity prevents continuous cloud processing. A baggage conveyor vibration model can run near the asset and send only health indicators; a camera-quality model can process images locally without exporting security video; and a gateway can continue monitoring during wide-area network interruption. Edge models must still be centrally governed, versioned, monitored, and updated. Otherwise, airports may accumulate inconsistent models that cannot be audited.

The data platform links operational signals to asset context. Raw sensor values are insufficient without asset identifiers, location, manufacturer, model, installation date, maintenance history, operating mode, environmental exposure, and work orders. A common asset hierarchy and semantic model are therefore essential. Time-series databases, event streams, maintenance records, documents, and images can be combined in a lakehouse or other governed architecture. Data-quality controls should detect missing values, clock drift, sensor replacement, duplicated events, unit inconsistency, and changes in sampling rate.

AI methods serve different purposes. Unsupervised anomaly detection learns normal patterns and flags deviations where labeled failure data are scarce. Methods include clustering, isolation forests, autoencoders, one-class classifiers, and change-point detection. Supervised classification predicts known fault types when sufficiently labeled examples exist. Regression and survival models estimate degradation or time to failure. Deep learning can learn complex temporal relationships from multivariate sensor streams, while probabilistic models express uncertainty. Hybrid models combine engineering physics, rules, and machine learning, often improving trust and sample efficiency.

Remaining useful life estimation is attractive but difficult. A numerical RUL value may appear precise even when confidence is low. Airport operators should use prediction intervals and risk bands, such as “inspect within 48 hours,” rather than relying only on a single estimated number. Models should consider maintenance lead time, spare-parts availability, redundancy, operational peaks, and consequence of failure. Decision optimization can then schedule work during low-demand windows and group tasks by location or skill.

Digital twins extend monitoring by creating a continuously updated representation of an asset or system. A twin may range from a dashboard with live state to a physics-informed simulation that tests maintenance scenarios. At airport scale, twins can connect asset health to operational consequences: for example, forecasting whether several degraded conveyors will reduce baggage capacity below the demand expected for a pilgrimage peak. Research emphasizes that digital twins require reliable data, interoperability, lifecycle information, and clear purpose; visually impressive three-dimensional models alone do not constitute a useful maintenance twin.

Natural-language processing can extract knowledge from fault descriptions, technician notes, manuals, and service bulletins. It can standardize symptom descriptions, recommend similar past cases, and support troubleshooting. Generative AI may help summarize history or draft work instructions, but safety-critical recommendations should be grounded in approved technical documentation, with source traceability and human approval. The most effective architecture is therefore multimodal: numerical sensors, event logs, images, documents, and expert knowledge are combined to produce a transparent maintenance recommendation.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722478

VI. PROPOSED AI-IOT PREDICTIVE MAINTENANCE FRAMEWORK

The proposed framework contains six connected layers. Layer one is asset strategy and criticality. Operators define service functions, critical assets, failure modes, consequence categories, redundancy, inspection obligations, and performance targets. This prevents technology teams from selecting use cases only because data are easy to obtain. Each use case should have a business and safety case that specifies the current maintenance problem, baseline cost, expected benefit, false-alarm tolerance, and decision owner.

Layer two is sensing and secure connectivity. Existing OEM data should be used where reliable, supplemented by retrofit sensors only when justified. Sensors require calibration, environmental protection, health monitoring, and documented ownership. Gateways should enforce network segmentation, least-privilege access, encryption, signed software, secure time synchronization, and controlled remote support. Data collection must not compromise equipment certification or vendor warranties.

Layer three is the governed data foundation. A national or operator-level asset taxonomy links each signal to a unique asset, subsystem, airport, location, and work history. Data pipelines perform validation and preserve lineage. Maintenance records should use controlled failure codes and root-cause classifications so that labels improve over time. Access should be role-based, and sensitive security-system data should be separated according to classification and operational need.

Layer four is analytics and digital-twin services. Models generate anomaly scores, fault probabilities, RUL ranges, confidence levels, and operational impact estimates. Multiple models may be used for one asset: a fast edge detector for immediate anomalies, a central model for long-term degradation, and a rules engine for mandatory limits. A digital twin can test capacity consequences and maintenance options. Model selection should prioritize interpretability and robustness before complexity.

