

International Journal Research Publication Analysis

Page: 01-35

DECEIVING THE DIGITAL TWIN: ADVERSARIAL ROBUSTNESS OF PREDICTIVE-MAINTENANCE MODELS IN INDUSTRIAL CYBER-PHYSICAL SYSTEMS

Kelly Okogbenin*, Tedun Awi Daniel

Independent Researcher.

Article Received: 18 August 2026

*Corresponding Author: Kelly Okogbenin

Article Revised: 06 September 2026

Independent Researcher.

Published on: 26 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.5213>

ABSTRACT

This review examines the adversarial robustness of predictive-maintenance models operating within digital-twin-enabled industrial cyber-physical systems, with particular emphasis on how malicious manipulation can compromise maintenance intelligence and physical reliability. A structured review methodology was applied, combining systematic literature searching, predefined eligibility criteria, evidence classification, and thematic analysis across digital-twin architecture, predictive modelling, cyber-physical security, adversarial machine learning, robustness evaluation, and governance. The synthesis shows that digital twins create substantial operational value through continuous sensing, state estimation, fault diagnosis, prognosis, and maintenance optimization, yet their dependence on interconnected data pipelines also expands the attack surface. Particular attention is given to the distinction between legitimate equipment degradation, benign distribution shift, and deliberately engineered perturbations capable of deceiving virtual representations. Evasion attacks, sensor manipulation, training-data poisoning, model extraction, and integrity compromise can distort anomaly detection, remaining-useful-life estimation, and maintenance prioritization while preserving superficially plausible system behaviour. The review further finds that adversarial training, robust learning, secure data exchange, runtime monitoring, multimodal validation, continual adaptation, and access-control mechanisms can improve resilience, although current evidence remains limited by inconsistent benchmarks, weak reproducibility, insufficiently realistic attack models, and inadequate consideration of downstream operational consequences. The study concludes that robustness should be treated as a lifecycle property spanning data acquisition, model development, deployment, updating, and

governance rather than as an isolated algorithmic characteristic. It recommends standardized industrial adversarial benchmarks, physically constrained attack testing, transparent reporting protocols, continual-learning defenses, explainable assurance mechanisms, stronger provenance controls, independent validation, and post-deployment monitoring. Integrating these measures with engineering reliability, cybersecurity standards, and regulatory accountability is essential for sustaining trustworthy maintenance decisions in evolving industrial environments.

KEYWORDS: Digital twins; predictive maintenance; adversarial machine learning; industrial cyber-physical systems; adversarial robustness; cybersecurity.

1. INTRODUCTION

1.1 Digital Transformation of Industrial Maintenance

Industrial maintenance has evolved from a reactive support function into a digitally enabled capability integrated with production strategy and asset management. Maintenance philosophies relied on repairing equipment after failure or servicing assets at predetermined intervals. Digital transformation changes this logic by using connected sensing, analytics and real-time support to infer equipment condition before failure. In the Nigerian mechanical-systems context, the transition toward predictive maintenance has been associated with intelligent monitoring, data analytics and organisational adaptation, demonstrating that maintenance modernisation is simultaneously technological and managerial rather than merely an equipment upgrade (Sunday et al., 2020).

Industry 4.0 provides the technological architecture for this transition. Cyber-physical systems connect shop-floor assets with computational environments in which operating states can be monitored, interpreted and acted upon. The resulting architecture links machine-level sensing, data conversion, representations, cognition and configuration, allowing maintenance information to move from isolated inspection records toward updated digital knowledge. This integration alters maintenance visibility because deviations in vibration, temperature, load, pressure or energy consumption can be evaluated with historical operating behaviour and system dependencies (Lee, Bagheri & Kao, 2015).

The digital twin extends cyber-physical integration by maintaining a virtual representation linked through information exchange with its physical counterpart. Distinguishing digital models, digital shadows and fully integrated twins is important for maintenance because predictive decisions require more than static simulation. A maintenance-oriented twin must

assimilate asset data and represent condition, degradation and operating context. Digital transformation therefore shifts maintenance from periodic observation toward persistent virtual–physical synchronization, creating the informational foundation for prognosis, scenario testing and intervention planning (Kritzinger et al., 2018).

Machine learning further transforms maintenance by extracting failure-related structure from industrial data. Classification, regression, and other learning approaches allow organisations to identify abnormal behaviour, estimate equipment health and support remaining-useful-life decisions where fixed schedules may be inefficient. Their value, however, depends on suitable data, feature representation, model selection and evaluation. Machine-learning-based predictive maintenance consequently represents a transition from deterministic maintenance rules toward probabilistic and data-dependent judgments, making model quality and information integrity consequential to operational reliability (Carvalho et al., 2019).

Maintenance 4.0 also changes how maintenance work is organised. Industrial Internet of Things platforms, cloud services, mobile devices, augmented reality and advanced analytics enable remote diagnosis, condition-based intervention and autonomous maintenance functions. Effective transformation requires integration across technologies, work processes and human decision-making rather than digitising isolated tasks. This perspective remains crucial because maintenance personnel must interpret alerts, validate abnormal conditions and convert algorithmic outputs into safe physical interventions (Silvestri et al., 2020).

Predictive maintenance consequently becomes a central Industry 4.0 application because it connects high-frequency asset data with decisions intended to reduce unplanned downtime, unnecessary intervention and disruption. Research spans monitoring architectures, data processing and prediction methods, reflecting the multidisciplinary nature of maintenance intelligence. The transformation is therefore not simply a progression from preventive to predictive scheduling; it restructures maintenance around continuous information flows and anticipatory decision-making across interconnected production assets (Zonta et al., 2020).

Operational excellence remains a constraint on this transformation. Integrating reliability-centred maintenance with process-improvement disciplines illustrates how digital intelligence should support asset criticality, process stability, lifecycle economics and measurable manufacturing performance. In Nigeria, a Lean Six Sigma and reliability-centred maintenance perspective identifies predictive analytics and enterprise-level digital convergence as enablers of coordinated reliability governance. This integration matters, as organisations must justify digital investments through improved availability and better

allocation of maintenance resources rather than through technology adoption alone (Olutimehin& Ganiu, 2022).

Implementation remains uneven across industrial contexts. Evidence from the South African railway industry shows that data-driven and machine-learning-based predictive maintenance requires more than technical feasibility; adoption is shaped by infrastructure, organisational readiness, skills and socioeconomic conditions. These constraints matter for industrial cyber-physical systems because digital maintenance increases dependence on sensors, networks, models and synchronized data pathways. As maintenance decisions become mediated by digital representations, reliability becomes inseparable from the trustworthiness of information feeding those representations, creating the foundation for examining how manipulated inputs or compromised predictive models could deceive a digital twin and distort maintenance decisions (Nethamba& Grobbelaar, 2023).

1.2 Emerging Adversarial Risks in Digital Twins

Digital twins critically mediate between industrial assets and predictive-maintenance models used to interpret condition. Their value depends on exchange among sensors, communication networks, control devices, models, and virtual representations. This connectivity creates adversarial pathways through which manipulated telemetry, compromised edge devices or falsified control messages can corrupt the twin's representation of physical reality. Research on digital substations shows that IoT-enabled protection improves responsiveness but introduces cyber-physical dependencies whose compromise can undermine operational resilience (Shittu, Shittu & Olagunju, 2024).

The risk is intensified because maintenance-oriented twins aggregate data streams differing in provenance, latency, quality and trustworthiness. South African railway digital-twin implementations demonstrate integrating diverse data sources across changing infrastructure and user requirements. In an adversarial setting, these integration points may become trust boundaries: malicious alterations in one source can propagate into the virtual model and influence diagnosis, maintenance prioritisation or intervention timing (Doubell et al., 2024).

For industrial cyber-physical systems, adversarial exposure also extends to the learning and detection mechanisms that distinguish legitimate behaviour from malicious activity. Nigerian research on intrusion detection demonstrates the growing reliance on deep learning to identify network attacks within interconnected CPS environments. Where attackers deliberately shape inputs to evade detection or corrupt learned representations, apparently normal data can conceal hostile behaviour, allowing compromised information to reach maintenance analytics and undermine confidence in automated decisions (Ibor et al., 2025).

Digital twins can simultaneously function as targets and defensive instruments. Attack simulation within a twin environment can support threat assessment without disrupting the physical system; however, the integrity of the twin and its analytical components must be protected. Explainable security architectures illustrate how attack vectors can be evaluated and interpreted, highlighting the need to distinguish genuine equipment degradation from maliciously induced anomalies in cyber-physical environments (Suhail et al., 2023).

The concern intensifies when predictive maintenance depends on machine-learning models. Carefully constructed perturbations can alter model outputs while remaining difficult for operators to detect. Experimental work on digital twins shows that adversarial inputs can degrade model performance and that combining preprocessing defenses with adversarial training can improve robustness. For industrial predictive maintenance, analogous manipulation could generate false alarms, suppress genuine failure indicators, distort remaining-useful-life estimates, or trigger inappropriate maintenance actions, converting model vulnerability into operational and safety risk (Shamshiri, Liu & Sohn, 2025).

