International Journal of Multidisciplinary Research and Bulletin
ISSN 3108-1428 (Online)

Article History
Received: 09 Aug 2026
Accepted: 06 Oct 2026
Published: 17 Oct 2026

International Journal of Multidisciplinary Research and Bulletin
Volume 5 Issue 5 (Sep – Oct) 2026

DOI:
10.5281/zenodo.23437027

Copyright © 2026, Authors retain copyright. Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Keywords: Industrial Internet of Things, Fault Tolerance, Artificial Intelligence, Machine Learning, Industrial Automation.

Fault Tolerance in IoT Networks for Industrial Automation Using Artificial Intelligence

Mubarak Jibril Yeldu

***Correspondence:** Mubarak Jibril Yeldu

Department of Computer Science, Abdullahi Fodio University of Science and Technology Aliero, Nigeria.

ABSTRACT

The Industrial Internet of Things (IIoT) has become a fundamental component of modern industrial automation by connecting sensors, actuators, programmable logic controllers, robotic systems, machines, edge devices, and cloud platforms for continuous monitoring and intelligent control. However, the dependence of industrial operations on interconnected IoT networks introduces significant risks associated with communication failures, sensor faults, hardware degradation, software errors, cyber-attacks, congestion, and edge computing failures. A single failure can interrupt production, reduce product quality, increase maintenance costs, or create safety hazards. This paper examines the application of Artificial Intelligence (AI) to improve fault tolerance in IoT networks used for industrial automation. The paper reviews recent developments in AI based fault detection, anomaly detection, predictive maintenance, intelligent routing, and edge based recovery, and adaptive resource management. Recent studies demonstrate that machine learning can identify abnormal device and sensor behavior before failures propagate, while Software Defined Networking can support rapid route restoration and network recovery. AI enabled edge computing further reduces response latency by moving fault analysis closer to industrial devices. The paper proposes a conceptual AI enabled fault tolerant architecture consisting of an IoT sensing layer, resilient communication layer, edge intelligence layer, AI fault analysis layer, decision and recovery layer, and industrial control layer. The proposed approach combines real-time monitoring, machine-learning-based prediction, redundant communication paths, automated recovery, and predictive maintenance. The paper concludes that integrating AI with fault-tolerance mechanisms can improve industrial network availability, reliability, resilience, and operational continuity. Nevertheless, challenges involving data quality, explain ability, computational

resources, cyber security, interoperability, and validation in real industrial environments require further investigation.

1. INTRODUCTION

The Industrial Internet of Things (IIoT) has become an important technological foundation for modern industrial automation because it enables machines, sensors, controllers, robots, actuators, gateways, and computing platforms to exchange operational information continuously. The integration of IoT with artificial intelligence (AI), edge computing, and advanced analytics has created opportunities for real-time monitoring, predictive maintenance, process optimization, quality control, and autonomous decision making. However, increased connectivity also creates a larger number of components and communication paths that may fail. A malfunctioning sensor, communication link, gateway, edge device, controller, or industrial machine can therefore affect other interconnected components and potentially interrupt production. The reliability of IIoT systems has consequently become an important research issue, particularly for industrial environments where continuous operation, safety, and timely response are essential.

Industrial automation systems generate large quantities of operational information through temperature, vibration, pressure, current, voltage, speed, acoustic, energy-consumption, and equipment-status sensors. These data provide an important basis for identifying abnormal conditions and predicting potential failures. Recent research has demonstrated that machine learning techniques can use relatively accessible device-level measurements to detect and classify faults in IIoT embedded devices. This study on industrial IoT embedded devices developed a machine-learning pipeline for fault detection and classification and reported high performance using energy, processing, and application-related measurements obtained from an industrial test bed. The results demonstrate that AI can identify abnormal device behavior before it develops into a more serious operational problem the need for intelligent fault management is particularly important because traditional fault-tolerance mechanisms are often based on predefined thresholds, periodic inspections, redundancy, preventive maintenance, or manually configured recovery rules. Although these mechanisms remain useful, they may not adequately address highly dynamic industrial environments in which operating conditions change continuously. Recent research has consequently shifted toward machine learning and deep learning methods capable of learning complex relationships between equipment conditions and failure patterns. (Saeed et al. 2025), for example, reviewed deep-learning approaches for

intelligent industrial machinery health management and fault diagnosis and emphasized the importance of intelligent fault diagnosis, remaining-useful life prediction, condition monitoring, and edge-based architectures. Their work also highlights a major limitation of many existing AI approaches: they frequently assume that complete, balanced, and abundant training data are available, whereas actual industrial environments often contain incomplete, imbalanced, noisy, and limited fault data.

