INDUSTRIAL IOT

Integration of Industrial IoT and SCADA Technologies for Digital Oil Field Transformation under Saudi Vision 2030

Bilal Ahmed

Published November 2026

Abstract

Saudi Arabia's oil and gas sector is moving from instrumented production assets towards connected, analytically supported operations. Yet the value of industrial Internet of Things (IIoT) deployments depends on their interaction with supervisory control and data acquisition (SCADA), rather than the number of sensors installed. This detailed critical review carefully examines how that interaction can improve surveillance, maintenance, production decisions and environmental accountability while protecting safety-critical control functions. Thirty peer-reviewed publications dated 2020–2025 were selected through a focused, transparent review of oilfield digitalisation, industrial communications, edge computing, cyber-physical security and associated applications. Evidence was coded by operational use, integration mechanism, validation setting and reported limitation. The synthesis distinguishes deterministic control from advisory analytics and proposes a layered architecture in which field devices, local controllers, historians, edge services and governed analytical applications exchange contextualised information. The strongest practical opportunities concern fault detection, remote asset surveillance and prioritised intervention; attribution of production or emissions gains remains less secure without robust baselines. Saudi deployment consequently requires interoperable information models, resilient communications, independent safety barriers, cybersecurity assurance and workforce development. A staged implementation and evaluation framework is presented with measurable indicators and explicit decision rights. The review argues that a digital oilfield is successful when trustworthy information changes operational decisions safely, not merely when equipment becomes connected.

Keywords: Industrial Internet of Things; SCADA; digital oilfield; edge computing; Saudi Vision 2030; operational technology; asset integrity

1 Introduction

Oilfields are physically dispersed systems in which reservoir behaviour, artificial lift, treatment, compression and export infrastructure evolve on different timescales. Pressure transients may demand a controller response within seconds, while maintenance prioritisation can tolerate minutes or hours and field-development decisions require considerably longer horizons. Digital transformation therefore cannot be reduced to sending every instrument reading to an enterprise dashboard. It involves allocating observations and decisions to suitable layers, preserving process safety and demonstrating operational value. Wanasinghe et al. (2020) describe the industry's fragmented adoption of digital twins, whereas Al-Rbeawi (2023) places data integration alongside the changing organisation of upstream work. These observations explain why well-funded technology pilots may fail to become reliable field-wide capabilities.

Saudi Arabia presents an important setting because substantial mature production infrastructure must coexist with evolving digital capabilities and national ambitions for industrial competitiveness,

energy efficiency and technical employment. The country's energy operators manage large facilities and remote assets whose production continuity and environmental performance depend on dependable instrumentation. Although IIoT is sometimes presented as a replacement for SCADA, the two have different responsibilities. SCADA communicates supervisory states and authorised commands through industrial control infrastructure; IIoT extends sensing, contextual data access and analytics across organisational boundaries. Nechibvute and Mafukidze (2024) identify substantial integration potential, while Babayigit and Abubaker (2024) show that connectivity alone does not resolve legacy architectural constraints.

The central concern is the quality of the operational feedback loop. A vibration anomaly is valuable only if its timestamp, asset identity and operating context are correct, the alert reaches a responsible person, and action occurs before failure without creating another hazard. Pipeline monitoring faces equivalent difficulties when normal pressure changes resemble leakage events. Research on digital monitoring accordingly needs to consider networks, control authority, maintenance practice and validation together, rather than reporting isolated algorithm scores (Wu et al., 2023; Javid and Salahshoor, 2025). This review develops that integrated argument for Saudi digital oilfields.

2 Aim, objectives and review questions

The aim is to critically determine the technical and organisational conditions under which IIoT–SCADA integration can support dependable digital oilfield transformation in Saudi Arabia. Four distinct objectives guide the analysis: to clarify the responsibilities and interfaces of field sensing, supervisory control and analytical systems; to evaluate evidence for asset reliability, production and environmental applications; to identify cybersecurity, interoperability and information-quality risks; and to develop an implementation framework linking digital capabilities to measurable outcomes and national priorities. Rather than assuming that integration is beneficial, the review asks where it changes decisions, which barriers constrain deployment, how safety-critical authority should be separated and what evidence is needed before benefits can be attributed to the intervention.

3 Review methodology

A structured critical literature review was adopted because the question crosses petroleum engineering, industrial automation, information systems and operational security. The design aims to explain relationships and assess practical transferability, not to estimate a single pooled effect. Scholarly material published from January 2020 to December 2025 was identified through targeted searches of publisher platforms, engineering databases, indexing records and reference chains. Search combinations included “oilfield” OR “oil and gas”, together with “industrial IoT”, “SCADA”, “digital twin”, “remote monitoring”, “edge computing”, “pipeline leakage”, “predictive maintenance” or “industrial control cybersecurity”. The attached industry review informed the breadth of topics but was not treated as evidence for unverified numerical outcomes.