Layer five is maintenance decision and execution. Predictions become valuable only when integrated with the computerized maintenance management or enterprise asset-management system. Alerts should create a review task rather than uncontrolled automatic work orders. A qualified engineer evaluates evidence, checks operational context, and accepts, modifies, or rejects the recommendation. Approved actions then reserve labor, tools, spares, permits, and access windows. The outcome—confirmed fault, no fault found, component condition, downtime, and root cause—is fed back to improve the model.

Layer six is governance and performance assurance. A multidisciplinary board should include maintenance, operations, safety, security, cybersecurity, data science, procurement, legal, and quality functions. It approves use cases, risk classifications, validation criteria, model changes, vendor access, and retirement decisions. Each model should have an owner, intended use, prohibited use, training-data description, performance thresholds, fallback method, and monitoring plan. Human authority remains explicit.

The framework is designed for different airport sizes. Major hubs can operate extensive local data platforms and system twins, while regional airports can use standardized sensor kits and secure shared analytics. Federated learning may eventually allow models to learn across airports without centralizing all raw data, although privacy, security, and statistical heterogeneity must be addressed. A national knowledge base can record failure modes, validated features, benchmark data, and lessons learned while respecting security restrictions.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722478

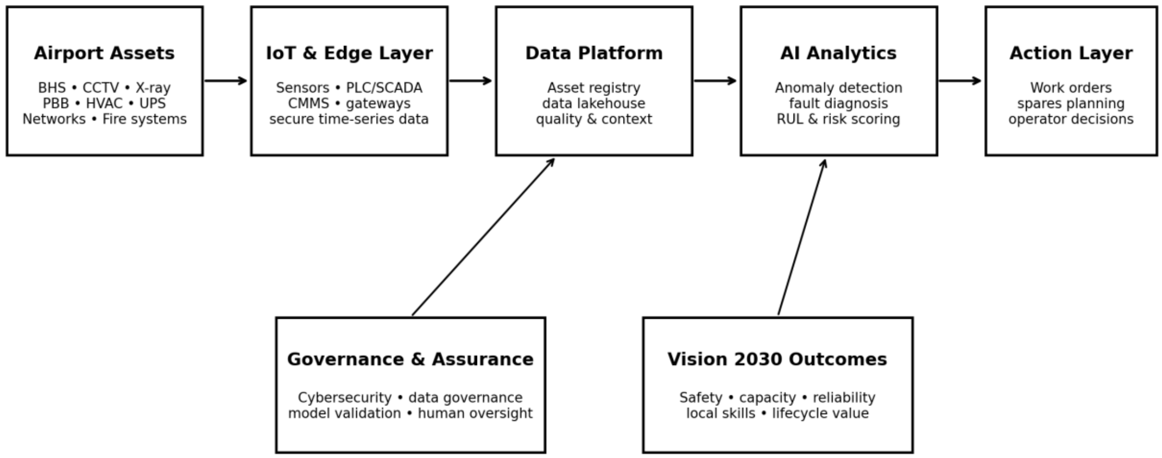

Figure 1. Layered AI–IoT predictive-maintenance framework for Saudi airports

VII. AI MODELS, VALIDATION, AND HUMAN DECISION-MAKING

Predictive-maintenance model development begins with a clearly defined target. "Predict failure" is too vague. The target may be detection of bearing degradation seven days before functional failure, identification of camera obstruction within five minutes, or prediction that a UPS battery string will fail a capacity test within three months. The horizon must match the time needed to inspect, procure, and repair. Labels should be verified through maintenance evidence rather than inferred from alarm logs alone.

Data splitting must respect time and asset identity. Randomly mixing records from the same asset across training and test sets can exaggerate accuracy. More realistic validation trains on earlier periods and evaluates later periods, or trains on some assets and tests on unseen assets. Rare failures require metrics beyond accuracy. Precision measures how many alerts are useful; recall measures how many true failures are detected; lead time measures operational usefulness; and calibration measures whether predicted probabilities match observed outcomes. Cost-weighted evaluation should reflect the different consequences of false positives and false negatives.

