Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i04.003

OPEN ACCESS

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

Original Research Article

AI-Based Threat Detection and Response for Remote Artifical Lift (ESP) Wells and Pipeline Monitoring Systems

Shajji Mohiuddin[1]*
[1]L & T Technology Services: Mumbai, India

***Corresponding Author**
Shajji Mohiuddin
L & T Technology Services: Mumbai, India

Article History
Received: 13.05.2026
Accepted: 01.07.2026
Published: 04.07.2026

Abstract: Remote oil and gas assets are increasingly operated through connected instrumentation, supervisory control platforms, historians, cloud analytics and integrated operations centres. This digital shift improves production surveillance, artificial-lift optimisation, reservoir management and pipeline integrity, but it also creates a cyber-physical attack surface in which manipulated telemetry, unauthorised commands, delayed alarms or compromised remote access can produce safety, environmental and production consequences. This review develops an artificial intelligence (AI)-based threat detection and response model for remote wellheads, electric submersible pump (ESP) systems and pipeline monitoring environments. Evidence published between 2020 and 2025 is synthesised across operational technology (OT) security, industrial anomaly detection, petroleum analytics, Permanent Downhole Monitoring Systems (PDHMS), downhole gauges, variable-frequency drive (VFD) monitoring and critical-infrastructure guidance. The review argues that PDHMS should not be treated as a separate topic; bottom-hole pressure, downhole temperature, vibration, intake and discharge pressure, motor current and real-time production data are integrated evidence sources for cyber-physical resilience. The proposed model combines data assurance, process-aware baselines, network intrusion detection, asset criticality, explainability, and operator-approved response playbooks. For wellheads, the key requirement is to detect command and pressure-flow inconsistencies before unsafe valve or choke action occurs. For ESP systems, cyber analytics must distinguish genuine pump degradation from malicious manipulation of VFD settings, vibration, motor current, frequency and downhole gauge data. For pipelines, detection must integrate SCADA anomalies, leak indicators, geospatial evidence and communications integrity. The review therefore prioritises cyber-physical consequence rather than alert volume, linking AI outputs to verification, containment, safe-state operation, recovery and continuous learning.

Keywords: Artificial Intelligence, Threat Detection, Operational Technology, SCADA, Electric Submersible Pump, Pipeline Monitoring.

1. INTRODUCTION

Unconventional and conventional oil and gas operations increasingly depend on remote monitoring, automated control and advanced analytics across production sites, gathering systems and long pipeline corridors. AI is already used for exploration, production forecasting, reservoir engineering, artificial-lift decisions and health, safety and environment analytics [1]. These developments are valuable because the same data streams that optimise production also support safety decisions, pump surveillance, shutdown logic, chemical injection, leak verification and maintenance dispatch. A field sensor is therefore not only a production

indicator. It can also influence a control-room decision, a remote command or an emergency response.

Cybersecurity in this environment must be understood as a cyber-physical problem. A compromise of an enterprise workstation is serious, but a compromise of a remote terminal unit (RTU), programmable logic controller (PLC), VFD, historian interface, satellite backhaul link or engineering workstation can alter what operators believe is happening in the field. Operational technology (OT) security guidance stresses that safety, reliability, determinism and physical consequences distinguish OT from ordinary information technology [2]. Industrial automation standards also require risk assessment to consider zones, conduits, security levels, segmentation and lifecycle controls rather than relying only on perimeter defence [3]. These principles are especially important for assets located across deserts, offshore facilities and isolated pipeline corridors, where the first response may be a remote operator working from incomplete telemetry.

AI-based threat detection can close part of this visibility gap when it is designed for field operations. Conventional signature tools are useful for known malware or policy violations, whereas AI can learn relationships among pressure, flow, temperature, vibration, motor current, pump frequency, valve position, communication timing and user behaviour. Machine-learning studies in industrial control systems (ICS) show that supervised, semi-supervised and unsupervised methods can support network-level intrusion detection and physical-process anomaly detection [8-14]. The same studies caution that near-perfect laboratory scores may not survive noisy sensors, unknown attacks, changing production modes or data drift [9-11]. AI should therefore be framed as an explainable decision-support layer constrained by engineering knowledge, safety interlocks, validation workflows and accountable response governance.

The problem addressed in this review is the lack of an integrated model that connects AI detection, risk prioritisation and response for remote wellhead, ESP and pipeline monitoring systems. Petroleum AI studies often focus on production or equipment performance, while cybersecurity studies often focus on industrial networks without asset-specific petroleum context [1-14]. Operators need a practical model that can assess whether an abnormal ESP current trend is pump wear, gas lock, power-quality instability or adversarial manipulation; whether a pressure imbalance is caused by a leak, instrumentation failure, valve misoperation or false data injection; and whether a remote wellhead command should be approved, challenged, blocked or escalated. A defensible review must therefore connect reservoir signals, downhole gauges, surface instrumentation, OT security evidence and response maturity.

2. Aim and Objectives of the Study

The aim of this review is to develop a cyber-resilience model for AI-based threat detection and response in remote wellhead, ESP and pipeline monitoring systems. The model is intended for high-availability oil and gas operations where production continuity, worker safety, environmental protection and equipment integrity must be maintained even when communications, telemetry or supervisory systems are under attack.

The objectives are sixfold. First, the review identifies the main cyber-physical assets and data streams that require protection, including sensors, controllers, RTUs, PLCs, ESP drives, VFDs, pipeline leak detection systems, historians, engineering workstations, wireless links, edge gateways, PDHMS, permanent downhole gauges and operations-centre applications. Second, it classifies attack patterns relevant to these assets, including false data injection, replay, unauthorised command execution, denial of service, credential abuse, malicious engineering changes, ransomware, sensor spoofing and alarm-threshold manipulation. Third, it synthesises AI techniques suitable for detecting these threats, with attention to time-series models, ensemble learning, process-aware residuals, graph analytics, hybrid rule-learning and explainable alerting. Fourth, it proposes a risk-prioritisation mechanism that weights detection outputs by asset criticality, safety impact, operational consequence, confidence and response urgency. Fifth, it outlines response playbooks that support containment, fail-safe operation, recovery and learning without creating unsafe automated reactions. Sixth, it clarifies how PDHMS, downhole gauges, ESP vibration monitoring and real-time field analytics strengthen reservoir surveillance, pump life-cycle improvement, predictive maintenance, reduced field visits and return on investment.