Eligible items were peer-reviewed journal articles or substantive review papers containing relevant technical concepts, evaluated applications, or defensible analysis of system design. Studies of unrelated domestic IoT, generic business digitalisation without industrial interfaces, conference abstracts without adequate methods, and material outside the specified publication window were excluded. An intentionally bounded set of thirty publications was retained to achieve balanced coverage of the integration problem. This is a purposefully selected review corpus, not a claim that

every eligible publication across all databases was retrieved. No fictitious screening counts, pooled sample sizes or unperformed experimental procedures are presented.

Each paper was examined against a common extraction frame: sector and asset type; control or data-transport layer; source of observations; analytical method; evaluation environment; reported result; and limitations concerning causality, deployment or security. Claims derived from laboratory experiments, simulation, industrial demonstration and broad conceptual reviews were distinguished before synthesis. For example, a pipeline leak detector validated against simulated faults offers evidence of methodological feasibility, not proof of the same performance under Saudi heat, variable flow regimes and intermittent communications. Findings were grouped into telemetry, supervisory operations, computing architecture, asset integrity, environmental monitoring and cyber-physical assurance. Conflicting evidence was interpreted through differences in validation setting and operating conditions.

The synthesis used narrative comparison rather than meta-analysis because the studies report incompatible outcomes such as classification accuracy, maintenance intervals, response time, architecture characteristics and qualitative adoption barriers. Effect sizes cannot be meaningfully pooled without common baselines and comparable observation periods. Citation metadata, publication dates and digital object identifiers were checked against discoverable scholarly records. The review's evidential strength nevertheless remains constrained by heterogeneous reporting and restricted access to proprietary oilfield operating data. Throughout, proposed architectural practices are identified as analytical recommendations rather than findings from a new field trial.

4 Architectural foundations of the connected oilfield

A useful architecture begins with the physical process. Wellhead transmitters, multiphase meters, downhole gauges, pump controllers and gas-detection instruments produce observations with different sampling frequencies, calibration requirements and safety significance. Programmable logic controllers and remote terminal units should continue to execute deterministic interlocks and equipment control locally. The supervisory layer collects authorised operational points, annunciates alarms and supports human oversight; its historian provides time-aligned operating records. The IIoT layer adds managed device connectivity, metadata, application programming interfaces and scalable analytical access. Ramzey et al. (2024) emphasise the value of combining remote monitoring with edge processing, while Rashad et al. (2022) illustrate how programmable controllers and supervisory interfaces can coexist with machine-learning functions.

Integration should follow a controlled information path rather than an unrestricted bridge between operational technology and enterprise networks. A gateway can map vendor-specific tag structures into a common asset model while preserving units, timestamps, operating states and quality flags. Message brokers and read-only historian interfaces then supply advisory applications without exposing controllers to arbitrary external commands. Shen et al. (2021) describe the role of synchronised observations in production-oriented digital twins, but model feedback must not be confused with permission to manipulate a live control loop. Figure 1 depicts the distinction between acquisition, control, contextual analytics and governed decision-making.

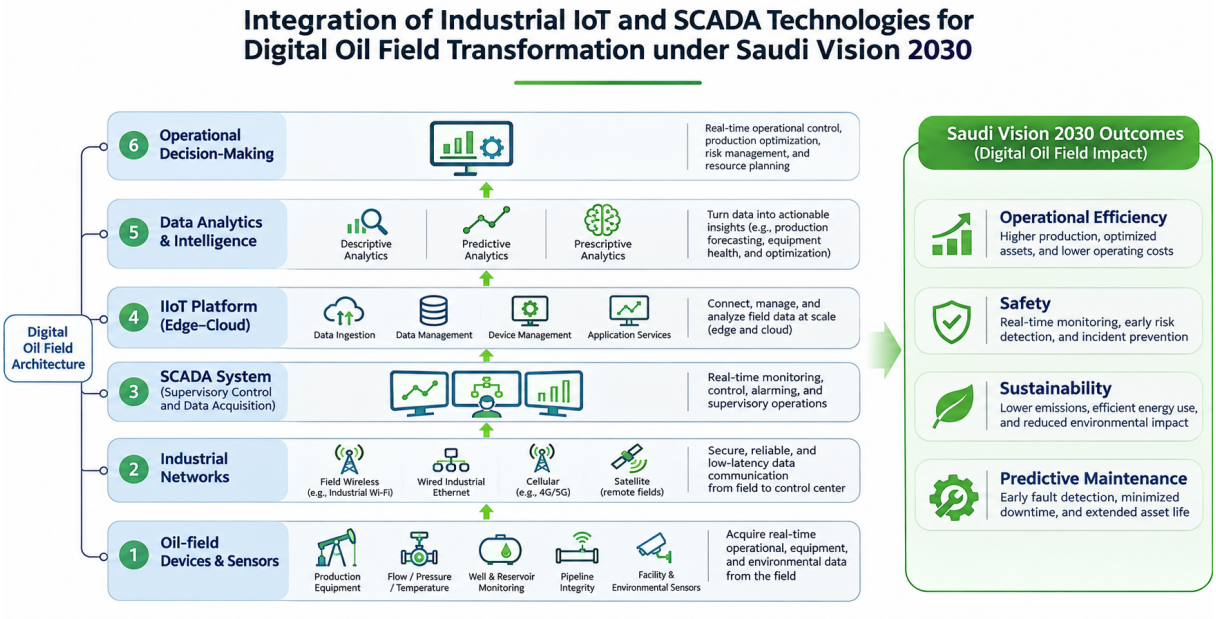


Figure 1. Layered architecture for IIoT–SCADA-enabled digital oilfield operations (author-developed conceptual representation).