1.3 Review Objectives, Scope, and Contributions

This review critically examines the adversarial robustness of predictive-maintenance models operating within digital-twin-enabled industrial cyber-physical systems. Jointly led from complementary industrial and computational perspectives, the review seeks to determine how deliberate manipulation of data, model inputs, learning processes, and communication pathways can compromise maintenance intelligence and subsequently affect physical asset reliability. Particular attention is directed toward vulnerabilities capable of distorting fault detection, condition assessment, remaining-useful-life estimation, anomaly recognition, and maintenance prioritization.

The review encompasses digital-twin architectures, predictive-maintenance pipelines, cyber-physical attack surfaces, adversarial threat mechanisms, model vulnerabilities, defensive architectures, runtime monitoring, recovery strategies, robustness evaluation, and practical deployment constraints. Its analytical scope extends beyond algorithmic accuracy to consider how compromised predictions may propagate into equipment availability, process continuity, operational safety, resource allocation, and infrastructure resilience.

A principal contribution of the review is the development of an integrated analytical perspective connecting adversarial entry points with affected data pathways, predictive functions, physical consequences, detection opportunities, and corresponding defensive strategies. By bridging predictive-maintenance engineering, digital-twin technology, adversarial machine learning, and cyber-physical security, the study addresses disciplinary

fragmentation within the existing literature. It further identifies deficiencies in current robustness benchmarks, highlights unresolved challenges surrounding adaptive attacks and real-time assurance, and establishes research priorities for trustworthy industrial deployment. Collectively, these contributions provide a structured foundation for designing predictive-maintenance ecosystems capable of sustaining dependable decision-making under evolving adversarial conditions.

2. Review Methodology and Evidence Synthesis

2.1 Literature Search and Database Strategy

The literature search was designed to identify peer-reviewed evidence addressing adversarial robustness, predictive maintenance, digital twins, and industrial cyber-physical systems through a transparent, systematic, and reproducible retrieval process. The protocol was established before formal screening and defined the review question, conceptual domains, bibliographic databases, search terminology, temporal boundaries, eligibility parameters, and record-management procedures. The search process was structured to permit clear documentation of study identification, duplicate removal, screening, eligibility assessment, and final inclusion, thereby creating an auditable methodological pathway rather than relying on retrospectively reconstructed search decisions.

Database selection reflected the interdisciplinary nature of the research problem. Scopus and Web of Science were employed to provide broad multidisciplinary coverage, while IEEE Xplore and the ACM Digital Library were used to capture literature in engineering, computer science, cybersecurity, machine learning, and industrial informatics. ScienceDirect and SpringerLink complemented these sources by strengthening coverage of predictive maintenance, reliability engineering, automation, digital-twin development, and cyber-physical systems. Employing multiple databases reduced the risk of disciplinary bias because no single indexing platform provides complete coverage of the diverse technical fields relevant to adversarially robust maintenance intelligence.

Search queries were organized around four principal concept blocks: digital twins, predictive maintenance, adversarial machine learning, and industrial cyber-physical systems. Representative terms included “digital twin*”, “predictive maintenance”, “condition monitoring”, “remaining useful life”, “industrial cyber-physical system*”, “industrial IoT”, “adversarial attack*”, “evasion attack*”, “data poisoning”, “sensor spoofing”, “model extraction”, “adversarial training”, and “robustness”. Boolean operators were used to

combine related concepts, while quotation marks, truncation symbols, field restrictions, and database-specific syntax were adapted according to the functionality of each search platform. The principal search window covered January 2015 through December 2025. This period was selected to capture the rapid development and convergence of industrial digital twins, data-driven maintenance, machine-learning-based prognosis, and adversarial artificial-intelligence research. Searches focused primarily on English-language, peer-reviewed journal articles and full conference papers. High-quality review studies were also retained where they contributed relevant taxonomies, conceptual frameworks, methodological approaches, or consolidated evidence. For transparency, the search process documented database names, execution dates, complete search strings, applied filters, and the number of records retrieved from each source. Search sensitivity was strengthened through iterative query refinement. Preliminary searches were first conducted to identify terminology used across engineering, cybersecurity, artificial intelligence, and maintenance research communities. Synonyms, alternative spellings, and closely related technical expressions were subsequently incorporated where they improved retrieval without expanding the review beyond its defined scope. This process was particularly important because similar concepts may be described differently across industrial engineering, computer science, reliability analysis, and cyber-security literature. Search-term refinement therefore proceeded as a controlled methodological activity rather than as an unrestricted expansion of the evidence base.

Google Scholar was used as a supplementary discovery and citation-tracing resource rather than as the primary systematic search platform. Its broad disciplinary coverage was valuable for locating potentially relevant studies not retrieved through structured bibliographic databases. However, because result ranking, indexing coverage, and retrieval reproducibility can vary considerably, it was not relied upon as the sole source of evidence. Backward reference searching and forward citation tracking were used selectively to identify additional studies connected to highly relevant publications while preserving the primacy of reproducible database searches.

All retrieved records were exported into a centralized reference-management environment containing bibliographic metadata such as titles, abstracts, keywords, authors, publication years, journal or conference sources, and digital object identifiers where available. Records from different databases were combined into a master library. Duplicates were identified through DOI matching, title comparison, author names, and publication-year verification, followed by manual inspection where automated matching produced uncertainty. A detailed search log distinguished records obtained directly from databases from those identified

through citation chaining, thereby maintaining traceability throughout the evidence-selection process.

The overall strategy was designed to balance comprehensiveness with methodological control. Particular attention was given to avoiding disciplinary blind spots because relevant evidence is distributed across machine learning, industrial control, predictive maintenance, digital-twin engineering, cybersecurity, and reliability research. Database diversification, structured search strings, iterative refinement, citation tracking, and transparent record management were therefore treated as complementary components of a unified retrieval strategy. This approach ensured that the subsequent screening and synthesis stages were founded on a broad yet clearly bounded body of literature capable of supporting rigorous analysis of adversarial threats, robustness mechanisms, and predictive-maintenance decision reliability within industrial digital-twin environments.

2.2 Study Selection and Eligibility Criteria

Study selection was governed by pre-specified eligibility criteria designed to preserve conceptual relevance, methodological transparency, and comparability across literature concerning digital twins, predictive maintenance, adversarial machine learning, and industrial cyber-physical systems. Following deduplication, titles and abstracts were screened against the review objectives before potentially relevant records proceeded to full-text assessment. Eligibility decisions were based on predefined and consistently applied rules that distinguished studies directly addressing the research problem from tangential or insufficiently relevant material. This approach reduced the likelihood of subjective inclusion decisions and strengthened the transparency of the evidence-selection process.

Studies were included when they examined industrial digital twins, predictive or condition-based maintenance, machine-learning-enabled fault diagnosis, adversarial attacks, cyber-physical security, model robustness, defensive mechanisms, or closely related assurance problems. Eligible publications consisted primarily of peer-reviewed journal articles and full conference papers published between 2015 and 2025. To qualify for inclusion, studies were required to provide sufficient methodological, technical, or empirical detail to support meaningful synthesis. Review articles were retained when they contributed relevant taxonomies, conceptual frameworks, benchmark evidence, comparative analyses, or consolidated findings capable of informing the review questions.

Records were excluded when they addressed digital twins solely as visualization or simulation tools without relevance to predictive maintenance, cybersecurity, or model robustness. Studies focusing on maintenance without data-driven prediction were also

excluded, as were cybersecurity papers lacking relevance to cyber-physical or learning-enabled systems. Similarly, machine-learning studies were excluded when they offered no meaningful connection to industrial maintenance, adversarial robustness, fault detection, prognosis, or digital-twin operation. Editorials, extended abstracts, presentation materials, inaccessible full texts, duplicate records, non-scholarly commentary, and publications lacking sufficient analytical or methodological substance were also removed from consideration.

Screening followed a staged procedure. During the first stage, titles and abstracts were assessed for broad relevance to the defined research scope. Records retained at this stage underwent full-text examination, during which greater attention was given to system context, predictive-maintenance function, attack or failure mechanism, analytical method, robustness strategy, and reported outcomes. This progressive narrowing process ensured that studies were not excluded prematurely while still maintaining a focused and technically coherent final evidence base.

Particular consideration was given to interdisciplinary studies positioned at the boundaries of industrial engineering, artificial intelligence, cybersecurity, and reliability analysis. Borderline records were evaluated according to whether their methods, findings, or frameworks could materially inform the understanding of adversarial vulnerabilities or robustness within maintenance-oriented digital twins. Studies were not retained merely because they contained related terminology; substantive relevance to the analytical objectives was required.

All exclusions made during full-text assessment were documented with explicit reasons. Where eligibility was uncertain, decisions were resolved through discussion between the lead and joint author rather than through unilateral judgment. This collaborative process strengthened consistency across complex cases involving ambiguous industrial relevance, indirect adversarial implications, or partially aligned predictive-maintenance applications. The resulting audit trail provided a transparent account of how the initial search corpus was progressively refined into a focused body of evidence suitable for defensible synthesis and comparative analysis.

2.3 Evidence Classification and Analytical Framework

Evidence synthesis was organized through a structured analytical framework designed to compare heterogeneous studies without obscuring important distinctions among digital-twin architectures, predictive-maintenance models, adversarial mechanisms, and industrial operating contexts. Each eligible study was coded across five principal dimensions: system layer, analytical function, adversarial condition, operational consequence, and defensive

response. This multidimensional approach enabled the evidence to be examined simultaneously from computational, operational, and cyber-physical perspectives rather than being grouped solely by publication theme or disciplinary origin.