The review has a practical orientation. It does not claim that AI can remove uncertainty from remote operations. It argues that AI is valuable when it reduces the time between abnormal evidence and an appropriate response. The intended outcome is a model that helps OT engineers, production supervisors, security operations centre (SOC) analysts and safety teams share a common view of risk while keeping final high-impact actions under accountable human authority.

3. REVIEW METHODOLOGY

A structured narrative review approach was applied. The evidence base was limited to material published between 2020 and 2025, which is the period in which digital oilfield platforms, cloud-connected historians, AI-enabled monitoring and OT-specific security guidance matured rapidly. Four literature streams were considered. The first covered AI in oil and gas exploration, production forecasting, reservoir engineering and health, safety and environment analytics [1-28]. The second covered OT and ICS security guidance, including operational technology security guidance, industrial automation security standards, cybersecurity performance goals, adversary-behaviour knowledge bases and Saudi cybersecurity controls [2-6]. The third examined machine learning for intrusion detection and anomaly detection in ICS environments, including experimental limitations, context-aware modelling, digital twins and deployment risks [7-16]. The fourth focused on asset-specific petroleum monitoring, including ESP fault detection, pump vibration, downhole gauges, pipeline anomaly identification, field analytics and industry digitalisation examples [29-32].

Each source was coded against five operational questions. First, what asset or process does the source help protect: wellhead, ESP, pipeline, controller, network, historian, downhole gauge or integrated operations centre? Second, what data type is used: packets, logs, alarms, command histories, sensor time series, vibration, motor current, downhole pressure, downhole temperature, geospatial observations or engineering limits? Third, what algorithmic family is proposed: supervised classifier, anomaly detector, deep sequence model, digital twin, ensemble method, optimisation model or knowledge-based rule layer? Fourth, what weakness is reported: poor generalisation, limited labels, high false positives, weak explainability, limited real-time validation or poor connection to response? Fifth, how can the findings be translated into an operating model for remote oil and gas assets?

Quality was assessed through relevance, recency, technical specificity and operational applicability. Sources that linked AI to real process signals, threat detection, response or oil and gas use cases were prioritised. Conceptual material was used where it clarified governance, architecture or standards. A biomedical-style reporting framework was not used because the subject is an engineering and cyber-physical systems review. The synthesis produced two outputs: an integrated detection and response architecture, and a risk-prioritised operating workflow. These outputs are shown in Figures 1 and 2 and translated into Tables 1 and 2 for implementation planning. To strengthen the transparency of the review synthesis, Table 1 compares the main literature streams used in this study. The table shows how each stream contributes to AI-enabled cyber-physical resilience in remote oil and gas assets, while also identifying the limitations that justify the integrated model proposed in this review.

Table 1: Comparative literature synthesis for AI-enabled cyber-physical resilience in remote oil and gas assets

Literature stream	Representative sources	Main contribution	Common limitation	Relevance to this review
AI in oil and gas operations	[1-28]	Shows how AI supports exploration, reservoir characterisation, production forecasting, artificial lift and HSE analytics.	Often focuses on optimisation rather than adversarial manipulation or response governance.	Provides the process and production context needed to interpret cyber-physical anomalies.
OT/ICS security guidance and standards	[2-6]	Defines OT risk, segmentation, asset protection, security levels, critical-infrastructure controls and response expectations.	Usually remains high-level and does not provide asset-specific AI logic for wells, ESPs or pipelines.	Provides the governance and control boundaries within which AI detection must operate.
Machine learning for ICS anomaly detection	[7-16]	Demonstrates network and process anomaly detection using supervised, unsupervised, deep-learning and hybrid methods.	Laboratory performance may not generalise to noisy field telemetry, unseen attacks or changing operating modes.	Supports the layered analytics approach, while highlighting the need for validation and explainability.
ESP, pump and downhole	[29]	Shows the diagnostic value of vibration and	Usually treats faults as mechanical or	Supports integration of motor current,

Literature stream	Representative sources	Main contribution	Common limitation	Relevance to this review
monitoring literature		operating signals for identifying pump faults and degradation.	operational issues rather than possible cyber-physical manipulation.	vibration, VFD logs and downhole gauge evidence.
Digital oilfield and oil and gas cyber literature	[30-32]	Shows the operational importance of AI, smart fields, sensors, automation and large-scale field analytics.	Open publications often provide limited technical detail on data integrity and incident response.	Justifies treating real-time field analytics and cybersecurity analytics as one operating discipline.

4. Operational Context and Threat Surface

Remote wellheads, ESP systems and pipelines share a common digital pattern. Field devices produce high-frequency measurements, local controllers convert measurements into control action, communications infrastructure forwards evidence to supervisory platforms, and operators or automated logic initiate responses. Each asset class, however, has a distinct cyber-physical consequence profile. A wellhead automation package may include pressure and temperature transmitters, choke or valve actuation, shutdown inputs and remote command capability. A cyber incident can hide pressure excursions, spoof flow, alter command history or create unauthorised valve movement. Because wellheads are often dispersed, physical inspection can be slow. Detection must therefore emphasise command provenance, pressure-flow consistency, alarm integrity and unusual remote-access behaviour.