External validation is essential when a model is transferred between airports or equipment generations. Heat, dust, humidity, loading, maintenance practice, and firmware may alter patterns. Models should be commissioned through shadow mode, in which they generate predictions without changing maintenance. Engineers review results and establish a safe operating threshold. Controlled pilot deployment follows, with fallback to existing preventive procedures. Only after evidence demonstrates stable benefit should maintenance intervals be changed.

Explainability should support the technician's decision. Useful explanations identify which signals changed, how the current pattern differs from normal, relevant past cases, and the uncertainty of the forecast. A complex explanation graphic is less valuable than an operational statement such as: "Drive-end vibration at the bearing frequency has increased for 18 days and is now outside the range observed for comparable motors; inspect alignment and lubrication within 72 hours." Explanations should not imply causality when the model only detects correlation.

Human factors are central. Too many low-value alerts create alarm fatigue; poorly integrated dashboards force technicians to duplicate work; and opaque models can weaken professional accountability. Maintenance personnel should participate in model design, threshold selection, and post-event review. Training should cover both data literacy and limits of AI. The decision interface should show asset context, current health, trend, evidence, uncertainty, recommended action, safety restrictions, and links to approved procedures.

Continuous monitoring is required after deployment. Data drift, sensor drift, software updates, asset overhaul, and seasonal changes can reduce performance. Monitoring should track missing data, alert volume, confirmation rate, lead time, model calibration, and subgroup performance by asset type and airport. Significant change should trigger revalidation. In safety- or security-relevant cases, a model update should be managed like an engineering configuration change, with approval, version control, rollback, and documented testing.

VIII. CYBERSECURITY, DATA GOVERNANCE AND SAFETY ASSURANCE

Connecting airport operational technology increases cyber exposure. Sensors and gateways may become entry points; remote maintenance accounts may be abused; data can be manipulated to hide degradation or create false alarms; and centralized platforms may become high-value targets. Predictive maintenance should therefore follow security-by-design principles. Network architecture should separate enterprise IT, passenger services, security systems, and operational technology. Communications should be authenticated and encrypted, and devices should have inventory records, secure configuration, vulnerability management, and controlled update processes.

AI systems introduce additional threats. Data poisoning can distort training; adversarial inputs can mislead classifiers; model theft can expose proprietary or security information; and compromised pipelines can alter health scores. Defenses include data provenance, signed artifacts, independent validation, anomaly monitoring on the analytics pipeline, access logging, and segregation of development and production. Security teams should test not only the application but the entire machine-learning lifecycle.

Data governance defines who may collect, use, retain, share, and delete data. Some maintenance data are operationally sensitive because they reveal system vulnerabilities, airport layouts, or security-device performance. Video, access records, and staff-related data may also involve privacy obligations. Purpose limitation and data minimization should be applied: a vibration model does not need personal information, and a camera-health model may use image-quality features rather than stored scenes. Contracts should define data ownership, localization, subcontractor access, model portability, and access after termination.

Safety assurance requires evidence that the new system does not create unacceptable risk. The predictive model should be classified according to its role. A low-risk model may recommend inspection of an HVAC fan; a higher-risk model may influence maintenance of fire detection, screening, or power protection. The higher the consequence, the stronger the required verification, independence, documentation, and fallback. AI should not silently suppress mandatory alarms or extend regulated inspection intervals without formal approval.

A safety case can document the claim that the system supports safe maintenance, the evidence for model performance, the competence of users, cybersecurity controls, operating limits, and emergency fallback. Incident reporting should include model-related events, such as missed degradation, misleading explanations, data gaps, or unapproved model changes. This creates organizational learning and prevents AI failures from being treated merely as software defects.

Table 2. Principal implementation risks and controls

Risk	Potential consequence	Recommended control
Poor data quality	Unreliable alerts or missed degradation	Data lineage, validation, sensor-health monitoring
Model drift	Reduced accuracy after environmental or operational change	Continuous monitoring, revalidation, rollback
False positives	Alarm fatigue and unnecessary work	Risk-based thresholds, human review, precision monitoring
False negatives	Unexpected failure and service disruption	Conservative fallback, redundancy, recall and lead-time targets
Cyberattack	Manipulated data, outages, information exposure	Segmentation, identity, encryption, signed models, SOC monitoring
Vendor lock-in	High cost and limited transparency	Open interfaces, data ownership, portability requirements
Weak change management	Low adoption and poor feedback	Technician co-design, training, accountable process ownership

IX. OPERATIONAL AND ECONOMIC VALUE

The value of predictive maintenance should be measured at system level. A reduction in component failures is useful only if it improves airport outcomes. Relevant operational indicators include asset availability, mean time between failure, mean time to repair, unplanned downtime, maintenance lead time, passenger-processing capacity, baggage mishandling, gate outages, queue duration, delay minutes, and service-level compliance. Safety and security indicators may include overdue critical defects, degraded-system operating hours, alarm reliability, and audit findings.