Fault tolerance in IIoT must also address the communication network rather than concentrating exclusively on physical equipment. Industrial automation depends on reliable communication between sensors, controllers, edge devices, and supervisory systems. Network failures can result from link interruption, congestion, interference, gateway malfunction, routing errors, device overload, or malicious activity. Therefore, an industrial fault-tolerant architecture needs to detect both equipment-level and network-level abnormalities. Recent research on computational intelligence for IoT reliability identifies machine learning, deep learning, and evolutionary approaches as important techniques for fault diagnosis, fault prediction, and fault tolerance in distributed IoT environments

Artificial intelligence can improve fault tolerance by changing the traditional approach from reactive failure management to predictive and adaptive management. Instead of waiting for a component to fail completely, an AI model can continuously analyze operational data, identify deviations from normal behavior, estimate the likelihood of failure, determine the probable cause, and recommend or initiate an appropriate recovery action. This capability is particularly useful for predictive maintenance, where the objective is to identify equipment degradation before it produces an unexpected production interruption. Recent research on streaming industrial IoT data has investigated combinations of deep reinforcement learning, Random Forest, and Gradient Boosting for adaptive fault prediction and maintenance decisions. Such approaches demonstrate the potential of combining different AI techniques to accommodate dynamic operating conditions and improve fault-prediction reliability (Varalakshmi & Kumar, 2025).

Edge computing further strengthens AI-enabled fault tolerance. Sending all industrial sensor data to a centralized cloud platform can increase communication latency and create dependence on external connectivity. Processing data at or close to the industrial edge allows abnormal conditions to be identified rapidly and recovery decisions to be initiated locally. Recent work on IoT-based predictive-maintenance anomaly detection has demonstrated the value of edge

processing and computationally efficient statistical features for real-time machinery fault detection in resource-constrained environments

Deep learning is also becoming increasingly relevant because industrial sensor signals are often complex and multidimensional. Convolutional neural networks can learn representations from vibration and other signal patterns, while recurrent architectures can model temporal changes in equipment behavior. Recent work on deep-learning-based predictive maintenance in IIoT applications identifies CNN, RNN, and hybrid deep-learning approaches as promising techniques for processing real-time sensor information and predicting equipment degradation. However, data quality, scalability, interpretability, and edge-cloud integration remain important concerns (Deep Learning-based Predictive Maintenance for Industrial IoT Applications,

Another important development is the use of AI to support adaptive maintenance and recovery decisions. Conventional predictive maintenance may indicate that a machine is likely to fail, but an intelligent fault-tolerant system should go further by determining what action should be taken. For example, the system may isolate a defective sensor, activate a redundant sensor, reroute network traffic, migrate computation to another edge node, reduce the workload of an overloaded device, or schedule maintenance during a low-production period. Recent comparative research has examined Random Forest, Support Vector Machines, neural networks, and gradient-boosting techniques for predictive maintenance in IIoT and found that model selection involves a trade-off between predictive performance and computational requirements (Giorgianni et al., 2025).

AI-driven fault tolerance is therefore increasingly viewed as a combination of intelligent monitoring, fault diagnosis, failure prediction, resilient communication, edge intelligence, and automated recovery. Nevertheless, several challenges remain. Industrial AI models require reliable data, appropriate training datasets, computational resources, cyber security protection, explain ability, and validation under realistic industrial conditions. Fault data are also typically less abundant than normal-operation data, creating class-imbalance and generalization problems. Furthermore, an AI model that performs well in a laboratory environment may not necessarily maintain the same performance when exposed to equipment ageing, changing workloads, sensor noise, communication interference, and previously unseen faults.

This research paper therefore examines fault tolerance in IoT networks for industrial automation using artificial intelligence. The research focuses on the application of machine learning, deep learning, anomaly detection, predictive maintenance, edge intelligence, and intelligent recovery mechanisms to improve the reliability and resilience of industrial IoT systems. It further proposes

a conceptual architecture in which IoT sensing, resilient communication, edge computing, AI-based fault analytics, and automated recovery operate as interconnected components of a fault-tolerant industrial automation environment.

2. Literature Review

2.1 Fault Detection in Industrial IoT

Fault detection represents the first stage of an effective fault-tolerance mechanism. It involves determining whether an industrial component, sensor, communication channel, or computing resource has deviated from its expected operating condition. Conventional detection approaches often use fixed thresholds established from engineering specifications. Although threshold-based methods are computationally simple, they can produce false alarms when industrial operating conditions change.

Machine learning provides a more adaptive alternative because models can learn relationships between operational variables and equipment states. The study on IIoT embedded devices demonstrated this approach by using machine-learning models to detect and classify common faults from energy, processing, and application-related measurements. Its reported results showed that machine learning can achieve high detection and classification performance using measurements that can be obtained from embedded industrial devices this development is important because industrial IoT devices frequently operate under resource constraints. A fault-detection model that requires excessive computational resources may not be appropriate for deployment directly on an industrial edge device. Consequently, current research increasingly considers the balance between prediction accuracy, computational complexity, memory requirements, and response latency.