ESP systems add a more complex diagnostic challenge. Their performance is inferred through motor current, voltage, frequency, intake pressure, discharge pressure, bottom-hole pressure, downhole temperature, vibration, pump speed, VFD status and production response. Machine learning can support artificial-lift decisions and production forecasting [19-23], and pump-monitoring studies show that vibration and operational data can detect failure patterns in submerged pump equipment [29]. In cybersecurity terms, the same variables can be manipulated. An attacker may alter VFD settings, suppress overload alarms, imitate normal current traces or force repeated start-stop cycles that reduce equipment life. AI detection must therefore separate process faults from intentional manipulation. It should compare electrical, hydraulic, vibration and production evidence because genuine pump degradation has different cross-signal behaviour from a forged telemetry stream.

Pipeline monitoring expands the perimeter still further. Pipelines rely on pressure, flow, acoustic, temperature, valve-state, corrosion, inline inspection and sometimes satellite, drone or fibre-optic evidence. Cyber threat patterns include false leak suppression, false leak generation, communication jamming, manipulation of mass-balance calculations, unauthorised valve sequencing, ransomware affecting dispatch and compromise of engineering workstations used to modify leak detection parameters. Pipeline integrity decisions also involve environmental and public-safety consequences. Detection should therefore combine process-model residuals with network and geospatial evidence. A pressure drop that coincides with abnormal packet timing, disabled alarms and changed valve status should be ranked differently from a pressure fluctuation during scheduled maintenance.

Across all three asset classes, the attack surface is shaped by IT-OT convergence, vendor remote access, protocol legacy, harsh environments, intermittent communications and high availability requirements. OT guidance recommends compensating controls because many field devices cannot be patched or rebooted like enterprise assets [2]. Industrial security standards recommend zones and conduits because flat networks allow a compromise to move from a low-criticality host towards control systems [3]. Threat knowledge bases help map tactics such as initial access, lateral movement, command manipulation, impact and inhibition of response functions to specific detection logic [5]. These controls are not separate from AI. They provide the asset context and constraints that make AI outputs meaningful.

4.1 PDHMS, Downhole Gauges and Real-Time Field Analytics

Permanent Downhole Monitoring Systems (PDHMS), often implemented through permanent downhole gauges and associated surface electronics, are critical to modern reservoir and artificial-lift management. They should not be treated as a separate monitoring island. Bottom-hole pressure, downhole temperature, intake pressure, discharge pressure, motor current, oil temperature, vibration and surface production data are all part of the same real-time evidence chain. PDHMS gives operators continuous visibility into reservoir, wellbore and ESP

behaviour, enabling them to monitor reservoir performance and flood-front movement without relying only on costly and risky well interventions. This improves decision speed, reduces operational exposure and supports safer reservoir management [1].

Downhole gauges are typically designed for harsh, high-pressure and high-temperature environments. Vendor-specific ratings vary, but permanent gauges used in ESP and reservoir surveillance applications are commonly specified for severe operating envelopes, including pressures around 8,000 psi and temperatures around 350°F, or 177°C. Their value is not only that they record data. Their value is that they continuously track core parameters that can be compared with surface measurements. Intake and discharge pressure show the pressure of fluid entering and leaving the pump, helping prevent dry running, gas lock or overload. Motor current and oil temperature indicate the thermal and electrical condition of motor windings and oil, allowing the system to prevent thermal burnout. Vibration analysis, including three-axis vibration where available, can reveal mechanical imbalance, pump wear or poor alignment before catastrophic failure occurs. Leakage-current monitoring can also alert operators to insulation degradation or electrical shorts in the power cable or motor.

In many ESP installations, downhole sensors convert physical measurements into digital signals and transmit those signals to the surface through the ESP power cable or through dedicated telemetry paths. At the surface, the signal is decoded and fed into the surface controller, VFD, supervisory control and data acquisition (SCADA) system or historian. This arrangement makes PDHMS data operationally powerful, but it also makes data integrity essential. If bottom-hole pressure, downhole temperature, vibration or pump-performance data is manipulated, delayed or hidden, operators may make incorrect decisions about reservoir behaviour, pump health or pipeline safety. AI-based detection should therefore validate downhole and surface telemetry together, compare expected and observed pump behaviour, and flag inconsistencies that may indicate sensor spoofing, false data injection, unauthorised setpoint changes or communication interference [2-14].

The benefits of integrated PDHMS and real-time analytics are operational as well as defensive. Extended run-life is supported when abnormal vibration, overheating and dry-running conditions are detected early. Production optimisation is supported when engineers can match pump flow rates to changing reservoir conditions in real time. Troubleshooting improves because downhole gauges provide forensic evidence when a pump trips or when production suddenly changes. When historical and live field data are analysed together, AI systems can predict future challenges, reduce unnecessary field visits, improve energy use, accelerate maintenance decisions and support a more consistent production cycle. These benefits make cyber-resilience investment easier to justify because it protects safety while also improving uptime, productivity and return on investment.

4.2 Published Saudi Smart-Field Example

A published Saudi example illustrates why the proposed model must integrate PDHMS, surface sensors, automation and AI instead of treating them as isolated layers. Public Aramco material describes as one of its major intelligent oil fields, with large-scale use of sensors, smart wells, analytics and automation to monitor hundreds of wells and improve operational decisions [31, 32]. The same public descriptions associate digital solutions with increased production, improved troubleshooting response and safer maintenance practices. These claims should be presented as an industry example rather than as confidential project data unless the operator has formally approved the exact figures for publication.

For this review, the important lesson from such smart-field deployments is architectural. Large numbers of downhole and surface sensors do not automatically produce resilience. They produce resilience only when the data is trusted, correlated, prioritised and acted upon through clear operating playbooks. A field with thousands of sensors, ESPs, downhole gauges, fibre-optic pipeline monitoring and robotics still requires secure command paths, model validation, alarm integrity, asset criticality scoring and response governance. AI can forecast well behaviour and equipment problems, but it must also recognise when the evidence stream itself may be compromised. This is why the proposed model treats real-time field analytics and cybersecurity analytics as a single cyber-physical discipline.