Interoperability is simultaneously semantic and technical. A flow value lacking phase description, meter location or maintenance status can be formally transmitted and still mislead a model. Asset identifiers must therefore remain consistent across engineering drawings, historian tags, condition-monitoring systems and work orders. A versioned information model should record sensor calibration, uncertainty, data ownership and the relationship between equipment and production streams. Design choices also depend on field communications: fibre and industrial Ethernet may suit processing clusters, whereas remote wells can require cellular, microwave or satellite backhaul. Edge gateways should tolerate temporary link loss through buffered acquisition and local alarms, without weakening the existing control network (Knebel et al., 2023).

5 Evidence synthesis and thematic findings

5.1 Sensor observability and data trust

The primary contribution of IIoT is not an abstract quantity of data but improved observability of mechanisms that affect production. Pressure, temperature, electrical current, vibration and valve position can indicate developing pump wear, unstable separation or declining injectivity. However, sensor drift, duplicated packets and gaps in transmission may imitate faults. Data acquisition requires explicit timestamp synchronisation, outlier handling, measurement-unit reconciliation and preservation of raw records for forensic review. Jiang and Chen (2022) demonstrate the importance of network-traffic context for industrial anomaly classification, while Anwar et al. (2022) show that enriching SCADA communications with additional attributes can improve the interpretation of abnormal behaviour.

Sampling should be dictated by the physical question. High-frequency vibration is needed for certain rotating-equipment faults, whereas periodic pressure snapshots may suffice for long-term surveillance. Unfiltered high-rate streams can overwhelm limited remote links and increase storage costs without changing decisions. Local feature extraction can transmit a spectral indicator or confidence score alongside selected raw windows; analysts can retrieve detailed records when a threshold is

crossed. Quality assurance must distinguish missing data from a true zero and a temporarily isolated asset from a healthy operating state. Field engineers should approve sensor ranges and alarm rationalisation before machine-generated recommendations influence maintenance schedules. In this way the data layer becomes a controlled engineering asset rather than an ungoverned collection of dashboards.

5.2 Supervisory control, alarms and remote operations

SCADA's enduring strength is its clear supervisory function: it displays process state, records events and transfers commands through defined control hierarchies. Integration can increase situational awareness across remote well pads and central facilities, but unlimited alert propagation is undesirable. Alarm floods, stale readings and poor prioritisation can reduce operator confidence precisely when rapid action is needed. A modern digital oilfield should maintain authoritative alarm sources, rationalised severity levels and explicit acknowledgement rules. Operators also need visible evidence of whether a proposed intervention is advisory, approved for dispatch or executed. Historical data should retain the originating device, command authorisation and subsequent process response.

The petroleum terminal study by Rashad et al. (2022) indicates how supervisory automation can be extended by classification functions, while Babayigit and Abubaker (2024) explain why modern IIoT services differ from conventional SCADA in flexibility and scale. The implication is complementary design rather than wholesale replacement. At remote sites, automatic protective functions remain with local controllers and independently engineered safety systems. Supervisory operators can alter permitted setpoints only through validated control pathways. Analytics should initially recommend actions with traceable explanations; any transition towards automated optimisation must undergo hazard review, change management and controlled testing. These requirements matter especially during startup, abnormal operations and communication disruption, when a sophisticated model may have the least representative training data.

5.3 Edge, cloud and real-time analytical boundaries

The location of computation should reflect latency, connectivity, confidentiality and consequence of failure. Near-equipment edge processing supports immediate filtering, transient detection and continuity during network outages; central platforms support cross-field comparison, model training and resource-intensive simulation. Knebel et al. (2023) find that privacy, infrastructure and implementation maturity complicate cloud adoption in oil and gas. Ramzey et al. (2024) similarly frame edge computing as a means of distributing monitoring tasks. Neither finding justifies transferring safety-related control to an internet-dependent platform. Instead, local autonomy and secure replication should be designed together.

A robust pipeline separates the operational historian from the analytical store, maintains immutable event records and defines how model versions are promoted to production. During an outage, remote gateways should buffer measurements within specified retention limits and report the extent of data loss upon reconnection. Analytical services must expose freshness indicators, because a visually current dashboard can otherwise conceal outdated inputs. Resource scheduling also matters: continuous vibration analysis may require acceleration hardware, whereas a lightweight anomaly rule can execute on a modest industrial computer. A sensible deployment tests the lowest-complexity method that meets the operating requirement before choosing a more elaborate model. Cloud investment then follows a documented need for fleet learning or collaborative analysis rather than fashion.