2.2 Machine Learning for Predictive Maintenance

Predictive maintenance is closely connected to fault tolerance because it attempts to identify equipment deterioration before complete failure occurs. Instead of maintaining equipment according to a fixed schedule, predictive maintenance uses condition information to determine when maintenance is actually required.

Recent research demonstrates the use of Random Forest, Support Vector Machines, neural networks, and gradient-boosting models for IIoT predictive maintenance. Comparative studies indicate that different algorithms offer different advantages depending on prediction accuracy, computational complexity, scalability, and real-time requirements (Giorgianni et al., 2025).

(Varalakshmi and Kumar 2025) further investigated predictive maintenance for streaming IIoT data through an ensemble framework involving Deep Reinforcement Learning, Random Forest, and Gradient Boosting. Their work demonstrates the potential for adaptive AI models to respond to continuously changing industrial conditions and optimize maintenance decisions rather than relying exclusively on static predictions.

2.3 Deep Learning for Industrial Fault Diagnosis

Deep learning has become an important research direction because industrial faults are frequently represented by complex time-series, vibration, acoustic and multivariate sensor patterns. Deep neural networks can learn features directly from raw or minimally processed data, reducing the dependence on manually designed features.

(Saeed et al. 2025) reviewed deep-learning approaches for intelligent industrial machinery health management and highlighted intelligent fault diagnosis, remaining-useful-life prediction, and edge-based architectures as important areas of research. Their review also identifies the problem of limited and imbalanced industrial fault data, which can affect the ability of deep-learning models to generalize to real-world operating conditions.

Similarly, recent research on deep-learning predictive maintenance in IIoT applications considers CNNs for sensor-pattern analysis, RNN-based models for temporal prediction, and hybrid approaches for improving maintenance decisions. The research emphasizes that AI-enabled predictive maintenance can improve operational efficiency but must address data quality, interpretability, scalability, and deployment challenges

2.4 Edge Computing and Real-Time Fault Detection

Industrial automation applications often require immediate responses. A delay between the occurrence of a fault and the execution of a corrective action can result in equipment damage or production disruption. Edge computing addresses this problem by moving computation closer to sensors and machines.

Recent research integrating IoT, machine learning, and edge computing for predictive-maintenance anomaly detection demonstrates that relatively lightweight statistical features can support responsive fault detection in resource-constrained IoT environments. This suggests that not every industrial fault-tolerance application requires a large deep-learning model; carefully selected lightweight algorithms may be more suitable when low latency and limited computing resources are priorities

Edge intelligence can therefore complement cloud computing. The edge can perform immediate fault detection and preliminary diagnosis, while the cloud can support historical analysis, model training, long-term maintenance planning, and centralized monitoring.

2.5 AI-Based Anomaly Detection

Anomaly detection is particularly useful when labelled examples of every possible fault are unavailable. In many industrial environments, normal operating data are abundant while actual failure events are relatively rare. Unsupervised and semi-supervised learning can therefore be used to learn normal system behavior and identify deviations.

AI-based anomaly detection can be applied to sensor values, machine vibration, energy consumption, network traffic, communication latency, packet-loss rates, and device behavior. The ability to identify previously unseen abnormalities is especially important in fault-tolerant systems because not all industrial failures can be predicted during system development.

The increasing use of computational intelligence for IoT reliability further supports this direction. Recent research reviews machine learning, deep learning, and evolutionary approaches for fault detection, prediction, diagnosis, and fault tolerance, emphasizing the need for intelligent approaches capable of handling distributed and heterogeneous IoT environments

2.6 AI and Network-Level Fault Tolerance

Equipment reliability alone cannot guarantee reliable industrial automation. Communication networks must also remain operational when individual links or nodes fail. Network-level fault tolerance involves redundancy, alternative routing, load balancing, link monitoring, and rapid recovery.

AI can contribute by learning network behavior and predicting congestion or link degradation. When a communication path becomes unreliable, an intelligent controller can select an alternative route before communication is completely interrupted. Such approaches can be integrated with programmable networking technologies to provide adaptive network recovery.

The broader development of AI-based fault tolerance in IoT also supports this approach by combining intelligent prediction with distributed recovery mechanisms. Recent research on robust federated learning and computational intelligence emphasizes that reliability in distributed IoT systems requires mechanisms capable of addressing device failures, communication problems, and dynamic operating conditions rather than concentrating on a single component.

2.7 AI, IoT and Intelligent Quality Control

Fault tolerance also contributes to industrial product quality. An undetected machine or sensor fault can produce defective products even when the production process continues running. Machine learning can analyze production-line sensor information to identify abnormalities and estimate maintenance requirements.