Economic evaluation should include avoided disruption, emergency callouts, overtime, spare-parts consumption, secondary damage, lost asset life, and contractual penalties. Implementation costs include sensors, networking, cybersecurity, data platforms, integration, model development, validation, training, and ongoing monitoring. Benefits may take time because maintenance records and labels improve gradually. A pilot should therefore establish baseline cost and use a whole-life business case rather than promising immediate savings from model accuracy alone.

Spare-parts optimization is a major opportunity. Airport operators often hold expensive critical spares to protect continuity, yet excessive stock ties up capital and components may expire. Health forecasts can improve demand planning, but predictions should be combined with supplier lead time, repairability, commonality, and consequence of stockout. Workforce planning can also improve because predicted work can be scheduled with the right skills and access permits before a peak period.

Environmental benefits arise from longer asset life, efficient energy use, fewer emergency visits, and reduced premature replacement. Condition data can identify motors, fans, pumps, and cooling systems that consume excess energy because of degradation. Sustainability metrics should avoid double counting and should consider the energy and hardware footprint of the digital platform itself. The objective is optimized lifecycle performance, not technology for its own sake.

X. IMPLEMENTATION ROADMAP FOR SAUDI AIRPORTS

Phase 1 should establish governance, asset criticality, and data readiness. Operators map critical systems, maintenance maturity, failure history, network architecture, cybersecurity constraints, and business outcomes. Two or three use cases are selected using transparent criteria: high consequence or cost, measurable condition, sufficient failure opportunity, feasible integration, and a responsible operational owner. Baggage conveyors, passenger boarding bridges, UPS batteries, cooling equipment, and camera health are often suitable starting points.

Phase 2 conducts pilots in shadow mode and controlled deployment. Sensors and gateways are installed with engineering approval. Data are collected across normal, peak, and environmental conditions. Models are compared with simple baselines such as thresholds and statistical control charts. Technicians review alerts, and confirmed findings are recorded in structured form. The pilot should last long enough to capture seasonal and operational variation; a short demonstration with no real failures is not evidence of predictive capability.

Phase 3 scales successful use cases and integrates them with CMMS/EAM, spare-parts planning, and operational dashboards. Standard asset identifiers, interfaces, and cybersecurity patterns are reused. Digital twins may be added where system interactions or capacity consequences justify them. Procurement specifications should require access to relevant data, documented interfaces, cybersecurity support, and model portability.

Phase 4 develops cross-airport and national optimization. Validated models and lessons can be shared through a governed centre of excellence. Saudi universities and training providers can support research, certification, and workforce development. National benchmarks can compare reliability without exposing sensitive details. Federated analytics may help smaller airports benefit from broader evidence while retaining local data control.

Across all phases, change management is continuous. Engineers and technicians must see how the system improves their work rather than replaces judgment. Management should reward accurate feedback, including rejection of incorrect alerts, because such feedback improves the model. Governance should periodically stop use cases that do not demonstrate value. A mature programme is defined not by the number of connected sensors but by reliable decisions, measurable outcomes, and controlled risk.