5.4 Digital twins, equipment reliability and asset integrity

A digital twin becomes operationally credible when its representation is updated from trustworthy measurements and its decisions are checked against the physical asset. Wanasinghe et al. (2020) identified fragmented implementations; Shen et al. (2021) subsequently demonstrated a production-oriented combination of measured information and optimisation models. The evidence has expanded to subsea systems: Yang et al. (2023) use simulated and measured signals for composite-fault diagnosis, while Tao et al. (2024) integrate a dynamic Bayesian network with a twin to assess subsea-control reliability. These approaches are potentially valuable where physical access is expensive and degradation mechanisms interact.

Yet predictive maintenance is not synonymous with a successful failure classifier. An alarm delivered after the maintenance window has closed produces little practical benefit, while excessive false positives can waste scarce spares and offshore intervention capacity. Gupta et al. (2024) discuss architecture, explainability and model limitations across predictive-maintenance applications. Yao et al. (2024) extend the discussion to gas compressors with constrained and sensitive data, illustrating the importance of transferability across equipment. Saudi operators should therefore evaluate predicted failure lead time, missed high-consequence events, maintenance actions completed and avoided production interruptions alongside conventional accuracy measures. Model retraining must respect equipment replacements, process changes and shifts in operating envelopes.

5.5 Pipeline integrity and environmental performance

Pipeline surveillance provides a demanding test of integration because fluid transients, instrumentation noise and operational switching can produce signatures resembling leaks. Wu et al. (2023) distinguish hardware-based monitoring from analytical approaches and show that practical adoption depends on robustness as well as sensitivity. Liang et al. (2023) develop a continuously updated data-driven pipeline representation, whereas Javid and Salahshoor (2025) combine filtering and sequence learning on an IoT-enabled leak-detection platform. These studies support a layered approach: calibrated field instruments generate observations, SCADA captures operational context, and analytical services combine multiple indicators before escalation.

Environmental value requires equally careful measurement. Early detection may reduce spill consequence, but that outcome depends on confirmation time, isolation authority, intervention logistics and actual released volume. Similarly, energy dashboards cannot establish carbon reduction without verified consumption baselines, production-normalised intensity and the emissions factor of supplied energy. Digital monitoring may improve accountability by identifying excess flaring, abnormal compressor loading or unnecessary equipment cycling; attributing avoided emissions to the platform requires stronger evidence than a plausible optimisation narrative. The appropriate review conclusion is that IIoT–SCADA integration enables better monitoring and potentially better outcomes, while process-specific validation remains essential.

5.6 Cybersecurity and functional safety

Connecting previously isolated operational networks expands the attack surface and can compromise availability, integrity or confidentiality. A manipulated sensor value may produce an incorrect engineering decision even when the communications link appears healthy. Mohammed et al. (2023) analyse attacks directed at oil and gas control communications, and Alanazi et al. (2023) document why conventional enterprise controls cannot simply be transferred to SCADA environments. Zhu and Liyanage (2021) further distinguish cyber risks to safety-instrumented systems from routine

information-security concerns. The fundamental principle is that additional analytical connectivity must not undermine independent protection layers.

Security should begin with a verified asset inventory and documented trust boundaries. Segmented networks, tightly controlled jump hosts, authenticated updates and least-privilege service accounts can constrain unauthorised reachability. Where supported, gateways should enforce protocol allowlists and unidirectional data transfer for monitoring-only use cases. Monitoring should combine network indicators with physical-process plausibility, because normal-looking packets can still carry unsafe commands. Rehman and Bahşi (2024) examine process-aware monitoring, while Hotellier et al. (2024) derive detection logic from system specifications. Upadhyay et al. (2024) evaluate security arrangements in a combined SCADA–IoT test environment, supporting the case for testing protections under realistic industrial constraints.

Attack detection is not the whole assurance problem. Ma and Tsou (2024) propose combined passive and active detection, but active probing must be assessed for potential effects on controllers and production. Khalil et al. (2024) highlight deficiencies in threat-model validation; a digital oilfield consequently needs exercises involving operators, cyber responders and safety engineers. Protective shutdown logic, manual override and emergency communications should remain available when corporate networks or analytical services fail. Security events also require timestamped records linking cyber observations with operating conditions. The objective is recoverable safe operation, not the pursuit of a nominally perfect detection score in a laboratory dataset.

6 Saudi Arabia: Opportunities and deployment conditions

Within Saudi Vision 2030, digital oilfields can contribute to industrial capability development through highly reliable production, engineering innovation and local digital skills. That relationship should be presented as an operational pathway rather than an automatic causal effect. Technologies that help a single well pad do not necessarily scale across geographically distant assets with different generations of controllers, communications infrastructure and contracting arrangements. The strongest opportunities appear in asset-condition surveillance, integrated field operations, alarm management and production-loss analysis, provided that the underlying measurements are sufficiently reliable. Al-Rbeawi (2023) identifies wider process and workforce changes as a necessary component of digitalisation; Dua (2025) similarly reports that leadership, training and organisational integration shape adoption outcomes.