The system-layer dimension differentiated physical assets, sensors and actuators, communication infrastructure, edge and cloud environments, digital-twin models, predictive algorithms, and decision-support interfaces. This separation was essential because adversarial manipulation may originate within one component of the architecture while producing consequences across several interconnected layers. Classifying studies according to the location of compromise made it possible to trace how malicious inputs, corrupted communication, compromised models, or unauthorized access could propagate through the digital-twin ecosystem and ultimately influence maintenance decisions.

The analytical-function dimension categorized studies according to monitoring, anomaly detection, fault diagnosis, prognosis, remaining-useful-life estimation, optimization, and maintenance scheduling. This classification enabled the review to distinguish vulnerabilities according to the specific predictive or decision-making function affected. Evidence was subsequently mapped against adversarial characteristics, including attacker knowledge, capabilities, objectives, access level, attack strategy, and point of intervention. This approach supported systematic comparison of threats targeting training data, model parameters, sensor inputs, communication pathways, inference processes, and decision outputs.

Digital-twin studies were further classified according to data integration, model fidelity, predictive capability, real-time synchronization, simulation, adaptive behavior, and decision-support functionality. These dimensions were retained because digital twins differ substantially in architectural maturity and operational purpose. A static simulation model, for example, does not present the same adversarial exposure as a continuously synchronized twin connected to live sensors and automated maintenance systems. Capturing these contextual distinctions prevented inappropriate comparison of systems with fundamentally different cyber-physical dependencies.

Evidence relating to industrial artificial intelligence was additionally classified according to deployment architecture, performance objectives, scalability, interoperability, safety requirements, explainability, and algorithmic reliability. This ensured that adversarial robustness was assessed alongside practical implementation considerations rather than treated as an isolated property of predictive models. Particular attention was given to whether reported defenses remained feasible under industrial constraints such as limited

computational resources, latency requirements, heterogeneous sensors, imbalanced fault data, and evolving operating conditions.

Cross-study synthesis then examined relationships among attack vectors, affected system layers, compromised predictive functions, operational consequences, and defensive mechanisms. Convergent findings were distinguished from contradictory evidence, while underrepresented attack scenarios, methodological weaknesses, and unresolved assumptions were identified systematically. The resulting framework provided a consistent basis for evaluating how adversarial manipulation can propagate through maintenance-oriented digital twins and for comparing the effectiveness, limitations, and practical relevance of proposed robustness strategies across diverse industrial cyber-physical environments.

3. Digital-Twin Predictive-Maintenance Foundations

3.1 Digital-Twin Architectures and Data Pipelines

Digital-twin architecture in cyber-physical systems is a layered computational structure connecting physical assets, sensing infrastructure, communications, data management, virtual models, analytics, and services. For predictive maintenance, architectural quality determines whether heterogeneous measurements can be transformed into trustworthy representations of equipment condition at sufficient speed for diagnosis and prognosis. A mature twin therefore requires more than a three-dimensional model: it depends on bidirectional connectivity, state synchronization, semantic consistency, and mechanisms for integrating historical and streaming data across the asset lifecycle (Fuller et al., 2020).

At the physical layer, industrial machines, electrical assets, controllers, sensors, and actuators generate observations describing operating state and environmental context. These observations enter the twin through acquisition interfaces and communication protocols before being normalized, timestamped, filtered, and contextualized. The IoT-oriented architectural view emphasizes that identity management, connectivity, information models, synchronization, and service exposure are foundational characteristics of a functional twin, particularly where multiple devices and applications must exchange state information continuously (Minerva, Lee & Crespi, 2020).

Data pipelines form the connective tissue between these layers. They must accommodate structured and unstructured data, reconcile differences in sampling frequency, manage missing or noisy measurements, and preserve lineage as data move from edge devices to local servers or cloud platforms. The five-dimensional digital-twin model further demonstrates that physical entities, virtual models, twin data, services, and connections are mutually dependent

components; accordingly, data management cannot be separated from simulation, analytics, or maintenance decision support (Qi et al., 2021).

Architectural fidelity also depends on the modeling strategy used to translate incoming measurements into meaningful virtual state. Physics-based models provide causal structure, while data-driven models can capture degradation patterns difficult to formulate analytically. Hybrid architectures increasingly combine both approaches, requiring pipelines that align sensor histories, simulation outputs, learned features, and uncertainty estimates. From a modeling perspective, digital twins therefore rely on computational pipelines supporting real-time prediction, optimization, monitoring, and control while maintaining consistency between changing physical conditions and their digital representations (Rasheed, San & Kvamsdal, 2020).

African research has contributed practical architectures for managing this complexity. A South African six-layer architecture separates the physical system, local data acquisition, IoT gateway, cloud-based information storage, data-to-information conversion, and simulation or application layers. Its aggregation extension further addresses interaction among multiple twins through vendor-neutral technologies and open communication mechanisms, an important requirement for industrial facilities where maintenance intelligence may depend on fleets of interdependent assets rather than isolated machines (Redelinghuys, Kruger & Basson, 2020).

Within Nigeria-linked smart-grid research, a five-layer digital-twin architecture for smart substations integrates physical assets, data acquisition, communications, digital simulation, and analytics. The architecture illustrates how real-time operational measurements can be transformed into fault-detection intelligence beyond conventional supervisory monitoring. For predictive maintenance, this arrangement is significant because the integrity and latency of every layer influence whether evolving equipment abnormalities are represented accurately enough to support intervention before functional failure occurs (Shittu et al., 2023).

Industrial automation platforms provide the operational substrate through which many such pipelines are implemented. Integrated environments such as Siemens TIA Portal consolidate programmable logic control, human-machine interfaces, device configuration, diagnostics, and network engineering, reducing fragmentation between control and information layers. Their relevance to digital twins lies in establishing standardized access to process variables and control states that can populate virtual models and maintenance analytics. Effective integration consequently requires interoperability between operational technology and higher-

level data services without compromising timing requirements or control reliability (Sunday & Omoegun, 2022).

More recent architectures increasingly combine edge, cloud, simulation, and artificial-intelligence components to reduce latency while preserving scalability. In renewable-energy applications, hybrid digital twins have coupled MATLAB/Simulink models with historical and live sensor streams, machine-learning inference, and cloud-edge processing to support real-time fault detection and operational optimization. Such configurations demonstrate why maintenance-oriented twins should be viewed as dynamic data ecosystems rather than static replicas. They also reveal a security-critical dependency: if sensor inputs, synchronization channels, intermediate transformations, or analytical outputs are manipulated, corrupted information can propagate through the pipeline and alter the twin's perception of asset health, creating the architectural conditions through which adversarial deception can influence maintenance decisions (Shittu & Shittu, 2024).

3.2 Predictive Models for Maintenance Intelligence

Below is a substantially strengthened version that integrates the predictive-maintenance pipeline, model classes, decision outputs, and adversarial exposure into a single analytical narrative. The table is designed to function as an evidence-synthesis device rather than merely repeat the prose.

3.2 Predictive Models for Maintenance Intelligence

Predictive maintenance intelligence constitutes the analytical core through which digital twins convert continuous condition-monitoring data into actionable assessments of asset health, fault progression, degradation behaviour, and remaining useful life (RUL). Rather than responding to failure after it occurs, predictive models infer the evolving condition of physical equipment from heterogeneous sensor streams and support maintenance decisions before degradation reaches a critical threshold. Their effectiveness therefore depends not only on algorithmic accuracy but also on the quality, representativeness, temporal consistency, and security of the data entering the predictive pipeline. Within cyber-physical environments, this dependency creates a direct relationship between predictive capability and adversarial exposure.

Vibration-based condition monitoring remains particularly important for rotating machinery because mechanical deterioration frequently produces measurable changes in amplitude, frequency distribution, spectral energy, and statistical characteristics before visible or functional failure occurs. Continuous acquisition and analysis of such signals can reveal imbalance, misalignment, bearing degradation, looseness, and other developing

abnormalities. LabVIEW-based machinery-monitoring approaches demonstrate how vibration measurements can be systematically acquired, processed, and interpreted to support early fault recognition and condition-based maintenance interventions (Omoegun et al., 2023). In a digital-twin architecture, these measurements provide a dynamic evidential link between the physical asset and its virtual representation, enabling the twin to update its estimate of equipment condition as operational behaviour changes.

The analytical value of predictive maintenance, however, extends beyond conventional threshold-based monitoring. Contemporary machine-learning approaches are increasingly designed to identify nonlinear and latent degradation relationships that may not be captured through predefined alarm limits. Machinery prognostics can consequently be conceptualised as an interconnected analytical pipeline comprising sensor-data acquisition, preprocessing and feature extraction, construction of health indicators, identification of health or degradation stages, fault diagnosis, and eventual estimation of RUL. Lei et al. (2018) demonstrate that prognostic performance is determined by the reliability of this complete chain rather than by the terminal prediction algorithm alone. This observation is especially significant for digital twins because erroneous information generated at an upstream stage can propagate through subsequent analytical layers and ultimately distort the virtual asset state and associated maintenance recommendation.