Research presented in demonstrates the integration of machine learning with IIoT quality-control systems, including CNN-based defect detection and recurrent neural networks for predictive maintenance. The work highlights the potential for IoT and machine learning to improve defect coverage, predictive capability, and industrial quality management

2.8 Digital Twins and AI-Based Maintenance

Digital twins provide another emerging direction for intelligent fault tolerance. A digital twin creates a virtual representation of a physical industrial asset or process and can be continuously updated using IoT data. AI can then use the digital representation to simulate possible operating conditions, estimate degradation, and evaluate maintenance strategies.

Recent research on digital-twin-driven predictive maintenance shows a movement from conventional machine-learning prediction toward integrated digital representations of industrial systems. This approach can potentially allow maintenance decisions to be evaluated virtually before being implemented on physical machinery.

2.9 Research Gap

The reviewed literature demonstrates significant progress in AI-based fault detection, predictive maintenance, anomaly detection, and intelligent industrial monitoring. However, several gaps remain.

First, many studies focus primarily on equipment fault diagnosis rather than considering the equipment, IoT devices, communication network, and edge infrastructure as one integrated fault-tolerant system.

Second, many AI models concentrate on detecting faults but provide limited mechanisms for automated recovery after detection. Detecting a fault is not sufficient for industrial automation; the system must also determine how to maintain operation.

Third, industrial AI research continues to face data scarcity and class imbalance because actual failure events are less frequent than normal operating conditions. This limits model generalization to unknown faults.

Fourth, there is a continuing need for lightweight AI models capable of operating directly on edge devices with limited computational and energy resources.

Finally, more research is required on the integration of AI, edge computing, resilient networking, redundancy, predictive maintenance, and automated recovery into a unified fault-tolerant architecture.

The proposed study addresses these gaps by conceptualizing an AI-enabled architecture in which industrial IoT data are continuously monitored, analyzed at the edge and or cloud, used to detect and predict faults, and subsequently connected to intelligent recovery mechanisms.

3. Role of Artificial Intelligence in Fault-Tolerant IoT Networks

Artificial intelligence strengthens conventional fault-tolerance techniques by enabling systems to learn from historical and real-time operational data.

3.1 AI-Based Fault Detection

Machine-learning algorithms can learn normal operating patterns and identify deviations. Classification algorithms such as Random Forest, Support Vector Machine, Decision Tree, and neural networks can classify devices or equipment according to their operational states.

For example, sensor measurements such as temperature, vibration, pressure, current, and rotational speed can be transformed into features that are supplied to an ML model. The model can then classify the equipment as normal, degraded, or faulty.

Research on IIoT embedded devices has demonstrated the effectiveness of machine learning based fault detection and classification using operational features such as energy consumption and processing behavior.

3.2 AI-Based Anomaly Detection

Anomaly detection is particularly valuable when labeled failure data are limited. An AI model can establish a representation of normal network or equipment behavior and identify unusual deviations.

Unsupervised and semi-supervised approaches are useful because industrial systems may experience many normal operating conditions but relatively few actual failures.

AI-based anomaly detection can identify:

i. unusual sensor readings
ii. abnormal network traffic

iii. unexpected device behavior
iv. sudden increases in latency
v. packet-loss abnormalities
vi. abnormal energy consumption
vii. unusual vibration patterns
viii. Potential cyber intrusions.

3.3 Predictive Maintenance

Predictive maintenance is one of the most important applications of AI in industrial fault tolerance. Instead of waiting for equipment failure, machine-learning models analyze historical and real-time sensor information to estimate equipment health and potential failure.

The basic process can be represented as:

Sensor Data → Data Processing → Feature Extraction → AI Model → Fault Probability → Maintenance Decision

3.4 AI for Intelligent Network Recovery

AI can also assist in determining the best recovery strategy when a network component fails. The system may select an alternative route, redistribute traffic, migrate computation to another edge node, or temporarily deactivate a faulty device.

SDN provides an important foundation for this approach because network conditions can be centrally monitored and network routes dynamically modified. Recent research proposed dynamic route protection for IIoT and demonstrated improvements in failure recovery, delay, packet loss, and packet delivery performance.

3.5 AI at the Edge

Sending every industrial data stream to a remote cloud server can introduce latency and create a dependency on network connectivity. Edge computing addresses this problem by placing computational resources close to the industrial equipment.

AI models deployed at the edge can therefore detect faults and initiate recovery actions locally. Research reviewing AI and edge computing for machine maintenance identifies reduced latency, improved availability, and reduced dependence on centralized processing as important advantages of edge-based industrial intelligence.

4. Proposed AI-Enabled Fault-Tolerant Architecture

The proposed architecture integrates IoT devices, resilient communication, edge computing, AI analytics, and automated recovery.