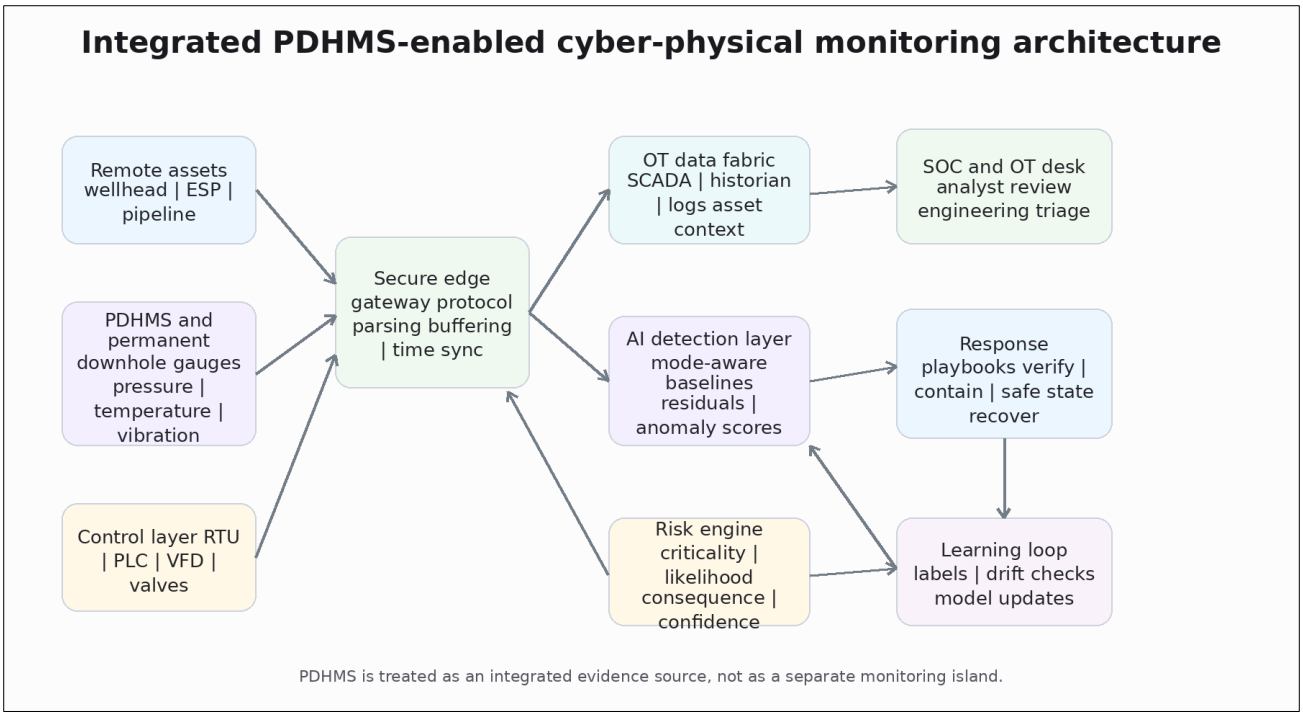

Figure 1: Integrated architecture for AI-based cyber-physical detection and response across remote wellhead, ESP, PDHMS and pipeline monitoring environments

Table 2: Integrated detection and response matrix for remote wellhead, ESP, PDHMS/downhole gauge and pipeline assets

Asset / evidence stream	Primary signals	Likely cyber or operational patterns	AI detection approach	Response priority
Remote wellhead	Pressure, flow, choke/valve state, shutdown status, command source	False pressure, unauthorised valve command, replay, alarm suppression	Pressure-flow residuals, command-provenance checks, mode-aware anomaly scoring	Block unverified commands; confirm field state; escalate if pressure limits are affected
ESP system with VFD	Motor current, voltage, frequency, vibration, intake/discharge pressure, temperature, VFD logs	VFD setpoint abuse, hidden overloads, forged normal current, repeated cycling	Cross-signal pump-performance models, LSTM/ensemble detection, drive-log correlation	Lock drive changes; restore approved setpoint; inspect if cyber and mechanical evidence align
PDHMS / downhole gauges	Bottom-hole pressure, downhole temperature, intake/discharge pressure, motor/oil temperature, vibration, leakage current	Sensor spoofing, delayed telemetry, false stability, dry running, gas lock, thermal stress	Downhole-surface consistency checks, pump curve residuals, vibration trend learning	Treat as critical evidence; verify sensor health; prioritise early pump protection
Pipeline monitoring	Flow balance, pressure waves, leak alarms, valve status, communication health, geospatial observations	Leak alarm manipulation, false data injection, ransomware, valve sequencing abuse	Mass-balance residuals, network-process fusion, geospatial correlation, confidence scoring	Verify leak logic; isolate affected segment only under approved safety criteria; preserve evidence