Saudi field conditions make engineering context decisive. Heat, dust, humidity and potentially hazardous atmospheres influence sensor specification and enclosure design. Remote transport links can experience variable performance; multilingual or distributed teams may require carefully standardised procedures and terminology. Brownfield integrations demand substantial tag reconciliation and planned outages, while greenfield projects can embed common data structures from commissioning. A phased programme should therefore begin with an asset-criticality assessment and the specific decisions that operators cannot currently make with sufficient confidence. Its first deliverables may be improved timestamp integrity or consolidated maintenance records rather than an advanced artificial intelligence dashboard.

The Khurais field is frequently discussed as an example of connected oilfield operations, but company-level performance statements should not be interpreted as independently controlled experimental estimates. Any reported improvements in inspection effort, maintenance expenditure or electricity use depend on time period, production conditions, comparison baseline and other

concurrent initiatives. The evidence-based task for Saudi operators is to define comparable local indicators before implementation. For reliability applications, those indicators may include mean time between functional failures, avoidable shutdown hours and verified maintenance lead time. For energy applications, they should include production-normalised electricity intensity and metered loads. Comparison against matched sites or interrupted time series would provide stronger attribution than uncomplicated before-and-after reporting.

7 Integrated discussion

Across the thirty studies, the recurring design issue is not absence of advanced algorithms but discontinuity between information, authority and action. Review papers offer convincing arguments for digitalisation, and individual technical studies demonstrate feasible diagnostics, but relatively few provide longitudinal evidence that integration improves operational outcomes across complete production systems. Korotkova et al. (2023) show why trust is negotiated during digital-twin adoption rather than delivered by technology suppliers. Belo et al. (2025) demonstrate that fundamental requirements need explicit specification before an oil-and-gas twin can be evaluated consistently. These findings reinforce the proposed distinction between a technically connected field and a governable digital operation.

A field-specific operational example makes the difference clear. A pump vibration model may identify abnormal behaviour, but its recommendation should be cross-checked against motor current, operating speed, production throughput and recent maintenance. The SCADA historian supplies the temporal context; an edge service computes a condition feature; the maintenance system creates a reviewed work request; and the operator decides whether intervention is economically and safely justified. Without these links, the detection remains an isolated software output. Mazzuto et al. (2025) illustrate the importance of combining process models, controller behaviour and anomaly prediction when considering operational resilience. Integration quality is therefore better assessed through completion of decision workflows than through the sheer volume of transmitted records.

Evidence must also be ranked by what it can legitimately establish. Simulated attacks reveal plausible vulnerabilities but cannot estimate incident frequency at a Saudi asset. Laboratory fault scenarios demonstrate analytical discrimination under defined conditions, not the reliability of unattended field deployment. Industrial case reports are more relevant to implementation but may conceal negative trials, confound multiple interventions or omit baseline uncertainty. Confidence should rise when independent datasets, long monitoring periods, operator acceptance, safety review and counterfactual comparisons converge. Table 1 translates these distinctions into practical evaluation requirements.

Table 1. Interpretation of evidence and validation requirements for oilfield integration studies.

Evidence setting	What it can establish	What it cannot establish	Field verification needed
Simulation or virtual faults	Feasibility and algorithm behaviour under stated assumptions	Unattended performance or realistic fault prevalence	Blind field data and operating-condition shifts
Laboratory control testbed	Protocol compatibility and controlled cyber response	Production resilience at scale	Latency, safety, overload and recovery tests

Evidence setting	What it can establish	What it cannot establish	Field verification needed
Instrumented industrial pilot	Usability, integration feasibility and initial workflow effects	Causal impact across all operating regimes	Matched baseline, outage accounting and operator logs
Longitudinal deployment	Observed operating trends and life-cycle burden	Attribution without controlling concurrent changes	Counterfactual comparison and uncertainty intervals
Narrative or synthesis	Transferable mechanisms and unresolved contradictions	Numerical benefit at a particular Saudi field	Local instrumentation and prospective validation

The economic case should be tested through a complete decision chain rather than a list of presumed technology savings. Initial expenditure includes hazardous-area instrumentation, communications redundancy, integration engineering, cybersecurity assessment, calibration, software support and training. Recurring expenditure includes model monitoring, historian storage, licences, network services and equipment replacement. Benefits are equally specific: reduced emergency dispatches, fewer avoidable shutdown hours, improved maintenance timing and better allocation of inspection effort. A credible business case assigns uncertainty ranges to each category, avoids double-counting outages and records unrealised benefits. The cost of false alarms must be included because repeated unnecessary dispatches can offset the value of earlier fault detection. Pilot economics should be revised as field evidence accumulates, not preserved as static procurement assumptions.