Deep-learning models further extend this capability by learning discriminative representations directly from raw or minimally transformed sensor data. Convolutional neural networks (CNNs), for example, can automatically identify diagnostic structures within vibration signals, reducing dependence on manually engineered features and supporting more automated classification of machinery faults. Evidence from industrial rotating-machinery applications indicates that CNN-based architectures can achieve strong fault-identification performance and therefore strengthen automated maintenance decision support (Souza et al., 2021). Their operational advantage nevertheless introduces an important security consideration: as maintenance systems become increasingly dependent on complex learned representations, incorrect or intentionally manipulated input patterns can influence predictions in ways that may be difficult for human operators to detect immediately.

Hybrid predictive architectures attempt to improve prognostic robustness by combining algorithms with complementary analytical strengths. Long short-term memory (LSTM) networks are particularly suited to sequential degradation histories because they can model temporal dependencies, while artificial neural networks can capture nonlinear relationships among operating variables. Optimisation methods such as genetic algorithms may further

improve parameter selection and predictive performance. The Moroccan study by Noumich, Jaafar and Ayoub (2025), combining LSTM, artificial neural-network and genetic-algorithm techniques, illustrates how historical degradation trajectories can be transformed into forward-looking estimates of equipment health and maintenance requirements.

Table 1. Predictive-model architecture for maintenance intelligence and associated adversarial exposure.

Predictive layer/model	Primary analytical function	Typical maintenance intelligence	Digital-twin contribution	Principal adversarial exposure
Vibration monitoring and signal analysis	Detects changes in amplitude, frequency and statistical characteristics	Early identification of mechanical abnormalities	Continuously updates observable physical-condition states	Sensor spoofing, signal injection, measurement alteration or suppression
Feature and health-indicator models	Converts raw measurements into diagnostically meaningful representations	Health indices, degradation indicators and anomaly scores	Provides compact condition variables for twin-state estimation	Feature manipulation, preprocessing corruption or strategically altered observations
Machine-learning prognostics	Learns nonlinear relationships between operating conditions and degradation	Fault probability, health-stage classification and failure prediction	Maps observed behaviour to inferred equipment condition	Training-data poisoning, model manipulation and crafted input perturbations
Convolutional neural networks	Automatically extracts discriminative patterns from sensor signals	Automated fault classification and diagnostic recommendations	Enables high-dimensional condition interpretation with limited manual feature engineering	Adversarial perturbations capable of inducing incorrect classifications
LSTM and temporal models	Captures sequential dependencies across degradation histories	Degradation trajectory and RUL estimation	Supports dynamic forecasting of future asset condition	Manipulated temporal sequences, missing observations and false degradation trends
Hybrid and optimised	Integrates complementary	Improved prognosis, health	Strengthens multi-model	Cross-model error

models	algorithms and optimisation mechanisms	forecasting and maintenance prioritisation	inference and decision support	propagation and exploitation of optimisation dependencies
Maintenance decision layer	Converts predictive outputs into operational actions	Inspection, repair, replacement or maintenance scheduling	Connects virtual intelligence with physical intervention	False alarms, suppressed warnings, delayed maintenance or unnecessary intervention

Source: Synthesised from Omoegun et al. (2023), Lei et al. (2018), Souza et al. (2021) and Noumich, Jaafar and Ayoub (2025).

The table illustrates that predictive intelligence should not be understood as a single algorithmic operation but as a layered chain extending from physical sensing to operational intervention. Each layer generates information consumed by the next, creating cumulative dependencies across the digital-twin maintenance architecture. Consequently, adversarial interference does not necessarily need to compromise the final predictive model directly. Manipulation of vibration measurements, preprocessing routines, extracted features, temporal sequences, or health indicators may be sufficient to alter downstream estimates of degradation and RUL.

This interconnectedness transforms predictive maintenance from a purely optimisation-oriented capability into a cyber-physical security concern. An attacker who strategically alters measurements or model inputs could suppress genuine deterioration, create fictitious anomalies, distort inferred degradation trajectories, or trigger misleading maintenance recommendations. The resulting consequences may include premature component replacement, unnecessary production interruption, delayed intervention, accelerated physical deterioration, or failure to recognise an emerging hazard. Predictive models within digital twins should therefore be evaluated not solely according to classification accuracy or RUL-prediction error, but also according to data provenance, adversarial robustness, uncertainty awareness, model interpretability, and resilience to corrupted inputs. Maintenance intelligence becomes operationally trustworthy only when the analytical pipeline can distinguish genuine equipment degradation from manipulated representations of physical condition.

3.3 Cyber-Physical Dependencies and Attack Surfaces

Industrial cyber-physical systems derive value from coupled relationships among physical assets, sensing devices, communication networks, controllers, data platforms, and supervisory applications. These dependencies improve observability and automation, but they also create pathways through which compromise at one layer can propagate into another. In power infrastructures, grounding, protection, communication, and control functions interact with equipment safety and service continuity; weaknesses in these dependencies can magnify disturbances beyond their point of origin (Adeniji et al., 2020).

Interconnection becomes more complex when distributed energy resources, market platforms, and peer-to-peer transactions are incorporated into cyber-physical environments. Blockchain-supported microgrids illustrate how smart contracts, communication interfaces, distributed ledgers, metering devices, and control logic become mutually dependent components. Although decentralization can strengthen transparency and resilience, each additional interface expands the system's exploitable surface and increases the importance of secure identity, data integrity, and trustworthy coordination (Shittu et al., 2021).

Similar dependencies arise when emerging energy carriers are integrated into national grids. Hydrogen-related generation, storage, conversion, and transport introduce physical processes alongside digital monitoring and optimization requirements. Their coordination increases reliance on interoperable models and data exchanges, creating points where corrupted telemetry or manipulated control information could misrepresent system state to predictive-maintenance applications or digital twins (Shittu et al., 2019).

Attack surfaces are therefore not confined to conventional information-technology endpoints. They include field devices, remote terminal units, programmable controllers, engineering workstations, human-machine interfaces, communication protocols, and maintenance connections. South African analyses of ICS/SCADA environments show that legacy designs, weak authentication, exposed interfaces, patching constraints, and connectivity can leave critical infrastructure vulnerable to cyber intrusion. For maintenance-oriented digital twins, exploitation of these surfaces may falsify sensor histories, alter control states, conceal degradation, or generate misleading operational evidence, allowing cyber compromise to become a physical reliability problem (Pretorius & van Niekerk, 2016).

4. Adversarial Threats Against Predictive Maintenance

4.1 Evasion Attacks and Sensor Manipulation

Evasion attacks are consequential in predictive-maintenance digital twins because they target the inference stage, where legitimate-looking measurements are converted into assessments of asset health. Rather than disabling a model outright, an adversarial input can preserve plausibility while shifting a classifier, anomaly detector, or regression model toward an incorrect maintenance interpretation. Across cyber-physical machine-learning systems, such attacks may modify a subset of features while maintaining credible values, making conventional accuracy metrics insufficient for judging resilience under hostile conditions (Wang et al., 2024).

Industrial control environments make this threat harder because model inputs originate from sensors affected by process dynamics, noise, communication delays, calibration error, and equipment degradation. Studies of industrial-control evasion show that attack feasibility depends on constraints such as observation access, manipulation latency, and the ability to alter process data without creating obvious inconsistencies. For digital twins, these realities mean adversarial robustness should be evaluated against realizable perturbations rather than unconstrained modifications applied only to static datasets (Erba et al., 2024).

Sensor manipulation represents a route for corrupting maintenance intelligence. In HVAC monitoring, temperature, pressure, airflow, vibration, and related measurements support fault recognition and operational assessment; consequently, distorted measurements can mischaracterize component condition or conceal degradation. Sensor-based fault-detection architectures therefore illustrate how maintenance decisions inherit trust assumptions embedded in measurement channels (Sunday & Omoegun, 2020).

An analytical difficulty is distinguishing malicious manipulation from transient sensor faults. Multi-sensor cyber-physical research demonstrates that inconsistent measurements can arise from both attack and disturbance, requiring detection logic that considers expected variation rather than treating every deviation as hostile. This distinction is essential in predictive maintenance because aggressive filtering may suppress genuine failure signatures, whereas permissive thresholds may allow crafted perturbations into the digital twin (Park et al., 2015). Manufacturing systems further expose adversarial opportunities through quality-control, sensing, and decision-support mechanisms. Research involving Egyptian manufacturing expertise shows that cyber-physical attackers can exploit monitoring and quality-assurance functions in ways that alter physical outcomes while weakening mechanisms revealing abnormal behavior. For maintenance-oriented twins, comparable exploitation could distort

condition indicators and create misleading evidence about whether an asset requires intervention (Elhabashy, Wells & Camelio, 2020).

The most dangerous manipulations are those designed to remain inconspicuous. Stealthy deception research shows that corrupted observations can alter state estimation while remaining difficult for conventional detectors to distinguish from normal system behavior. In a predictive-maintenance digital twin, such deception could suppress true anomalies, create false alarms, distort remaining-useful-life estimates, or shift maintenance timing. Robustness therefore depends on validating sensor provenance, cross-checking physical consistency, quantifying uncertainty, and testing predictive models against adversarially perturbed operating trajectories before outputs are trusted for reliable safety-relevant decisions in practice (Liu et al., 2024).