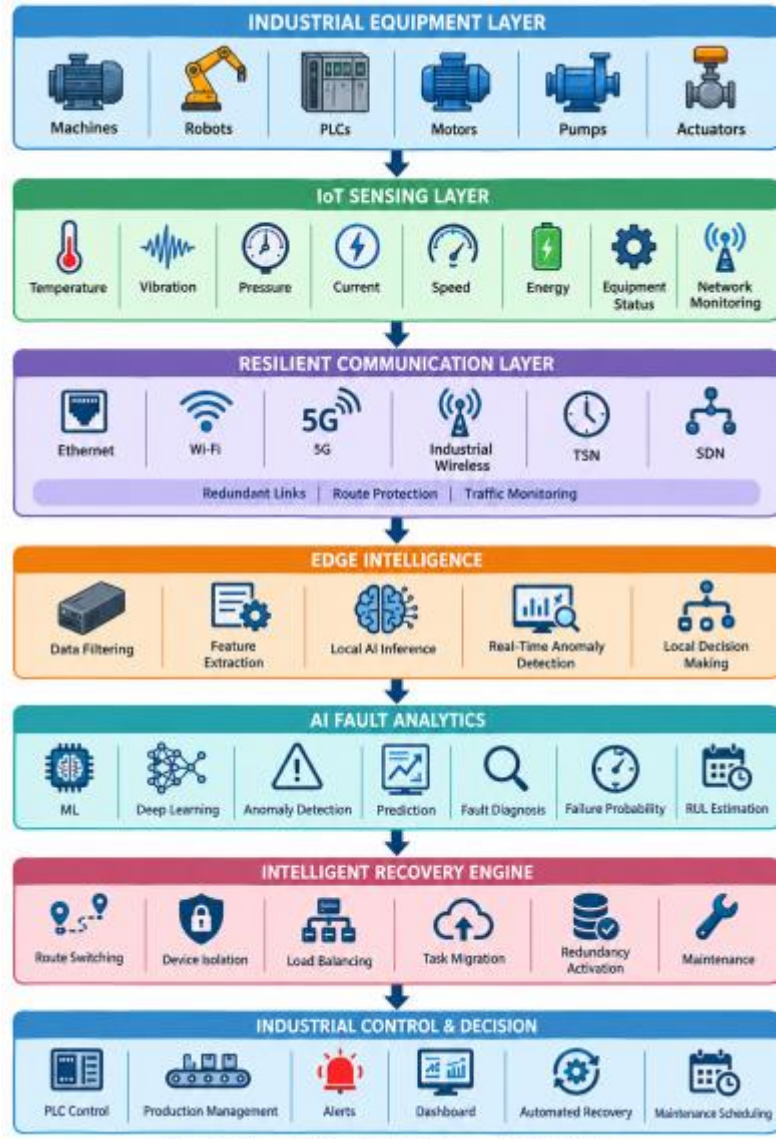


Figure 1. Proposed AI-Enabled Fault-Tolerant IoT Architecture

The architecture consists of seven major layers.

4.1 Industrial Equipment Layer

This layer contains physical industrial assets such as motors, pumps, robotic arms, conveyor systems, production machines, PLCs and actuators. These devices are the primary sources and targets of operational faults.

4.2 IoT Sensing Layer

Sensors continuously capture the condition of equipment. Typical variables include vibration, temperature, pressure, voltage, current, rotational speed, acoustic signals and energy consumption.

4.3 Resilient Communication Layer

The communication layer connects industrial equipment with gateways and computing resources. Technologies can include industrial Ethernet, Wi-Fi, 5G, time-sensitive networking and industrial wireless technologies.

Redundant communication paths should be provided for critical applications so that a failed link does not completely disconnect an industrial device.

4.4 Edge Intelligence Layer

The edge layer performs rapid processing close to the source of data. It filters noisy information, extracts relevant features and performs local AI inference.

This layer is particularly important for time-sensitive industrial applications because the system can continue detecting faults even when cloud connectivity is temporarily unavailable.

4.5 AI Fault Analytics Layer

This layer performs:

i. fault classification
ii. anomaly detection
iii. failure prediction
iv. remaining useful life estimation
v. network fault prediction
vi. equipment health assessment
vii. cyber-threat detection

4.6 Intelligent Recovery Layer

After identifying a fault, the system selects a suitable recovery action. Possible actions include switching to a redundant communication path, isolating a defective device, redistributing network traffic, migrating an edge task, restarting a software component, or notifying maintenance personnel.

4.7 Industrial Control Layer

The final layer communicates the recovery decision to industrial control systems and human operators. Where appropriate, automated recovery can be performed without waiting for human intervention.