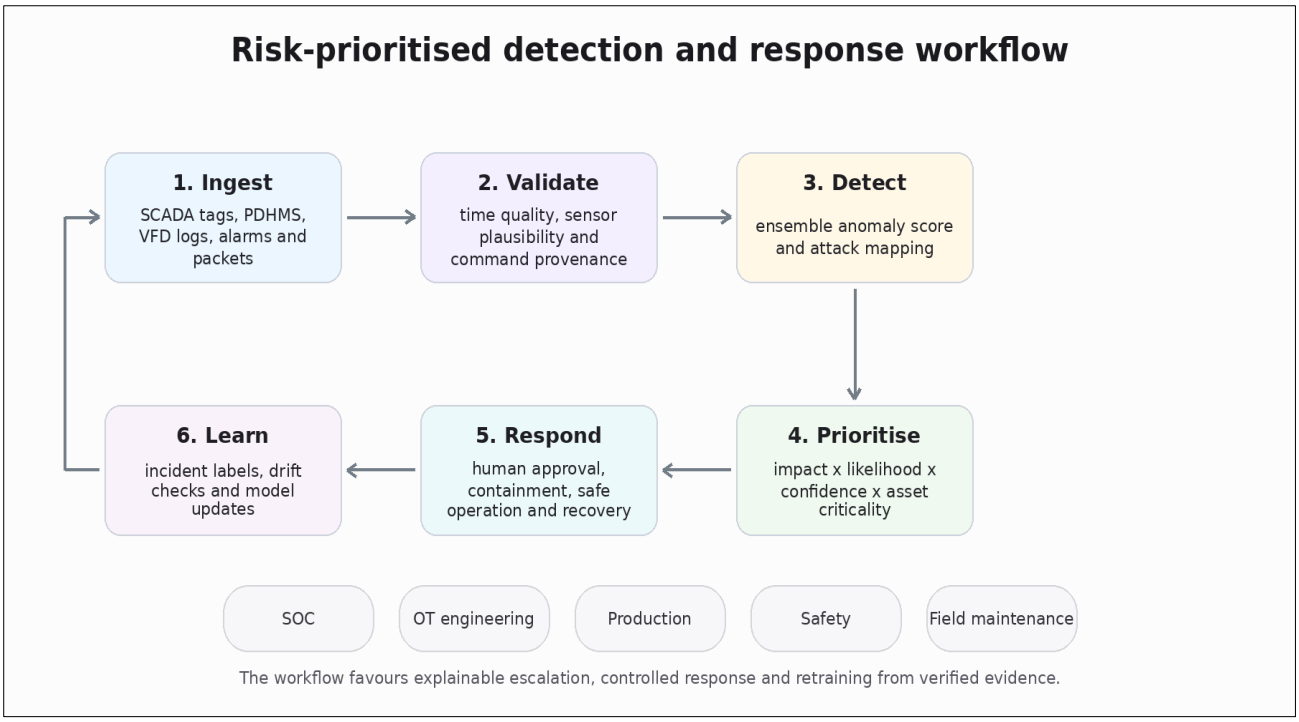

Figure 2: Risk-prioritised workflow linking telemetry validation, detection, consequence scoring, response playbooks and continuous learning

5. AI-Enabled Threat Detection Model

The proposed detection model uses layered analytics rather than a single algorithm. The first layer is data assurance. Before any model classifies behaviour, the system checks time synchronisation, missing values, sensor range, signal quality, duplicate packets, user identity, command path and maintenance state. This step is essential because remote oil and gas telemetry often contains gaps caused by power fluctuation, bandwidth limits or environmental conditions. If data quality is ignored, AI may learn communication noise as normal behaviour or treat legitimate production changes as attacks. Data assurance also detects primitive attack indicators such as replayed packets, repeated timestamps, impossible setpoint transitions and values outside known engineering limits.

The second layer is process-aware anomaly detection. Time-series models such as long short-term memory autoencoders, gated recurrent units and temporal convolutional networks can learn normal relationships among pressure, flow, pump current, vibration and command states. Deep-learning research in ICS environments shows that sequence models can detect stealthy anomalies when they process measured data and temporal dependencies [13]. However, evaluation studies warn that models trained on known attacks may fail against unknown attack types [9-11]. For that reason, process-aware detection should not depend only on attack labels. It should learn normal operating envelopes by mode: start-up, steady production, shut-in, maintenance, ramp-up, ESP frequency change, pigging, pressure testing and emergency shutdown. An anomaly score should be calculated relative to the active mode, not against a generic average.

The third layer is network and identity analytics. Remote operations depend on routers, firewalls, terminal servers, wireless links, jump hosts, vendor access platforms and authentication services. Machine-learning surveys in ICS networks show that intrusion detection can use packet flows, protocol fields, timing, command sequences and host logs [8-14]. For oil and gas operations, useful indicators include unexpected Modbus, DNP3 or OPC traffic, new communication pairs, unusual engineering workstation sessions, repeated failed logins, commands outside maintenance windows, changes to PLC logic and traffic bursts that degrade telemetry. Network analytics alone cannot prove a cyber-physical attack, but it can raise confidence when process anomalies appear at the same time.

The fourth layer is asset-specific modelling. For wellheads, the model evaluates pressure-flow-choke consistency, authorised command paths, alarm suppression and the expected pressure response after valve movement. For ESP systems, it evaluates current-frequency-pressure-vibration relationships, start-stop cycles, VFD parameter changes, thermal trends, pump-performance curves and PDHMS evidence. Where permanent downhole gauges are available, the model correlates downhole pressure,

downhole temperature and vibration behaviour with surface ESP signals to detect abnormal pump performance, sensor manipulation or false operational stability. For pipelines, the model evaluates flow balance, pressure wave behaviour, valve sequencing, leak alarms, communication integrity and geospatial indicators. Random forests and gradient boosting can rank features and support interpretable triage, while deep learning can capture nonlinear temporal behaviour. Hybrid architectures are preferable because each asset type has both physics-driven relationships and cyber observables.

The fifth layer is explainability and alert composition. An alert is useful only when it states why the condition matters. Instead of returning a generic anomaly score, the system should identify the affected asset, abnormal variables, baseline comparison, possible causes, supporting network evidence, safety implication and recommended verification steps. Deployment studies show that alert fatigue and uncertainty are major barriers to AI adoption in ICS environments [10-16]. A well-designed system should suppress weak alarms, combine related anomalies into incidents, and separate advisory, warning, critical and emergency conditions. Explainability also supports audit evidence because operators can show which signals, thresholds and model outputs justified a response.