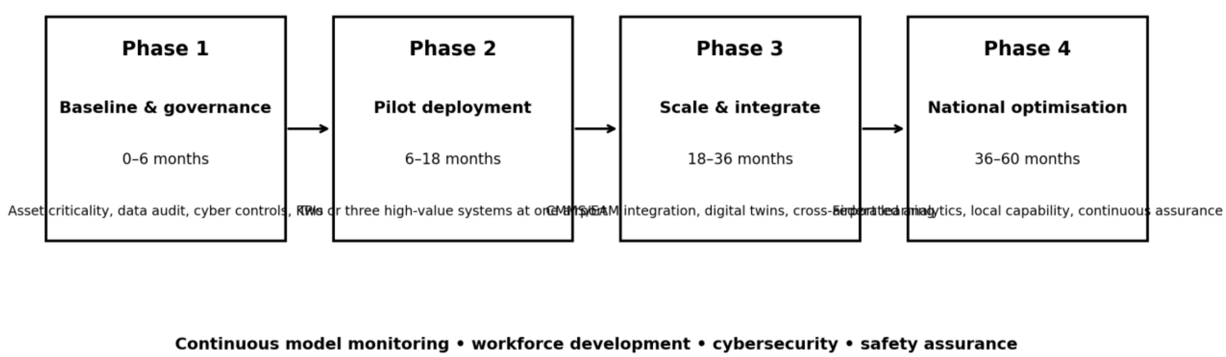

Figure 2. Phased implementation roadmap

XI. RESEARCH GAPS AND FUTURE DIRECTIONS

Several gaps require further research. First, public datasets for airport infrastructure maintenance are limited. Aircraft engine datasets are widely used, but baggage systems, boarding bridges, screening devices, and distributed airport facilities have different degradation patterns. Anonymized benchmark datasets and shared failure taxonomies would improve comparability.

Second, models must handle rare events and changing conditions. Self-supervised learning, transfer learning, physics-informed models, and synthetic data may reduce dependence on labeled failures, but each can introduce bias. Research should evaluate methods under realistic concept drift, sensor replacement, maintenance intervention, and environmental variation.

Third, system-level prediction is less mature than component monitoring. Airports need models that connect asset health to passenger flow, baggage capacity, gate planning, and resilience. Graph neural networks, simulation, and digital twins may help, but validation must be operationally grounded.

Fourth, explainability and human-AI teamwork need field evidence. Studies should measure technician trust, alert fatigue, diagnostic time, quality of decisions, and training needs rather than only model accuracy. Fifth, cyber-resilient predictive maintenance requires methods that distinguish equipment degradation from malicious manipulation. Sixth, lifecycle economics and sustainability need standardized evaluation.

For Saudi Arabia, research should examine heat, dust, coastal humidity, pilgrimage peaks, distributed airport operations, Arabic maintenance text, local supply chains, and workforce capability. Collaboration among airport operators, GACA, universities, technology firms, and equipment manufacturers could create a distinctive Saudi research programme in intelligent aviation infrastructure.

XII. CONCLUSION

AI- and IoT-enabled predictive maintenance can help Saudi airports move from reactive restoration and rigid schedules toward evidence-based, risk-informed maintenance. The strongest applications are found where critical assets generate meaningful condition data and where early intervention can protect capacity, safety, security, passenger experience, and lifecycle cost. Baggage handling, boarding bridges, security screening, CCTV, access control, power, cooling, communications, and airfield support systems all offer relevant use cases.

Technology alone is insufficient. Predictive maintenance depends on asset criticality, reliable sensors, secure connectivity, governed data, validated models, integration with work management, technician participation, and continuous assurance. Predictions should support accountable human decisions, and high-consequence applications require conservative operating limits and fallback procedures. Cybersecurity and data governance must be embedded from the start.

The proposed framework and roadmap align predictive maintenance with Saudi Vision 2030 by protecting aviation capacity, strengthening infrastructure resilience, improving service quality, developing local digital skills, and optimizing public and private investment. The appropriate measure of success is not the sophistication of the algorithm. It is whether airport systems remain available, safe, secure, efficient, and sustainable as the Kingdom's aviation network grows.

REFERENCES

[1] General Authority of Civil Aviation (GACA). (2026). Saudi Aviation Strategy. Riyadh, Saudi Arabia.

[2] General Authority of Civil Aviation (GACA). (2026). Saudi 2030 Elevates Aviation: Innovation for Sustainable Aviation. Riyadh, Saudi Arabia.