4.2 Poisoning Attacks and Training Corruption

Poisoning attacks compromise predictive-maintenance intelligence by targeting training rather than test-time inputs. In digital-twin environments, models are retrained from sensor records, maintenance logs, inspection outcomes, and operational data. An adversary able to alter labels, inject crafted observations, or contaminate model updates can reshape the decision boundary before deployment. Foundational work demonstrated that poisoning samples can increase classification error while remaining embedded within a legitimate training set, revealing the vulnerability when learning algorithms trust training distributions (Biggio, Nelson & Laskov, 2012).

The threat becomes more consequential when maintenance models are distributed or collaboratively trained. Federated-learning research involving Nigerian and Namibian institutions identifies data poisoning and model poisoning among prominent security risks, because malicious participants may submit corrupted local data or manipulated parameter updates without exposing raw datasets. In an industrial digital twin, analogous compromise could bias fault classifiers, anomaly detectors, or remaining-useful-life estimators across connected assets, causing systematic rather than isolated maintenance errors (Guembe, Misra & Azeta, 2024).

Training corruption may be targeted, seeking a specific misclassification, or indiscriminate, degrading model utility. It can involve backdoors that preserve normal performance while activating malicious behavior under particular patterns. Survey evidence shows that poisoning can attack training data, model parameters, learning procedures, and distributed updates, making defenses dependent on trusted provenance, robust aggregation, dataset sanitization, anomaly screening, and validation against clean reference data. For predictive-

maintenance twins, these controls should span the model lifecycle because compromised learning can persist invisibly through inference, synchronization, and maintenance planning (Wang et al., 2022).

4.3 Model Extraction and Integrity Compromise

Model extraction threatens predictive-maintenance digital twins when adversaries repeatedly query diagnostic or prognostic models and use returned labels, confidence scores, explanations, or other outputs to reconstruct surrogate models. Such replication can expose intellectual property, reveal decision boundaries, and provide attackers with an environment for designing subsequent evasive manipulation against maintenance intelligence. Explanation-guided extraction research demonstrates that auxiliary interpretability information can substantially increase what an adversary learns about a black-box model, extending the confidentiality risk beyond ordinary prediction outputs (Yan et al., 2023).

Integrity compromise is equally consequential because digital twins depend on trusted exchanges among field devices, SCADA platforms, analytics engines, and model repositories. Nigerian research on blockchain-assisted SCADA data exchange shows how cryptographic verification, distributed records, and tamper-resistant transaction structures can strengthen integrity, auditability, and traceability across cyber-physical infrastructures. For predictive maintenance, these mechanisms can reduce opportunities for unauthorized alteration of measurements, analytical inputs, or operational records that would otherwise distort inferred asset health (Shittu et al., 2022).

Access control provides an additional safeguard because model integrity can be undermined through unauthorized interaction with digital-twin resources, interfaces, or physical entities. South African research on digital-twin-supported cyber-physical access control demonstrates how synchronized virtual representations can support identity-aware monitoring and real-time enforcement around protected assets. Applied to maintenance environments, comparable controls can restrict model-query privileges, monitor sensitive interfaces, and identify anomalous access before extraction or tampering escalates, thereby preserving confidentiality, provenance, authorization, and dependable twin state in operational industrial settings (Greaves, Coetzee & Leung, 2022).

5. Adversarial Robustness and Defensive Architectures

5.1 Robust Learning and Adversarial Training

Robust learning is fundamental to predictive-maintenance digital twins because maintenance decisions depend on models that must remain reliable when data are noisy, manipulated, or

perturbed. Adversarial training strengthens this reliability by incorporating modified examples into learning, forcing models to form decision boundaries less sensitive to hostile input changes. In autonomous-system research involving Nigerian scholarship, adversarially trained deep-learning models have demonstrated improved resistance to crafted attacks, highlighting their relevance to safety-critical industrial environments where incorrect predictions may trigger unnecessary interventions or conceal developing faults (Osoko, Rahmon & Azeez, 2023).

For predictive maintenance, however, robustness should extend beyond resistance to a single attack configuration. Industrial assets operate under changing loads, environmental conditions, degradation states, and sensor characteristics, meaning defensive models must remain stable across multiple perturbation types and intensities. Robust-learning strategies combining adversarial training, attack-aware evaluation, and adaptive optimization can improve resilience while exposing trade-offs among clean-data accuracy, worst-case performance, computational cost, and deployment latency. Such trade-offs are important in digital twins that rely on continuous synchronization and near-real-time inference (Eleftheriadis, Symeonidis & Katsaros, 2024).

Generalization is another critical requirement because predictive-maintenance systems encounter operating conditions not represented perfectly in historical training data. South African research on input margins shows that margin-based measures can provide insight into how learned decision boundaries generalize beyond observed samples. In maintenance contexts, these measures can help determine whether fault classifiers remain stable when sensor values shift within physically plausible ranges, supporting disciplined interpretation of robustness under operational uncertainty (Mouton, Theunissen & Davel, 2024).

Randomization offers a complementary defense by reducing deterministic sensitivity to adversarial inputs. Randomized classifiers can improve local robustness by introducing stochasticity into prediction while preserving acceptable performance on clean data. Within industrial digital twins, such mechanisms may reduce the effectiveness of attackers who depend on predictable model responses and support uncertainty-aware maintenance decisions when data provenance is uncertain. Their value is strongest when combined with adversarial training, model validation, sensor cross-checking, and continuous monitoring rather than deployed as an isolated safeguard (Pinot et al., 2022).

Accordingly, robust learning for maintenance intelligence should be treated as a lifecycle capability rather than a one-time training intervention. Models require reassessment against evolving attacks, newly observed degradation patterns, distribution shifts, and changing

sensor configurations. In digital-twin environments, this means integrating robustness testing into model updates, simulation workflows, and deployment governance so predictive decisions remain dependable as the physical system and threat landscape evolve.

6. Evaluation, Assurance, and Industrial Deployment

6.1 Robustness Metrics and Evaluation Protocols

Robustness evaluation in predictive-maintenance digital twins should establish whether a model remains dependable under nominal conditions and adversarial perturbations. Conventional accuracy alone is inadequate because a model may perform strongly on clean data yet fail when small, targeted changes are introduced. Accordingly, evaluation protocols should report clean accuracy alongside robust accuracy, attack success rate, false-positive rate, false-negative rate, precision, recall, F1-score, and area under the receiver operating characteristic curve. Foundational adversarial evaluation research demonstrates that robustness claims must be tested against strong attacks rather than inferred from apparent resistance to weak perturbations (Carlini & Wagner, 2017).

Evaluation should define the threat model explicitly, including attacker knowledge, accessible sensor channels, perturbation budget, attack objective, and physical feasibility. Robustness scores become difficult to compare when studies employ different attack strengths, input constraints, or success definitions. Automated attack-ensemble evaluation offers a stronger protocol by exposing defenses to heterogeneous attacks and selecting effective attack combinations, reducing the risk that robustness is overstated because one evaluation method is poorly matched to the model (Liu, Peng & Tang, 2023).

For predictive maintenance, conventional process-performance metrics remain important because adversarial robustness must coexist with engineering reliability. Statistical process control provides mechanisms for monitoring variability, identifying abnormal shifts, and distinguishing common-cause variation from signals requiring intervention. Such principles support control limits, process capability measures, and longitudinal stability checks when evaluating maintenance models operating continuously rather than on isolated benchmark samples (Akanbi, Ganiu & Sunday, 2022).

Evaluation must also reflect sensor modality and operating-condition diversity. South African research integrating control charts with machine-learning models for incipient wind-turbine bearing faults illustrates the value of combining statistical monitoring with data-driven anomaly detection, allowing performance to be assessed across evolving condition indicators

rather than through classification accuracy alone. This is relevant to digital twins, where drift, imbalance, and rare-fault conditions can distort apparent robustness (Gbashi et al., 2025).

Simulation-based stress testing can determine whether model-driven decisions remain credible when the underlying physical system is exposed to disturbances. Nigerian work using MATLAB/Simulink to assess harmonic mitigation in an urban distribution network demonstrates how controlled scenarios, baseline comparisons, and system responses can provide reproducible evidence under degraded conditions. Comparable protocols can inject sensor perturbations, communication errors, and model attacks while tracking maintenance consequences (Okwe et al., 2025).

Finally, robustness should be evaluated against unseen attacks and distribution shifts rather than only perturbations encountered during training. Evidence shows that defenses effective against familiar attacks may generalize poorly to novel adversarial conditions, making cross-attack testing essential (Garaev, Rasheed & Khan, 2024). A rigorous industrial protocol should therefore combine clean-data performance, adversarial stress tests, physically plausible perturbation bounds, repeated trials, uncertainty reporting, and operational metrics such as detection latency, false maintenance alarms, missed faults, and remaining-useful-life error. This multidimensional approach better distinguishes laboratory accuracy from dependable robustness for consequential decisions within synchronized industrial digital twins.

7. Research Gaps and Future Directions

7.1 Benchmarking and Reproducible Adversarial Testing

Benchmarking adversarial robustness in predictive-maintenance digital twins requires protocols that make results comparable across models, assets, datasets, and threat assumptions. A credible benchmark should specify the physical process, sensor modalities, prediction task, model architecture, attack knowledge, perturbation budget, and success criterion before testing. Otherwise, apparent robustness may reflect easier datasets or weaker attacks rather than genuine resilience. Adversarial-evaluation research shows that optimization failures can create misleading impressions of security, supporting explicit diagnostics for broken attacks, gradient masking, and inadequate search procedures (Pintor et al., 2022).