A further challenge concerns evidence provenance and digital accountability. A predicted anomaly should carry its input period, model version, asset identifier, confidence measure and the reason for escalation. Ahakonye et al. (2023) demonstrate that intrusion detection depends on careful feature selection; the same lesson applies to operational analytics where redundant or misleading features can generate unstable conclusions. Accepted and rejected recommendations reveal adoption, support retraining and enable incident reconstruction. Decisions to retire a model should be as clearly governed as decisions to introduce one. These practices also strengthen the case for carefully controlled information exchange between operational and analytical teams, because trustworthy audit trails matter to safety-critical operations.

These findings suggest a progression from visibility to prediction and then to governed optimisation. Visibility requires functioning instruments and transparent alarms. Prediction adds validated models and operational context. Governed optimisation adds controlled authority, economic criteria, incident recovery and auditability. Attempts to automate an immature data environment risk accelerating incorrect decisions. Conversely, excessive central approval can prevent field teams from responding to genuine faults. The architecture must allocate autonomy according to risk: routine analytics can be automated, safety-critical interventions need protected local logic, and material production changes require approved operating procedures. This balanced approach is more defensible than promising a fully autonomous oilfield within a fixed implementation period.

8 Research gaps and future agenda

Five gaps deserve attention. First, published studies rarely compare IIoT–SCADA architectures using shared measures of data freshness, operational latency, availability and lifecycle cost. Second, model validation often concentrates on classification accuracy rather than the combined economic and safety cost of missed or false alarms. Third, evidence about cross-vendor semantics, tag migration

and long-term maintainability remains thinner than evidence about new sensing technologies. Fourth, few oilfield evaluations follow environmental indicators far enough to distinguish monitoring improvements from verified reductions in leakage or energy intensity. Finally, human factors, local workforce capability and decision accountability are often mentioned but insufficiently tested alongside technical architectures.

Future Saudi research should use comparative field designs wherever feasible, clearly separating baseline operations from intervention periods and reporting uncertainty. Multisite tests could compare edge-only with hybrid edge–central arrangements under communication degradation. Maintenance studies should measure response and work-order completion, not solely prediction metrics. Cyber-physical research should examine safe degradation during compromised communications and coordinated restoration with human operators. Mixed technical and organisational evaluation would make the evidence more useful to asset owners, regulators and local technology developers. Independent validation should also include planned shutdowns, sensor drift, network isolation and changes in operator response under operational pressure. Publication of anonymised benchmark datasets and transparent interface specifications would also improve reproducibility while protecting commercially sensitive operational details.

9 Implementation and evaluation framework

The proposed implementation comprises five decision gates. First, asset owners define high-value operational problems, safety constraints and pre-intervention measures. Second, engineering teams audit instrumentation, communications, historian quality and source-system identifiers. Third, a bounded pilot establishes secure read-only data flows, explicit model ownership and operator review procedures. Fourth, the solution is evaluated in normal and abnormal conditions, including sensor faults, network interruptions and rejected recommendations. Fifth, successful functions are incorporated into maintenance, management-of-change and cybersecurity processes before broader expansion. This sequence limits premature automation and makes each investment accountable to operational benefits (Table 2).

Table 2. Proposed five-gate pathway for implementation and evaluation in Saudi oilfields.

Gate	Technical and organisational deliverable	Acceptance criterion	Primary indicator
1 · Define	Use case, asset criticality and baseline	Named operational owner and measurable problem	Existing failure, response or energy baseline
2 · Prepare	Tag audit, timestamps, network and hazard assessment	Traceable measurements and protected control	Data quality and communication availability
3 · Pilot	Read-only integration and reviewed recommendations	Reliable workflow under controlled conditions	Alert lead time and action completion
4 · Validate	Abnormal-state, cyber and disconnection tests	Safe degraded mode and documented recovery	False alarms, recovery time and intervention risk
5 · Scale	Change control, workforce training and benefits review	Repeatable governance and sustained improvement	Production-normalised value and lifecycle cost

Governance should assign responsibility separately for instruments, local control, information models, analytical code and final operational decisions. A shared change register links model updates to process modifications and staff training. Procurement should favour documented interfaces,

exportable data, support for local testing and clear incident responsibilities, rather than dependence on a single vendor ecosystem. Training needs to include the ability to challenge an implausible recommendation and to operate safely without analytical assistance. Digital oilfield maturity is ultimately demonstrated when personnel can explain what a model knows, what it does not know and who is permitted to act on its output. Figure 2 traces the proposed sequence from digital integration to verified operational outcomes.