Several algorithmic options are suitable. Isolation forests and one-class support vector machines are useful where attack labels are scarce. Random forests and gradient boosting work well when labelled maintenance, fault and incident histories are available. LSTM autoencoders and temporal models are effective for sequence behaviour. Graph models can represent relationships among users, assets, protocols and commands. Digital twins can estimate expected process response and expose residuals. Reinforcement learning should be treated cautiously in live control because unsafe exploration is unacceptable, but it may support offline optimisation of response recommendations. The strongest model is therefore an ensemble governed by engineering constraints, not a black-box algorithm with unrestricted authority.

6. Risk Prioritisation and Response Model

Detection without prioritisation creates noise. Remote oil and gas operators may receive thousands of alarms from process control, network monitoring, safety systems and maintenance applications. The proposed model ranks each AI alert using impact, likelihood, confidence and asset criticality. Impact measures the potential consequence for safety, environment, production and equipment. Likelihood measures the probability that the event represents cyber activity rather than process variation or equipment fault. Confidence measures evidence quality, including data completeness and agreement among models. Asset criticality measures the importance of the well, pump or pipeline segment. A low-confidence anomaly on a marginal well should not outrank a high-confidence command anomaly affecting a trunk pipeline valve or a high-rate ESP.

The response model is built around four levels. Level 1 is observe and verify. It applies when anomalies are weak, reversible or explainable by maintenance. Actions include checking sensor health, confirming work orders, reviewing access logs and asking the control room to validate recent commands. Level 2 is contain and monitor. It applies when cyber evidence is plausible but physical consequence is limited. Actions include disabling non-essential remote sessions, increasing logging, moving the asset into enhanced monitoring and requiring secondary approval for commands. Level 3 is protect and stabilise. It applies when a high-value asset shows command manipulation, telemetry conflict or coordinated cyber and process evidence. Actions include isolating affected conduits, freezing configuration changes, moving to manual or local control where safe, and preparing field verification. Level 4 is emergency response. It applies when safety, environmental or major production consequences are imminent. Actions include shutdown, fail-safe positioning, emergency communications and formal incident escalation.

Response must be safety-preserving. Automated isolation may stop an attacker, but it can also remove visibility from operators or interrupt control loops. Automated pump shutdown can protect equipment, but it may increase reservoir or wellbore risk if performed without engineering review. Automated valve closure can limit a spill, but it can create overpressure or hydraulic surge. For this reason, the model uses operator-approved playbooks. AI recommends; authorised personnel approve high-impact action unless pre-approved emergency criteria are met. Playbooks should specify who can approve, what evidence is required, which control room and field teams are notified, how logs are preserved and how service is restored.

For wellheads, a typical playbook begins with command verification. If an unauthorised choke movement appears, the system compares the command source with approved remote-access records, checks pressure response and blocks further remote commands pending control-room confirmation. For ESP systems, a typical playbook compares electrical, hydraulic and vibration evidence. If current and vibration suggest abnormal pump behaviour while VFD logs show unauthorised

frequency changes, the response may include locking the drive, returning to approved setpoints and scheduling field inspection. For pipelines, a typical playbook correlates pressure imbalance, leak alarms, valve status, communications health and geospatial observations. If cyber evidence indicates alarm suppression or parameter tampering, the response escalates to integrity and emergency teams before automated leak logic is trusted.

Post-incident learning is part of the response model. After an event is closed, analysts label whether it was cyber, mechanical, process, communications or procedural. The model then updates thresholds, adds features, improves correlation rules and records lessons for future cases. This feedback loop is essential because remote operations are not static. Wells decline, ESPs age, pipelines are modified, communications links change and adversaries adapt. Learning should be governed by model management controls: versioning, training-data review, validation on unseen data, rollback capability and periodic challenge testing. Machine-learning deployment studies in ICS caution that model drift, unseen attacks and unrealistic datasets can create misplaced confidence [10, 11]. Continuous assurance is therefore a resilience requirement, not a data-science preference.

Table 3: Five-level maturity model for AI-enabled threat response in remote oil and gas operations

Level	Detection maturity	Risk prioritisation	Response capability	Evidence required
1 Basic	Static rules and manual alarm review	Severity based on local judgement	Manual verification and ad hoc escalation	Alarm lists, access logs, maintenance records
2 Managed	Asset inventory, baseline tags and network alerts	Criticality and safety impact included	Defined runbooks for common anomalies	Asset map, approved command paths, response tickets
3 Integrated	Process and network anomaly fusion	Likelihood, consequence and confidence scored	SOC and OT joint triage with controlled containment	Model output, packet evidence, command provenance
4 Predictive	Mode-aware AI, residuals and drift monitoring	Dynamic risk linked to production and integrity state	Pre-approved safe actions with human confirmation	Validation history, change records, exercise results
5 Adaptive	Continuous learning, adversarial testing and digital-twin support	Portfolio risk view across wells, pumps and pipelines	Measured recovery, automated evidence preservation and improvement loop	Model versions, incident lessons, recovery metrics

7. Governance, Compliance and Implementation Considerations

AI-enabled detection must align with governance. In Saudi and Gulf oil and gas environments, national and sectoral cybersecurity requirements emphasise governance, risk management, asset protection, continuous monitoring, incident response and OT controls. The Saudi National Cybersecurity Authority describes cybersecurity as a national reference function intended to safeguard critical infrastructure, vital interests and priority sectors [6]. For operators, this means that AI models should produce evidence that supports audits and decision accountability. Model outputs must be linked to asset inventory, risk acceptance, incident tickets, change records, training, vendor access approvals and recovery tests.

Implementation should begin with asset visibility. Many remote operations contain legacy controllers, field modems, protocol converters, contractor laptops and undocumented links. AI cannot protect assets it cannot see. The first step is a living inventory of wellhead controllers, ESP drives, VFDs, pipeline RTUs, communications paths, firmware versions, protocols, data owners and safety dependencies. The second step is network segmentation. Zones should separate safety systems, control systems, field telemetry, vendor access, historians, enterprise analytics and cloud services. The third step is data engineering. Tags must be normalised, timestamped, quality-coded and mapped to assets. Without this foundation, advanced models will amplify bad data rather than create insight.