Reproducibility also depends on standardized datasets and experimental pipelines. Nigerian comparative intrusion-detection research demonstrates the value of evaluating learning algorithms against a common dataset while reporting accuracy, precision, recall, F1-score,

and related measures under consistent preprocessing. For industrial digital twins, comparable practice should preserve fixed train-validation-test partitions, document class imbalance, publish preprocessing rules, and report random seeds and hyperparameters so that differences can be independently reproduced rather than attributed to undocumented choices (Oduwole, Muhammad & Anyachebelu, 2023).

Benchmark design should additionally incorporate operational constraints. Ghanaian research evaluating hybrid intrusion-detection models on NSL-KDD and CIC-DDoS2019 illustrates the importance of benchmark datasets, cross-validation, class-specific performance, and testing against unevenly represented attack classes. Predictive-maintenance benchmarks should similarly measure false alarms, missed faults, attack success rate, inference latency, remaining-useful-life error, and performance across rare failure modes because aggregate accuracy can conceal vulnerabilities in safety-relevant classes (Mills, Acquah & Sowah, 2024).

Multimodal evaluation is particularly important for digital twins because maintenance decisions may combine vibration, temperature, acoustic, electrical, process, and human-machine interaction signals. A unified multimodal assessment framework emphasizes synchronization, data-quality control, artifact management, computational efficiency, and consistent measurement across heterogeneous channels. These principles strengthen adversarial testing by ensuring perturbations are evaluated against sensor consistency and system-level effects (Adamolekun et al., 2025).

A reproducible protocol should release benchmark definitions, attack configurations, code, model checkpoints, processing scripts, evaluation seeds, and reporting templates where permitted. Testing should include white-box and black-box attacks, repeated trials, transfer attacks, physically constrained perturbations, clean-data baselines, and sensitivity analyses. For maintenance-oriented digital twins, benchmarking should determine whether identical experiments yield consistent robustness estimates and whether successful attacks produce meaningful changes in diagnosis, prognosis, or maintenance scheduling.

7.2 Adaptive Attacks and Continual Robustness

Adaptive attacks present a challenge for predictive-maintenance digital twins because adversaries can observe defensive behaviour, modify tactics, and repeatedly probe models until safeguards become ineffective. Static robustness assessments therefore provide only a snapshot of security. Continual robustness requires predictive models to preserve knowledge while adapting to evolving attack patterns, operating regimes, and degradation states. Research on adversarially robust continual learning shows that combining continual-learning

mechanisms with adversarial training can improve resistance to attacks while reducing catastrophic forgetting across sequential tasks (Bai et al., 2023).

The industrial setting introduces an additional difficulty: legitimate data distributions change over time. Equipment aging, maintenance interventions, component replacement, seasonal conditions, production changes, and sensor recalibration can produce concept drift that resembles model degradation or adversarial manipulation. Predictive-maintenance research demonstrates that drift detection can identify machine behaviour in continuous sensor streams and support model adaptation, making drift-awareness an essential component of maintenance intelligence (Zenisek, Holzinger & Affenzeller, 2019).

Adaptive resilience also depends on decision structures. Nigerian-linked research on multi-agent artificial intelligence and swarm coordination demonstrates how decentralized agents can respond dynamically to changing tasks, disturbances, communication constraints, and operational priorities. For digital-twin maintenance environments, distributed intelligence may support localized anomaly assessment and coordinated responses, but it also creates avenues for compromised agents, deceptive messages, or poisoned local observations to influence collective behaviour (Akanbi, Ganiu & Sunday, 2025).

Continual robustness must therefore extend beyond retraining. South African cybersecurity research emphasizes that adaptation to changing threats requires learning mechanisms capable of absorbing feedback, revising assumptions, and overcoming organizational inertia that delays defensive change. Applied to industrial digital twins, this principle implies governance for deciding when models should update, which observations are trustworthy, and when historical knowledge should be retained rather than overwritten (Nyakasoka & Naidoo, 2024).

7.3 Standards, Governance, and Regulatory Alignment

Governance of adversarially robust predictive-maintenance digital twins requires alignment between technical safeguards, organizational accountability, cybersecurity standards, and emerging artificial-intelligence regulation. Because maintenance models can influence equipment availability, worker safety, production continuity, and critical infrastructure reliability, governance should treat robustness as a lifecycle obligation rather than a one-time validation activity. The NIST AI Risk Management Framework offers a useful organizing logic through governance, mapping, measurement, and management functions, encouraging organizations to identify context-specific harms, document controls, and monitor residual risk throughout deployment (Tabassi, 2023).

For industrial cyber-physical systems, AI governance must integrate with operational-technology security practice. Predictive-maintenance twins depend on sensors, controllers, engineering workstations, networks, cloud services, and analytical models; consequently, compliance cannot be confined to machine learning. Industrial-control research shows that cyber-risk management requires asset identification, risk assessment, security controls, assurance mechanisms, and metrics adapted to operational constraints. This supports alignment with frameworks such as IEC 62443 while preserving safety and availability objectives (Knowles et al., 2015).

Regulatory alignment is increasingly risk-based. European AI governance distinguishes obligations according to the potential consequences of AI applications, emphasizing documentation, oversight, data governance, transparency, and accountability. For predictive-maintenance systems in safety-relevant infrastructure, this logic matters because an adversarially manipulated model can influence physical interventions even when the algorithm does not directly control equipment. Risk classification should therefore consider downstream maintenance decisions, dependence on automated recommendations, and the severity of foreseeable cyber-physical consequences (Veale & Zuiderveen Borgesius, 2021).

Compliance must extend beyond pre-deployment certification. Auditing research on European AI regulation emphasizes conformity assessment and post-market monitoring as complementary mechanisms for demonstrating that high-risk systems continue satisfying requirements after release. Applied to industrial digital twins, this implies maintaining model cards, data provenance records, attack-test results, change logs, incident reports, retraining approvals, and evidence of robustness after software, sensor, or process modifications. Governance should also define thresholds for suspending models whose performance or security assumptions deteriorate (Mökander et al., 2022).

National context remains important. Nigerian research on digital technology and AI governance identifies gaps between rapid technological adoption and sufficiently explicit ethical and security guidance. For industrial organizations, this reinforces the need to translate principles concerning privacy, accountability, transparency, security, and responsible innovation into auditable controls within maintenance workflows. Regulatory alignment should therefore combine domestic legal obligations with recognized technical standards rather than assume that imported governance frameworks automatically fit local institutional conditions (Alakitan& Makinde, 2025).

African regional experience further demonstrates that policy implementation depends on institutional capacity and ethical leadership, not merely formal strategies. Research within the

Southern African Development Community highlights how technological transformation can be weakened when implementation structures, accountability, and leadership do not sustain stated policy objectives. For adversarially robust digital twins, governance consequently requires assigned model owners, cybersecurity responsibilities, independent assurance, incident-response authority, and executive oversight capable of converting standards into enforceable practice (Enaifoghe, Dlamini & Agwuna, 2020).

A mature governance architecture should map every predictive-maintenance model to standards, legal duties, risk owners, validation evidence, and monitoring obligations. Procurement contracts should specify security requirements, audit rights, update responsibilities, vulnerability disclosure, and data-governance expectations. Organizations should establish adversarial testing, independent review of high-consequence models, human override procedures, traceable retraining approval, and documented recovery plans. Cross-border deployments should reconcile differences in data protection, AI regulation, cybersecurity requirements, and sector-specific safety rules. This layered approach turns regulatory alignment from documentation into an operational assurance system capable of preserving trustworthy maintenance intelligence as models, assets, threats, and legal expectations evolve.

CONCLUSION

This review examined how adversarial manipulation can undermine predictive-maintenance intelligence within digital-twin-enabled industrial cyber-physical systems and assessed the extent to which current robustness strategies can preserve trustworthy maintenance decision-making. The study achieved its objectives by integrating evidence on digital-twin architectures, predictive models, cyber-physical dependencies, adversarial attack mechanisms, defensive learning, evaluation protocols, and governance requirements. The synthesis showed that the principal vulnerability of maintenance-oriented digital twins lies in their dependence on interconnected data pipelines, where compromised sensors, poisoned training data, manipulated model inputs, or unauthorized model access can distort fault diagnosis, remaining-useful-life estimation, anomaly detection, and maintenance prioritization.

The review further established that adversarial robustness cannot be treated as a purely algorithmic property. Effective protection requires coordinated controls across sensing, communications, model development, runtime inference, access management, and system recovery. Adversarial training, robust learning, multimodal validation, sensor cross-checking,

secure data exchange, continuous monitoring, and adaptive retraining emerged as important defensive mechanisms. However, current research remains constrained by inconsistent benchmarks, limited use of physically realistic attacks, insufficient testing against adaptive adversaries, weak reproducibility, and inadequate integration of operational consequences into robustness assessment. These deficiencies are particularly consequential in safety-critical settings, where a seemingly minor prediction error can trigger unnecessary intervention, conceal emerging failure, or propagate operational disruption across assets.