5. AI Techniques for Fault-Tolerant Industrial IoT

AI Technique	Fault-Tolerance Application	Expected Benefit
Decision Trees	Fault classification	Simple and interpretable diagnosis
Random Forest	Equipment and sensor fault prediction	Robust classification
Support Vector Machine	Fault detection	Effective classification with limited data
K-Means	Anomaly identification	Detection of abnormal operating clusters
Autoencoders	Unsupervised anomaly detection	Identification of unknown faults
CNN	Vibration/image/signal analysis	Automated feature extraction
LSTM	Time-series fault prediction	Captures temporal behaviour
Reinforcement Learning	Adaptive routing and recovery	Dynamic decision-making
Federated Learning	Distributed fault diagnosis	Privacy-preserving collaborative learning
Digital Twins + AI	Simulation and predictive maintenance	Improved prediction and decision support

6. Fault-Tolerance Mechanisms

6.1 Redundancy

Redundancy involves maintaining additional devices, sensors, links, servers, or routes that can take over when the primary component fails.

For example:

Primary Sensor → Fault → Backup Sensor → Continued Monitoring

Redundancy remains particularly important for safety-critical industrial processes.

6.2 Dynamic Routing

Network failures can be handled by dynamically selecting alternative communication routes. AI can predict congestion or link degradation and proactively move traffic before complete failure occurs.

This approach can be combined with SDN because SDN provides centralized visibility and programmable network control. Recent research demonstrates the value of dynamic route protection in IIoT fault recovery.

6.3 Predictive Failure Detection

AI can estimate the probability that a device will fail within a particular period. This allows maintenance personnel to intervene before the fault causes production interruption.

6.4 Load Balancing

When an edge server becomes overloaded or begins showing abnormal behavior, workloads can be transferred to another edge node. Recent research specifically addresses reliable task offloading under edge-server failures in IIoT environments.

6.5 Automatic Device Isolation

If AI identifies a defective or compromised IoT device, the system can isolate it from the network while maintaining operation through redundant components.

6.6 Self-Healing

Self-healing refers to the ability of an industrial network to automatically detect a fault, determine an appropriate response, execute recovery, and verify that normal operation has been restored.

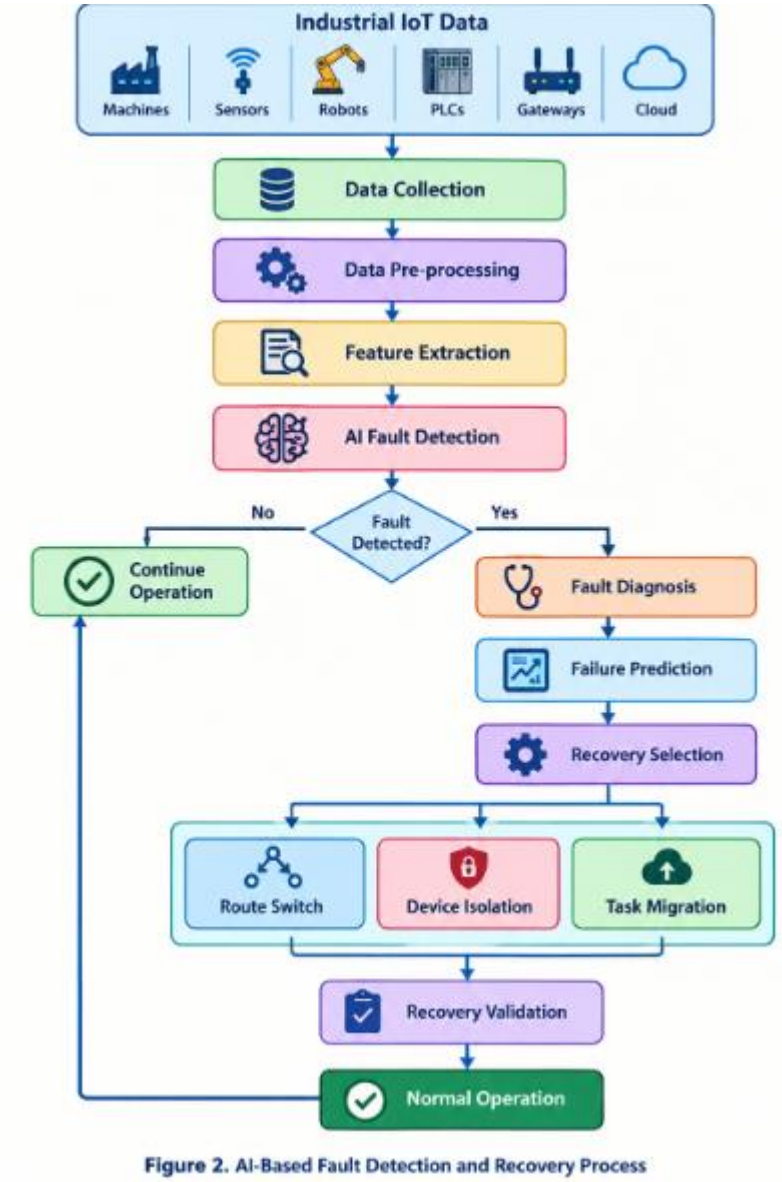


Figure 2. AI-Based Fault Detection and Recovery Process

7. Proposed Fault-Tolerance Workflow

The workflow begins with continuous data collection from industrial equipment and network components. Data preprocessing removes noise and missing or inconsistent observations. Relevant features are then extracted and supplied to an AI model.