The fourth step is model selection and validation. Operators should avoid deploying the most complex model first. A practical path starts with baseline rules and feature engineering, then adds anomaly models, and later adds deep sequence models where data volume and stability justify them. Each model should be tested against normal mode changes, maintenance periods, communication loss, sensor drift, simulated false data injection and historical faults. Performance metrics must include false positives, false negatives, detection delay, explainability, operator workload and response usefulness. Accuracy alone is insufficient because a

rare but high-consequence pipeline incident cannot be evaluated like a balanced laboratory classification problem.

The fifth step is integration with SOC and OT operations. A cyber alert about an ESP is not useful if analysts do not understand pump curves, and a production alarm is not useful if engineers do not see remote-access evidence. Cross-functional runbooks should define when the SOC contacts the control room, when production engineering joins triage and when field teams are dispatched. Training should use realistic scenarios, including spoofed wellhead pressure, malicious ESP frequency change, ransomware affecting historian access, false pipeline leak and suppression of leak alarms. These exercises build trust and expose gaps before a real event occurs.

8. DISCUSSION

The review indicates that AI can improve cyber resilience only when detection, prioritisation and response are designed together. In remote oil and gas assets, a technically accurate anomaly may still be operationally useless if it lacks context, arrives too late or proposes an unsafe action. Conversely, a simple rule can be valuable when it captures a safety-critical invariant such as impossible valve movement, unauthorised setpoint change or inconsistent pressure-flow response. The best architecture is therefore layered, modest and evidence-driven. It should combine deterministic checks, engineering models, machine learning and analyst feedback.

A recurring challenge is the boundary between cyberattack, equipment failure and process upset. ESP current anomalies may reflect gas interference, scaling, bearing wear, power-quality disturbance or malicious VFD manipulation. Vibration may indicate mechanical imbalance, poor alignment, worn impellers or forged stability if the telemetry stream is compromised. Pipeline pressure anomalies may reflect leak, pigging, compressor changes, sensor failure or command spoofing. Wellhead pressure changes may reflect reservoir behaviour, sand production, hydrate risk, choke adjustment or malicious command action. AI should not force these possibilities into a binary decision. It should calculate competing explanations and show the evidence for each. This supports better response because containment differs across root causes.

Another challenge is adversarial adaptation. Once attackers understand that a detector watches certain tags, they may manipulate correlated signals together, delay telemetry, poison training data or mimic normal distributions. This risk reinforces the need for independent evidence sources, secure logging, model-change control and adversarial testing. The future direction is not simply deeper models. It is safer models: models that recognise uncertainty, ask for verification, provide root-cause clues and degrade gracefully when data quality falls.

The candidate comments on PDHMS and ESP vibration highlight an important publication issue. A paper on remote wellhead, ESP and pipeline monitoring should not mention downhole monitoring only as a side feature. It should explain how downhole gauges, surface sensors, VFD logs and real-time analytics form a single diagnostic chain. Bottom-hole pressure and temperature explain reservoir and wellbore conditions. Intake and discharge pressure explain pump loading. Motor current and oil temperature explain electrical and thermal stress. Vibration explains mechanical stability and early degradation. When these signals are correlated, AI can detect pump failure earlier, reduce unplanned downtime, improve field-visit planning and support uninterrupted production. When those signals are inconsistent with command logs or network evidence, the same analytics can support cyber-physical threat detection.

Implementation should begin with a narrow pilot rather than an enterprise-wide deployment. A single pipeline segment, a cluster of high-rate ESP wells or a set of remote wellheads can provide enough telemetry to test data quality, model behaviour and operator workflow. Pilot scope should include historical faults, planned maintenance, communication outages and realistic cyber scenarios so that the team can measure detection delay and response usefulness. The learning from that pilot should inform tag standards, data retention, sensor hardening, model thresholds and playbook wording. This staged route reduces organisational resistance and avoids the common mistake of presenting AI as a finished product rather than a governed operational capability.

Procurement is also part of resilience. New controllers, drives, gateways, historians and analytics platforms should be evaluated for logging, secure remote access, role separation, time synchronisation, backup, configuration export and integration with monitoring platforms. If these capabilities are absent, the AI layer will infer risk from incomplete evidence. Procurement should treat observability as a security requirement, not a luxury feature. Vendors should provide data dictionaries, event formats, patch processes and safe recovery procedures. These requirements are especially important for ESP drives, downhole gauges and pipeline controllers that may remain in service for many years.

9. CONCLUSION

This review developed an AI-based threat detection and response model for remote wellhead, ESP and pipeline monitoring systems. The study shows that cyber resilience in oil and gas depends on linking process evidence, network evidence, asset criticality and response playbooks. AI is most valuable when it detects abnormal cyber-physical relationships that conventional tools overlook, including forged telemetry, suspicious command timing, manipulated pump settings, unsafe valve sequencing or pipeline pressure behaviour inconsistent with valve and flow evidence. Yet AI must remain governed by engineering constraints, explainability and human-approved response.

The revised model strengthens the earlier draft by integrating PDHMS, permanent downhole gauges, ESP vibration monitoring and real-time field analytics as core evidence sources rather than separate additions. Bottom-hole pressure, downhole temperature, intake and discharge pressure, motor current, oil temperature, vibration and VFD logs provide a rich picture of reservoir behaviour, pump health and operational continuity. Their integration enables predictive maintenance, reduced field visits, extended ESP run-life, faster troubleshooting and stronger return on investment. From a cyber-resilience perspective, these signals also help detect false data injection, sensor spoofing, unauthorised setpoint changes and communication interference.