[3] Costa, J., Farinha, J. T., Raposo, H., Marques Cardoso, A. J., Carmo, A., Gonçalves, P., &

Farto, J. (2026). A systematic literature review on AI-driven predictive maintenance and fault detection in aircraft systems. Applied Sciences, 16(7), 3381. https://doi.org/10.3390/app16073381

[4] Mehdipour, N., et al. (2026). Integrating digital twins, data management and artificial intelligence for predictive maintenance in aviation: A comprehensive review. Digital Twins and Applications. https://doi.org/10.1049/dgt2.70029

[5] Agustian, E. S., & Pratama, Z. A. (2024). Artificial intelligence application on aircraft maintenance: A systematic literature review. EAI Endorsed Transactions on Internet of Things, 10(1). https://doi.org/10.4108/eetiot.6938

[6] Migliavacca, M., et al. (2023). Digital twins for aircraft maintenance and operation: A systematic literature review and an IoT-enabled modular architecture. Internet of Things, 24, 100991. https://doi.org/10.1016/j.iot.2023.100991

[7] Akinosho, T. D., et al. (2023). Improve predictive maintenance through the application of artificial intelligence: A systematic review. Results in Engineering, 20, 101645. https://doi.org/10.1016/j.rineng.2023.101645

[8] Alnoman, H., Bahroun, Z., & Hassan, N. (2025). A review of emerging airport technologies from a passenger-centric perspective. Proceedings of Engineering and Technology Innovation. https://doi.org/10.46604/peti.2025.14586

[9] International Organization for Standardization. (2014). ISO 55000: Asset management—Overview, principles and terminology. Geneva: ISO.

[10] International Organization for Standardization. (2018). ISO 31000: Risk management—Guidelines. Geneva: ISO.

[11] International Organization for Standardization. (2022). ISO/IEC 27001: Information security management systems—Requirements. Geneva: ISO.

[12] International Electrotechnical Commission. (2016). IEC 62443 series: Security for industrial automation and control systems. Geneva: IEC.

[13] International Civil Aviation Organization. (2018). Safety Management Manual (Doc 9859), 4th ed. Montreal: ICAO.

[14] International Civil Aviation Organization. (2022). Global Aviation Safety Plan 2023–2025. Montreal: ICAO.

[15] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23.

[16] Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. Mechanical Systems and Signal Processing, 20(7), 1483–1510.

[17] Lei, Y., Li, N., Guo, L., Li, N., Yan, T., & Lin, J. (2018). Machinery health prognostics: A systematic review from data acquisition to RUL prediction. Mechanical Systems and Signal Processing, 104, 799–834.

[18] Carvalho, T. P., et al. (2019). A systematic literature review of machine learning methods applied to predictive maintenance. Computers & Industrial Engineering, 137, 106024.

[19] Zonta, T., et al. (2020). Predictive maintenance in the Industry 4.0: A systematic literature review. Computers & Industrial Engineering, 150, 106889.

[20] Khan, S., & Yairi, T. (2018). A review on the application of deep learning in system health management. Mechanical Systems and Signal Processing, 107, 241–265.

[21] Susto, G. A., et al. (2015). Machine learning for predictive maintenance: A multiple classifier approach. IEEE Transactions on Industrial Informatics, 11(3), 812–820.

[22] Ran, Y., Zhou, X., Lin, P., Wen, Y., & Deng, R. (2019). A survey of predictive maintenance: Systems, purposes and approaches. arXiv:1912.07383.

[23] Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. IEEE Access, 8, 108952–108971.

[24] Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the digital twin:

A systematic literature review. CIRP Journal of Manufacturing Science and Technology, 29, 36–52.

[25] NIST. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: National Institute of Standards and Technology.

[26] NIST. (2024). Cybersecurity Framework 2.0. Gaithersburg, MD: National Institute of Standards and Technology.

[27] European Union Aviation Safety Agency. (2023). Artificial Intelligence Roadmap 2.0: A human-centric approach to AI in aviation. Cologne: EASA.

[28] Mobley, R. K. (2002). An Introduction to Predictive Maintenance (2nd ed.). Butterworth-Heinemann.

[29] Selcuk, S. (2017). Predictive maintenance, its implementation and latest trends. Proceedings of the Institution of Mechanical Engineers, Part B, 231(9), 1670–1679.

[30] Khoshkenar, A., et al. (2026). A holistic framework for airport spatial data maintenance: Bridging theory and practice. Digital Twins and Applications. https://doi.org/10.1049/dgt2.70021