If the system identifies normal behavior, industrial operations continue. When an anomaly is detected, the AI system determines whether the anomaly represents a sensor fault, equipment fault, communication fault, edge-computing fault, or possible cyber attack.

The recovery engine subsequently selects the most appropriate response. For example, a communication failure can trigger route switching, while an edge-server failure can trigger task migration. After recovery, the system verifies whether performance has returned to an acceptable level.

8. Benefits of AI-Based Fault Tolerance

8.1 Reduced Downtime

Predicting equipment failures before catastrophic breakdown can reduce unexpected production interruptions.

8.2 Improved Network Reliability

Intelligent routing and redundancy allow communication to continue when network components fail.

8.3 Faster Fault Detection

Edge AI enables faults to be detected close to the source rather than waiting for data to travel to a remote cloud platform.

8.4 Improved Maintenance Planning

AI-based predictive maintenance allows organizations to schedule interventions based on actual equipment conditions.

8.5 Reduced Maintenance Cost

Replacing components only when their condition indicates a significant risk can reduce unnecessary maintenance activities.

8.6 Improved Safety

Early detection of abnormal temperature, pressure, vibration, electrical conditions, or network behaviour can help prevent dangerous industrial situations.

8.7 Adaptive Industrial Operations

AI allows recovery strategies to adapt to changing network and equipment conditions rather than depending entirely on static rules.

9. Challenges

Despite its potential, AI-enabled fault tolerance presents several challenges.

9.1 Poor Data Quality

AI models depend heavily on the quality of sensor data. Missing, noisy, biased, or incorrectly labelled data can reduce diagnostic performance.

9.2 Limited Fault Data

Real industrial failures are relatively rare compared with normal operations. Consequently, datasets may contain insufficient examples of important fault conditions.

9.3 Model Explainability

Industrial operators may be reluctant to trust a model that recommends a critical recovery action without explaining why the action is necessary.

9.4 Computational Constraints

Industrial IoT devices and edge nodes may have limited memory, processing power, and energy resources. Large deep-learning models may therefore be difficult to deploy directly at the edge.

9.5 Cyber security

An AI-enabled fault-tolerance system can itself become a target for attackers. Attackers may manipulate sensor data, poison training data, compromise models, or deliberately generate false anomalies.

Recent research on industrial control systems has consequently investigated combinations of federated learning and zero-trust architectures to address security and distributed learning requirements.

9.6 Interoperability

Industrial environments commonly contain equipment from different manufacturers using different communication protocols and data formats. Integrating AI-based fault tolerance into these heterogeneous environments remains difficult.

9.7 Real-World Validation

Many AI fault-diagnosis studies are validated using laboratory datasets or simulated environments. Industrial deployment requires validation under realistic conditions involving

noise, changing workloads, equipment ageing, communication interference, and unexpected failures.

9.8 Human AI Collaboration

10. Future Research Directions

Future research on AI enabled fault tolerance in industrial IoT should concentrate on the following areas.

First, explainable AI should be developed so that industrial engineers can understand why an AI system has classified a device as faulty or selected a particular recovery action.

Second, federated learning should receive greater attention because industrial organizations may be unwilling to transfer sensitive operational data to centralized servers. Federated approaches can allow models to learn from distributed industrial environments while limiting direct data sharing. Research has already demonstrated federated approaches for fault diagnosis across different machine domains.

Third, AI-enabled digital twins provide an important opportunity. A digital twin can simulate equipment behavior and allow AI models to examine possible failure scenarios before implementing recovery actions on physical equipment. Recent systematic research identifies AI-enhanced digital twins as an emerging direction for intelligent maintenance.

Fourth, self-healing industrial networks should combine AI prediction with programmable networking, redundancy, edge computing, and automated recovery.

Fifth, lightweight AI models are required for deployment on resource-constrained industrial edge devices.

Sixth, standardized industrial datasets and benchmarks should be developed. The lack of suitable benchmark datasets remains a significant challenge in industrial predictive-maintenance research.

11. Contribution to Knowledge

This paper contributes to the field by presenting a conceptual framework that combines AI-based fault detection, predictive maintenance, resilient networking, edge intelligence, and automated recovery within a unified industrial IoT architecture.

The major contributions are:

i. **An integrated AI-enabled fault-tolerance architecture** for industrial IoT networks.
ii. **Integration of equipment and network fault detection** rather than concentrating only on machine failure.

iii. **Combination of edge AI and intelligent recovery** to reduce response latency.

iv. **Integration of predictive maintenance with network resilience** to support proactive fault management.

v. **Identification of important research challenges**, including explain ability, cyber security, data scarcity, interoperability, and real-world validation.

vi. **A foundation for self-healing industrial IoT networks** capable of detecting, diagnosing, recovering from, and learning from faults.