Accordingly, industrial deployment should adopt lifecycle-oriented assurance frameworks that combine technical robustness with engineering reliability, cybersecurity governance, and regulatory accountability. Future research should prioritize standardized adversarial benchmarks for industrial time-series data, reproducible testing protocols, continual-learning defenses, explainable robustness assessment, and methods that distinguish malicious manipulation from legitimate drift or equipment degradation. Organizations should also implement model provenance controls, independent validation, human oversight, incident-response procedures, and post-deployment monitoring. Overall, the evidence demonstrates that dependable predictive maintenance in digitally connected industrial environments will require robustness to be designed, tested, governed, and continuously reassessed as an integral component of operational safety and resilience.

REFERENCES

1. Adamolekun, A., Logah, F.X., Alabi, C., Baanye, J., Wilson, M., Ganiu, O., Seong, Y. and Yi, S. (2025) 'Toward a unified framework for multimodal cognitive workload assessment in human-machine interaction systems', SSRN Electronic Journal, SSRN 5235980. DOI: 10.2139/ssrn.5235980.
2. Adeniji, I.O., Shittu, H.A., Elumilade, R.A., Opara, I.S. and Shittu, M.A. (2020) 'Grounding system design optimization for medium-voltage distribution networks in emerging power markets', *Iconic Research and Engineering Journals*, 3(11), pp. 547–565. DOI: 10.64388/IREV3I11-1714040.
3. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'Comprehensive review of statistical process control (SPC) for precision weight management in global food manufacturing', *Gyanshauryam: International Scientific Refereed Research Journal*, 5(3), pp. 433–461.
4. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2025) 'A multi-agent AI framework for swarm intelligence in autonomous mobile robot (AMR) fleet coordination', *International Journal of Scientific Research in Humanities and Social Sciences*, 2(1), pp. 81–109.

5. Alakitan, M. and Makinde, E.O. (2025) 'Where are the ethical guidelines? Examining the governance of digital technologies and AI in Nigeria', *Policy & Internet*, 17(1), e416. DOI: 10.1002/poi3.416.
6. Bai, T., Chen, C., Lyu, L., Zhao, J. and Wen, B. (2023) 'Towards adversarially robust continual learning', in 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1–5. DOI: 10.1109/ICASSP49357.2023.10096163.
7. Biggio, B., Nelson, B. and Laskov, P. (2012) 'Poisoning attacks against support vector machines', in *Proceedings of the 29th International Conference on Machine Learning (ICML '12)*, pp. 1467–1474. DOI: 10.5555/3042573.3042761.
8. Carlini, N. and Wagner, D. (2017) 'Towards evaluating the robustness of neural networks', 2017 IEEE Symposium on Security and Privacy (SP), pp. 39–57. DOI: 10.1109/SP.2017.49.
9. Carvalho, T.P., Soares, F.A.A.M.N., Vita, R., Francisco, R.P., Basto, J.P.T.V. and Alcalá, S.G.S. (2019) 'A systematic literature review of machine learning methods applied to predictive maintenance', *Computers & Industrial Engineering*, 137, 106024. DOI: 10.1016/j.cie.2019.106024. (IIT Comillas)
10. Doubell, G.D., Basson, A.H., Kruger, K. and Conradie, P.D.F. (2024) 'A digital twin system for railway infrastructure', *R&D Journal*, 39, pp. 23–34. DOI: 10.17159/2309-8988/2023/v39a3.
11. Eleftheriadis, C., Symeonidis, A. and Katsaros, P. (2024) 'Adversarial robustness improvement for deep neural networks', *Machine Vision and Applications*, 35, Article 35. DOI: 10.1007/s00138-024-01519-1.
12. Elhabashy, A.E., Wells, L.J. and Camelio, J.A. (2020) 'Cyber-physical attack vulnerabilities in manufacturing quality control tools', *Quality Engineering*, 32(4), pp. 676–692. DOI: 10.1080/08982112.2020.1737115.
13. Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Accessing the importance of ethical leadership for policy implementation in SADC', *Journal of Economics and Behavioral Studies*, 12(6), pp. 11–20. DOI: 10.22610/jeb.v12i6(J).3102.
14. Erba, A., Murillo, A.F., Taormina, R., Galelli, S. and Tippenhauer, N.O. (2024) 'On practical realization of evasion attacks for industrial control systems', in *Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security (RICSS '24)*. New York: Association for Computing Machinery, pp. 9–25. DOI: 10.1145/3689930.3695213.

15. Fuller, A., Fan, Z., Day, C. and Barlow, C. (2020) 'Digital Twin: Enabling technologies, challenges and open research', *IEEE Access*, 8, pp. 108952–108971. DOI: 10.1109/ACCESS.2020.2998358.
16. Garaev, R., Rasheed, B. and Khan, A.M. (2024) 'Not so robust after all: Evaluating the robustness of deep neural networks to unseen adversarial attacks', *Algorithms*, 17(4), 162. DOI: 10.3390/a17040162.
17. Gbashi, S.M., Olatunji, O.O., Adedeji, P.A. and Madushele, N. (2025) 'Control chart-integrated machine learning models for incipient fault detection in wind turbine main bearing', *Discover Artificial Intelligence*, 5, 149. DOI: 10.1007/s44163-025-00409-3.
18. Greaves, B., Coetzee, M. and Leung, W.S. (2022) 'Digital twin monitoring for cyber-physical access control', in Meng, W. and Katsikas, S.K. (eds.) *Emerging Information Security and Applications: 2nd International Symposium, EISA 2021, Revised Selected Papers. Communications in Computer and Information Science*, Vol. 1403. Cham: Springer, pp. 144–158. DOI: 10.1007/978-3-030-93956-4_9.
19. Guembe, B., Misra, S. and Azeta, A. (2024) 'Privacy issues, attacks, countermeasures and open problems in federated learning: A survey', *Applied Artificial Intelligence*, 38(1), 2410504. DOI: 10.1080/08839514.2024.2410504.
20. Ibor, A.E., Egete, D.O., Otiko, A.O. and Ashishie, D.U. (2025) 'Detecting network intrusions in cyber-physical systems using deep autoencoder-based dimensionality reduction approach and deep neural networks', *Journal of the Nigerian Society of Physical Sciences*, 7(3), 2689. DOI: 10.46481/jnsps.2025.2689.
21. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*, 9, pp. 52–80. DOI: 10.1016/j.ijcip.2015.02.002.
22. Kritzinger, W., Karner, M., Traar, G., Henjes, J. and Sihn, W. (2018) 'Digital Twin in manufacturing: A categorical literature review and classification', *IFAC-PapersOnLine*, 51(11), pp. 1016–1022. DOI: 10.1016/j.ifacol.2018.08.474. (CiNii Research)
23. Lee, J., Bagheri, B. and Kao, H.-A. (2015) 'A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems', *Manufacturing Letters*, 3, pp. 18–23. DOI: 10.1016/j.mfglet.2014.12.001. (DOI)
24. Lei, Y., Li, N., Guo, L., Li, N., Yan, T. and Lin, J. (2018) 'Machinery health prognostics: A systematic review from data acquisition to RUL prediction', *Mechanical Systems and Signal Processing*, 104, pp. 799–834. DOI: 10.1016/j.ymssp.2017.11.016.

25. Liu, Q., Wang, J., Ni, Y., Zhang, C., Shi, L. and Qin, J. (2024) 'Performance analysis for cyber–physical systems under two types of stealthy deception attacks', *Automatica*, 160, 111446. DOI: 10.1016/j.automatica.2023.111446.
26. Liu, S., Peng, F. and Tang, K. (2023) 'Reliable robustness evaluation via automatically constructed attack ensembles', *Proceedings of the AAAI Conference on Artificial Intelligence*, 37(7), pp. 8852–8860. DOI: 10.1609/aaai.v37i7.26064.
27. Mills, G.A., Acquah, D.K. and Sowah, R.A. (2024) 'Network intrusion detection and prevention system using hybrid machine learning with supervised ensemble stacking model', *Journal of Computer Networks and Communications*, 2024, Article 5775671. DOI: 10.1155/2024/5775671.
28. Minerva, R., Lee, G.M. and Crespi, N. (2020) 'Digital Twin in the IoT context: A survey on technical features, scenarios, and architectural models', *Proceedings of the IEEE*, 108(10), pp. 1785–1824. DOI: 10.1109/JPROC.2020.2998530.
29. Mökander, J., Axente, M., Casolari, F. and Floridi, L. (2022) 'Conformity assessments and post-market monitoring: A guide to the role of auditing in the proposed European AI regulation', *Minds and Machines*, 32(2), pp. 241–268. DOI: 10.1007/s11023-021-09577-4.
30. Mouton, C., Theunissen, M.W. and Davel, M.H. (2024) 'Input margins can predict generalization too', *Proceedings of the AAAI Conference on Artificial Intelligence*, 38(13), pp. 14379–14387. DOI: 10.1609/aaai.v38i13.29351.
31. Nethamba, L. and Grobbelaar, S. (2023) 'The development of an action priority matrix and technology roadmap for the implementation of data-driven and machine-learning-based predictive maintenance in the South African railway industry', *South African Journal of Industrial Engineering*, 34(3), pp. 318–335. DOI: 10.7166/34-3-2958. (SA Journal of Industrial Engineering)
32. Noumich, F., Jaafar, A. and Ayoub, A. (2025) 'LSTM-ANN-GA: A hybrid deep learning model for predictive maintenance of industrial equipment', *Proceedings on Engineering Sciences*, 7, pp. 861–868. DOI: 10.24874/PES07.02.014.
33. Nyakasoka, L. and Naidoo, R. (2024) 'Understanding the inertial forces impeding dynamic cybersecurity learning capabilities: The case of a South African healthcare software services firm', *South African Computer Journal*, 36(1), pp. 105–132. DOI: 10.18489/sacj.v36i1.18877.