The proposed architecture integrates data assurance, process-aware models, network analytics, asset-specific logic, risk scoring, playbooks and post-incident learning. Its main contribution is the shift from alert generation to risk-prioritised action. Future work should validate the model on real oilfield data, include adversarial testing, develop shared evaluation datasets and measure response outcomes rather than detection accuracy alone. For remote oil and gas operations, resilience is achieved when intelligence improves safety, continuity and trust at the same time.

REFERENCES

1. Chen, F.; Sun, L.; Jiang, B.; Huo, X.; Pan, X.; Feng, C.; Zhang, Z. A Review of AI Applications in Unconventional Oil and Gas Exploration and Development. Energies 2025, 18, 391.
2. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. Guide to Operational Technology Security, NIST Special Publication 800-82 Revision 3. 2023.
3. International Electrotechnical Commission. IEC 62443-3-2: Security for Industrial Automation and Control Systems - Security Risk Assessment for System Design. 2020.
4. Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals. 2023.
5. MITRE. ATT&CK for Industrial Control Systems Knowledge Base. 2024.
6. National Cybersecurity Authority. Essential Cybersecurity Controls, ECC-2:2024. 2024.
7. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for Industrial Control Systems: A Survey. Computers & Security 2020, 89, 101677.
8. Umer, M.A.; Junejo, K.N.; Jilani, M.T.; Mathur, A.P. Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations. International Journal of Critical Infrastructure Protection 2022, 38, 100516.
9. Raman, M.R.G.; Ahmed, C.M.; Mathur, A. Machine Learning for Intrusion Detection in Industrial Control Systems: Challenges and Lessons from Experimental Evaluation. Cybersecurity 2021, 4, 27.
10. Ahmed, C.M.; Palleti, V.R.; Mathur, A.P. Challenges in Machine Learning Based Approaches for Real-Time Anomaly Detection in Industrial Control Systems. CPSS 2020, 297-304.
11. Kus, D.; Wagner, E.; Pennekamp, J.; Wolsing, K.; Fink, I.B.; Dahlmanns, M.; Wehrle, K.; Henze, M. A False Sense of Security? Revisiting the State of Machine Learning-Based Industrial Intrusion Detection. 2022.
12. Muller, N.; Ziras, C.; Heussen, K. Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems. 2022.
13. Zhao, X.; Wang, J.; Jiang, C.; Li, Y. Anomaly Detection Approach in Industrial Control Systems Using Deep Learning. Information 2022, 13, 450.
14. Pinto, A.; Costa, J.; Santos, H.; Sousa, T. Survey on Intrusion Detection Systems Based on Machine Learning for Critical Infrastructures. Sensors 2023, 23, 2415.
15. Abraham, D.; Erceylan, G.; Gkioulos, V.; Houmb, S.H. Towards Enhanced Cybersecurity in Industrial Control Systems: A Review of Context-Based Modelling, Digital Twins and Machine Learning. International Journal of Information Security 2025.
16. Seo, J.K.; Kim, S.; Park, J.; Lee, H. AI-Based Anomaly Detection in Industrial Control and Cyber-Physical Systems. Electronics 2025, 15, 20.
17. Wang, S.; Sharma, M.M. Random Forest-Based Reservoir Characterisation and Oil Saturation Prediction from Production Data. 2021.
18. Liu, Y.; Zhang, H.; Wang, Z. Extreme Learning Machine for Multivariate Reservoir Property Characterisation in Tight Sandstone Gas Reservoirs. 2021.

19. Alarifi, S.; Miskimins, J. Hybrid LSTM-SVR Models for Production Forecasting in Unconventional Reservoirs. 2021.
20. Qiu, H.; Li, X. Bayesian-Optimised LSTM for Daily Production Forecasting in Tight Gas Reservoirs. 2022.
21. Zhou, X.; Guo, C. CNN-BiGRU Attention Model for Shale Oil Production Forecasting. 2023.
22. Li, Y.; Ma, X.; Zhang, K. Permeability Prediction in Nanoporous Shale Using Discrete Cosine Transform and Artificial Neural Networks. 2023.
23. Fang, J.; Carcione, J.M. Deep Neural Network Prediction of Permeability in Tight Oil and Gas Reservoirs. 2024.
24. Tavakolian, M.; Soroush, M.; Khosravi, A. Machine Learning Prediction of Methane and Carbon Dioxide Adsorption in Unconventional Reservoirs. 2024.
25. Wen, T.; Niu, X.; Jackson, R.B. Logistic Regression for Detecting Groundwater Methane Anomalies Near Oil and Gas Development. 2021.
26. Kong, B.; Chen, Z. XGBoost and Linear Regression Stacked Models for Cumulative Production Forecasting in Shale Reservoirs. 2021.
27. Yang, Y.; Liu, S.; Hu, J. Self-Attention Convolutional Neural Network with Transfer Learning for Gas Probability Prediction in Tight Sandstone Reservoirs. 2024.
28. Nath, S.; Asish, S.M. Bi-LSTM and Random Forest Models for Geomechanical Parameter Prediction from Well-Logging Data. 2022.
29. Wankhede, S.P.; Xie, X.; Alshehri, A.H.; Brashler, K.W.; Baadani, M.; Turcan, D.C.; Youcef-Toumi, K.; Du, X. In-Situ Fault Detection of Submerged Pump Impellers Using Encapsulated Accelerometers and Machine Learning. 2025.
30. Jha, R.; Alharthi, A.; Khan, M. Securing the Future: AI-Driven Cybersecurity Solutions for the Oil and Gas Industry. SPE Gulf of Mexico Technical Symposium 2025, SPE-224469-MS.
31. Saudi Aramco. AI and Big Data - Oil & Gas Industry. 2024. Available online: Aramco digitalisation and AI resources.
32. Aramco Life. Intelligent Khurais. 2020. Available online: Aramco Life, The Arabian Sun archive.