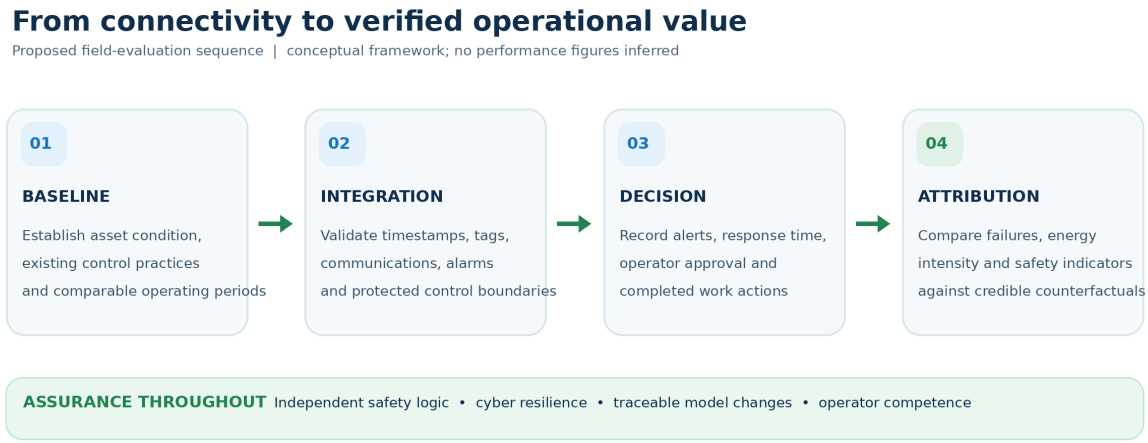


Figure 2. Proposed sequence for tracing digital integration to verified operational outcomes (conceptual; no field performance data).

10 Limitations

This article is a critical review and does not claim new measurements from Saudi production facilities. The thirty-paper corpus was purposefully bounded and cannot establish exhaustive coverage or bibliometric prevalence. Published results vary substantially in operating environment, asset scale and evaluation method, preventing quantitative pooling. Company narratives and technical demonstrations may also be affected by selective reporting. DOI and bibliographic checks establish that cited works are traceable, not that every claim within them has been independently replicated. Proposed deployment stages therefore constitute reasoned engineering guidance requiring prospective field validation. Any local implementation must additionally satisfy applicable operational, safety, cybersecurity and contractual requirements.

11 Conclusion

IIoT and SCADA can form a credible foundation for digital oilfield transformation when each contributes a distinct capability within an accountable operational architecture. SCADA preserves supervisory visibility and authorised control; IIoT broadens observation and analytical accessibility; edge systems protect responsiveness; and governed models support better maintenance and production decisions. The literature provides substantive support for improved diagnostic possibilities, yet evidence for sustained production, financial and environmental gains remains conditional on implementation quality and sound evaluation. For Saudi Arabia, the priorities are trustworthy field measurements, interoperable data definitions, secure operational boundaries and a workforce able to interpret and challenge analytical outputs. Phased deployment, independent safety arrangements and transparent outcome measurement can turn digital investment into defensible operational value.

Future studies should test these integrated mechanisms against field-level baselines rather than evaluating technical components in isolation.

References

[1] Ahakonye LAC, Nwakanma CI, Lee JM, Kim DS (2023). SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet of Things*, 21, 100676. https://doi.org/10.1016/j.iot.2022.100676

[2] Alanazi M, Mahmood A, Chowdhury MJM (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 125, 103028. https://doi.org/10.1016/j.cose.2022.103028

[3] Al-Rbeawi S (2023). A review of modern approaches of digitalization in oil and gas industry. *Upstream Oil and Gas Technology*, 100098. https://doi.org/10.1016/j.upstre.2023.100098

[4] Anwar M, Lundberg L, Borg A (2022). Improving anomaly detection in SCADA network communication with attribute extension. *Energy Informatics*, 5, 69. https://doi.org/10.1186/s42162-022-00252-1

[5] Babayigit B, Abubaker MB (2024). Industrial Internet of Things: A review of improvements over traditional SCADA systems for industrial automation. *IEEE Systems Journal*, 18(1), 120–133. https://doi.org/10.1109/JSYST.2023.3270620

[6] Belo RC, Pimenta MS, Salvador TT, Petry RH, Abel M (2025). Fundamental requirements of digital twins for production system in oil and gas industry: A systematic literature review. *Information and Software Technology*, 184, 107742. https://doi.org/10.1016/j.infsof.2025.107742

[7] Dua S (2025). Exploring the experiences of oil and gas industry executives in embracing industry 4.0: Insights, challenges, and strategies. *Computers & Industrial Engineering*, 208, 111377. https://doi.org/10.1016/j.cie.2025.111377

[8] Gupta S, Kumar A, Maiti J (2024). A critical review on system architecture, techniques, trends and challenges in intelligent predictive maintenance. *Safety Science*, 177, 106590. https://doi.org/10.1016/j.ssci.2024.106590

[9] Hotellier E, Sicard F, Francq J, Mocanu S (2024). Standard specification-based intrusion detection for hierarchical industrial control systems. *Information Sciences*, 659, 120102. https://doi.org/10.1016/j.ins.2024.120102

[10] Javid A, Salahshoor K (2025). Real-time leak detection system: A hybrid model of moving average and Kalman filters with long short-term memory (LSTM) on the Internet of Things (IoT) platform. *Process Safety and Environmental Protection*, 202, 107713. https://doi.org/10.1016/j.psep.2025.107713