34. Oduwole, O.O., Muhammad, U.A. and Anyachebelu, K.T. (2023) 'Comparative evaluation of machine learning algorithms for intrusion detection', *Asian Journal of Research in Computer Science*, 16(4), pp. 8–22. DOI: 10.9734/ajrcos/2023/v16i4366.
35. Okwe, G., Abdullahi, M., Ezianya, E., Shittu, H., Okara, C.C., Shittu, M., Harrison, E., Pelumi, A., Eghujovbo, V., Ali, D., Ogunnaike, O., Sunday, E. and Ogbuagu, D.C. (2025) 'Mitigating harmonics impact for efficient electricity distribution in Owerri-Urban using MATLAB/Simulink', *Journal of Electrical Systems*, 21(1s), pp. 313–319. DOI: 10.52783/jes.8797.
36. Olutimehin, A.O. and Ganiu, O.S. (2022) 'Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence', *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), pp. 983–996. DOI: 10.54660/IJMRGE.2022.3.6.983-996. (All Multidisciplinary Journal)
37. Omoegun, G.O., Sunday, E.A., Essien, M.A. and Oluokun, O.A. (2023) 'Vibration-based condition monitoring of rotating machinery using LabVIEW', *International Journal of Scientific Research in Civil Engineering*, 7(6), pp. 82–108. DOI: 10.32628/IJSRCE237529.
38. Osoko, E.A., Rahmon, S.O. and Azeez, M. (2023) 'Enhancing the security of AI-driven autonomous systems through adversarially robust deep learning models', *World Journal of Advanced Research and Reviews*, 20(1), pp. 1336–1351. DOI: 10.30574/wjarr.2023.20.1.2158.
39. Park, J., Ivanov, R., Weimer, J., Pajic, M. and Lee, I. (2015) 'Sensor attack detection in the presence of transient faults', in *Proceedings of the 6th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS '15)*. New York: Association for Computing Machinery, pp. 1–10. DOI: 10.1145/2735960.2735984.
40. Pinot, R., Meunier, L., Yger, F., Gouy-Pailler, C., Chevalere, Y. and Atif, J. (2022) 'On the robustness of randomized classifiers to adversarial examples', *Machine Learning*, 111, pp. 3425–3457. DOI: 10.1007/s10994-022-06216-6.
41. Pintor, M., Demetrio, L., Sotgiu, A., Demontis, A., Carlini, N., Biggio, B. and Roli, F. (2022) 'Indicators of attack failure: Debugging and improving optimization of adversarial examples', *Advances in Neural Information Processing Systems*, 35, pp. 23063–23076. DOI: 10.52202/068431-1676.
42. Pretorius, B.H. and van Niekerk, B. (2016) 'Cyber-security for ICS/SCADA: A South African perspective', *International Journal of Cyber Warfare and Terrorism*, 6(3), pp. 1–16. DOI: 10.4018/IJCWT.2016070101.

43. Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., Wang, L. and Nee, A.Y.C. (2021) 'Enabling technologies and tools for digital twin', *Journal of Manufacturing Systems*, 58, pp. 3–21. DOI: 10.1016/j.jmsy.2019.10.001.
44. Rasheed, A., San, O. and Kvamsdal, T. (2020) 'Digital Twin: Values, challenges and enablers from a modeling perspective', *IEEE Access*, 8, pp. 21980–22012. DOI: 10.1109/ACCESS.2020.2970143.
45. Redelinghuys, A.J.H., Kruger, K. and Basson, A.H. (2020) 'A six-layer architecture for digital twins with aggregation', in Borangiu, T., Trentesaux, D., Leitão, P., Giret Boggino, A. and Botti, V. (eds.) *Service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future. Studies in Computational Intelligence*, Vol. 853. Cham: Springer, pp. 171–182. DOI: 10.1007/978-3-030-27477-1_13.
46. Shamshiri, S., Liu, H. and Sohn, I. (2025) 'Adversarial robust image processing in medical digital twin', *Information Fusion*, 115, 102728. DOI: 10.1016/j.inffus.2024.102728.
47. Shittu, H.A. and Shittu, M.A. (2024) 'AI powered digital twins for predictive maintenance and operational optimization of renewable energy systems', *International Journal of Science, Architecture, Technology, and Environment*, 1(7), pp. 151–163. DOI: 10.63680/ijstate0324085.011
48. Shittu, H.A., Opara, I.S., Elumilade, R.A., Liadi, K.O. and Adeniji, I.O. (2019) 'Hydrogen as a secondary energy carrier: Modeling its integration in national grids', *Iconic Research and Engineering Journals*, 3(1), pp. 628–643. DOI: 10.64388/IREV3I1-1713909.
49. Shittu, H.A., Shittu, M.A. and Olagunju, F. (2024) 'Cyber physical resilience in digital substations: IoT enabled adaptive protection for secure DER integration', *International Journal of Science, Architecture, Technology, and Environment*, 1(3), pp. 81–99. DOI: 10.63680/ijstate032532.08.
50. Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain based energy trading models for peer-to-peer renewable microgrids', *International Journal of Research in Electrical and Electronics Engineering*, 4(3), pp. 1–19. DOI: 10.34218/IJREEE_04_03_001.
51. Shittu, M.A., Adeniji, I.O., Shittu, H.A. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', *Iconic Research and Engineering Journals*, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.

52. Shittu, M.A., Shittu, H.A., Adeleke, O.J. and Adedokun, O.J. (2023) 'Digital twin modeling for real time monitoring and fault detection in smart substations', *International Journal of Industrial Engineering Research and Development*, 14(2), pp. 25–44. DOI: 10.34218/IJIERD_14_02_003.
53. Silvestri, L., Forcina, A., Introna, V., Santolamazza, A. and Cesarotti, V. (2020) 'Maintenance transformation through Industry 4.0 technologies: A systematic literature review', *Computers in Industry*, 123, 103335. DOI: 10.1016/j.compind.2020.103335. (ScienceDirect)
54. Souza, R.M., Nascimento, E.G.S., Miranda, U.A., Silva, W.J.D. and Lepikson, H.A. (2021) 'Deep learning for diagnosis and classification of faults in industrial rotating machinery', *Computers & Industrial Engineering*, 153, 107060. DOI: 10.1016/j.cie.2020.107060.
55. Suhail, S., Iqbal, M., Hussain, R. and Jurdak, R. (2023) 'ENIGMA: An explainable digital twin security solution for cyber–physical systems', *Computers in Industry*, 151, 103961. DOI: 10.1016/j.compind.2023.103961.
56. Sunday, E.A. and Omoegun, G.O. (2020) 'Smart fault detection in HVAC systems using sensor-based monitoring', *International Journal of Scientific Research in Science, Engineering and Technology*, 7(4), pp. 380–403.
57. Sunday, E.A. and Omoegun, G.O. (2022) 'Automation of process control systems using Siemens TIA Portal: A case study approach', *International Journal of Scientific Research in Mechanical and Materials Engineering*, 6(5), pp. 30–55.
58. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) 'Transitioning from reactive to predictive maintenance in mechanical systems', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(6), pp. 425–447. (IJSRCSEIT)
59. Tabassi, E. (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.AI.100-1.
60. Veale, M. and Zuiderveen Borgesius, F. (2021) 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International*, 22(4), pp. 97–112. DOI: 10.9785/cri-2021-220402.
61. Wang, S., Ko, R.K.L., Bai, G., Dong, N., Choi, T. and Zhang, Y. (2024) 'Evasion attack and defense on machine learning models in cyber-physical systems: A survey', *IEEE*

- Communications Surveys & Tutorials, 26(2), pp. 930–966. DOI: 10.1109/COMST.2023.3344808.
62. Wang, Z., Ma, J., Wang, X., Hu, J., Qin, Z. and Ren, K. (2022) ‘Threats to training: A survey of poisoning attacks and defenses on machine learning systems’, *ACM Computing Surveys*, 55(7), Article 134, pp. 1–36. DOI: 10.1145/3538707.
63. Yan, A., Huang, T., Ke, L., Liu, X., Chen, Q. and Dong, C. (2023) ‘Explanation leaks: Explanation-guided model extraction attacks’, *Information Sciences*, 632, pp. 269–284. DOI: 10.1016/j.ins.2023.03.020.
64. Zenisek, J., Holzinger, F.C. and Affenzeller, M. (2019) ‘Machine learning based concept drift detection for predictive maintenance’, *Computers & Industrial Engineering*, 137, 106031. DOI: 10.1016/j.cie.2019.106031.
65. Zonta, T., da Costa, C.A., da Rosa Righi, R., de Lima, M.J., da Trindade, E.S. and Li, G.P. (2020) ‘Predictive maintenance in the Industry 4.0: A systematic literature review’, *Computers & Industrial Engineering*, 150, 106889. DOI: 10.1016/j.cie.2020.106889. (ScienceDirect)