[11] Jiang JR, Chen YT (2022). Industrial control system anomaly detection and classification based on network traffic. *IEEE Access*, 10, 41874–41888. https://doi.org/10.1109/ACCESS.2022.3167814

[12] Khalil SM, Bahsi H, Korõtko T (2024). Threat modeling of industrial control systems: A systematic literature review. *Computers & Security*, 136, 103543. https://doi.org/10.1016/j.cose.2023.103543

[13] Knebel FP, Trevisan R, Nascimento GS, Abel M, Wickboldt JA (2023). A study on cloud and edge computing for the implementation of digital twins in the oil and gas industries. *Computers & Industrial Engineering*, 182, 109363. https://doi.org/10.1016/j.cie.2023.109363

[14] Korotkova N, Benders J, Mikalef P, Cameron D (2023). Maneuvering between skepticism and optimism about hyped technologies: Building trust in digital twins. *Information & Management*, 60(4), 103787. https://doi.org/10.1016/j.im.2023.103787

[15] Liang J, Ma L, Liang S, Zhang H, Zuo Z, Dai J (2023). Data-driven digital twin method for leak detection in natural gas pipelines. *Computers and Electrical Engineering*, 110, 108833. https://doi.org/10.1016/j.compeleceng.2023.108833

[16] Ma YW, Tsou CW (2024). A novel passive-active detection system for false data injection attacks in industrial control systems. *Computers & Security*, 145, 103996. https://doi.org/10.1016/j.cose.2024.103996

[17] Mazzuto G, Pietrangeli I, Ortenzi M, Ciarapica FE, Bevilacqua M (2025). Leveraging digital twin for operational resilience in the oil and gas industry. *Array*, 27, 100443. https://doi.org/10.1016/j.array.2025.100443

[18] Mohammed AS, Anthi E, Rana O, Saxena N, Burnap P (2023). Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. *Computers & Security*, 124, 103007. https://doi.org/10.1016/j.cose.2022.103007

[19] Nechibvute A, Mafukidze HD (2024). Integration of SCADA and Industrial IoT: Opportunities and challenges. *IETE Technical Review*, 41(3), 312–325. https://doi.org/10.1080/02564602.2023.2246426

[20] Ramzey H, Badawy M, Elbaset AA (2024). Crude oil industry remote monitoring and management based on Industrial Internet of Things and edge computing integration: A comprehensive survey. *Results in Engineering*, 24, 103034. https://doi.org/10.1016/j.rineng.2024.103034

[21] Rashad O, Attallah O, Morsi I (2022). A smart PLC-SCADA framework for monitoring petroleum products terminals in industry 4.0 via machine learning. *Measurement and Control*, 55(7–8). https://doi.org/10.1177/00202940221103305

[22] Rehman MU, Bahşi H (2024). Process-aware security monitoring in industrial control systems: A systematic review and future directions. *International Journal of Critical Infrastructure Protection*, 47, 100719. https://doi.org/10.1016/j.ijcip.2024.100719

[23] Shen F, Ren SS, Zhang XY, Luo HW, Feng CM (2021). A digital twin-based approach for optimization and prediction of oil and gas production. *Mathematical Problems in Engineering*, 2021, 3062841. https://doi.org/10.1155/2021/3062841

[24] Tao H, Jia P, Wang X, Wang L (2024). Reliability analysis of subsea control module based on dynamic Bayesian network and digital twin. *Reliability Engineering & System Safety*, 248, 110153. https://doi.org/10.1016/j.ress.2024.110153

[25] Upadhyay D, Ghosh S, Ohno H, Zaman M, Sampalli S (2024). Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. *International Journal of Critical Infrastructure Protection*, 47, 100705. https://doi.org/10.1016/j.ijcip.2024.100705

[26] Wanasinghe TR, Wroblewski L, Petersen BK, et al. (2020). Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE Access*, 8, 104175–104197. https://doi.org/10.1109/ACCESS.2020.2998723

[27] Wu T, Chen Y, Deng Z, et al. (2023). Oil pipeline leakage monitoring developments in China. *Journal of Pipeline Science and Engineering*, 3(4), 100129. https://doi.org/10.1016/j.jpse.2023.100129

[28] Yang C, Cai B, Wu Q, et al. (2023). Digital twin-driven fault diagnosis method for composite faults by combining virtual and real data. *Journal of Industrial Information Integration*, 100469. https://doi.org/10.1016/j.jii.2023.100469

[29] Yao J, Liang W, Zheng Z, Ouyang Y, Liao C (2024). Research on maintenance cycle prediction for energy equipment with limited and sensitive data. *Engineering Failure Analysis*, 164, 108696. https://doi.org/10.1016/j.engfailanal.2024.108696

[30] Zhu P, Liyanage JP (2021). Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: A specific review of issues and challenges in safety instrumented systems. *European Journal for Security Research*, 6(2), 125–149. https://doi.org/10.1007/s41125-021-00076-2