12. Conclusion

Fault tolerance is a critical requirement for Industrial IoT networks supporting modern industrial automation. Increasing connectivity among machines, sensors, controllers, robots, gateways, edge servers, and cloud systems creates new opportunities for intelligent production but also introduces additional points of failure. Conventional fault-tolerance techniques such as redundancy, backup components, static routing, and preventive maintenance remain important, but they are increasingly complemented by AI-driven methods.

Artificial intelligence can enable industrial systems to identify abnormal behavior, predict equipment degradation, diagnose faults, optimize communication routes, balance computational workloads, and initiate recovery actions. The integration of AI with edge computing is particularly valuable because it enables rapid local decision-making and reduces dependence on remote cloud infrastructure. Similarly, SDN, redundant communication paths, federated learning, and digital twins can extend fault tolerance from individual devices to the wider industrial network.

Recent research confirms that AI, IoT, edge computing, predictive maintenance, and intelligent networking are converging toward more resilient industrial systems. However, practical deployment remains constrained by data scarcity, model explain ability, cyber security, computational limitations, interoperability, and limited validation under real industrial conditions. Therefore, future research should focus on explainable and lightweight AI, federated learning, digital twins, self-healing networks, standardized industrial datasets, and human–AI collaboration.

Article Publication Details
This article is published in the **International Journal of Multidisciplinary Research and Bulletin**, ISSN 3108-1428 (Online). In Volume 5 Issue 5 (Sep – Oct) 2026.
The journal is published and managed by **IRPG**.

Acknowledgements
We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

Funding
The authors declare that no funding was received for this work.

Data availability
No datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate
The author(s) declare that it is not applicable.

Consent for publication
The author(s) declare that this is not applicable.

Competing interests
The author(s) declare that they have no competing interests.

References

1. Borriello, P., Tessicini, F., Ricucci, G., Frosina, E., et al. (2024). A fault detection strategy for an ePump during EOL tests based on a knowledge-based vibroacoustic tool and supervised machine learning classifiers. *Meccanica, 59,* 279–304. https://doi.org/10.1007/s11012-024-01754-w
2. Chen, S., Turanoglu Bekar, E., Bokrantz, J., & Skoogh, A. (2025). AI-enhanced digital twins in maintenance: Systematic review, industrial challenges, and bridging research-practice gaps. *Journal of Manufacturing Systems, 82,* 678–699. https://doi.org/10.1016/j.jmsy.2025.07.006
3. Dadfarnia, M., Sharp, M. E., & Herrmann, J. W. (2025). Comprehensive evaluations of condition monitoring-based technologies in industrial maintenance: A systematic review. *Journal of Manufacturing Systems, 82,* 449-477. https://doi.org/10.1016/j.jmsy.2025.06.015
4. Hirsi, A., Audah, L., Salh, A., Alhartomi, M., Sun, Z., Hammoodi, A., & Ahmed, S. (2025). Artificial intelligence performance evaluation for URLLC of industrial IoT applications: A review, open challenges and future directions. *Physical Communication*. https://doi.org/10.1016/j.phycom.2025.102712

5. Li, P. (2024). A multi-scale attention-based transfer model for cross-bearing fault diagnosis. *International Journal of Computational Intelligence Systems*. https://doi.org/10.1007/s44196-024-00414-x
6. Lima, J., et al. (2025). Systematic review of predictive maintenance practices in the manufacturing sector. *Intelligent Systems with Applications, 26*, 200501. https://doi.org/10.1016/j.iswa.2025.200501
7. Prakash, V., Odedina, O., Kumar, A., Garg, L., & Bawa, S. (2024). A secure framework for the Internet of Things anomalies using machine learning. *Discover Internet of Things, 4*, 33. https://doi.org/10.1007/s43926-024-00088-z
8. Ramzan, F., & Reforgiato Recupero, D. (2025). A literature review on enhancing predictive maintenance in smart manufacturing industries: Fostering human-technology collaboration and overcoming data scarcity limitations with advanced AI models. *Operations Research Forum, 6*, 181. https://doi.org/10.1007/s43069-025-00584-0
9. Seba, A. M., Gemeda, K. A., & Ramulu, P. J. (2024). Prediction and classification of IoT sensor faults using hybrid deep learning model. *Discover Applied Sciences, 6*, 9. https://doi.org/10.1007/s42452-024-05633-7
10. Wang, et al. (2023). Federated domain generalization: A secure and robust framework for intelligent fault diagnosis. *IEEE Transactions on Industrial Informatics, 20*(2), 2662–2670. https://doi.org/10.1109/TII.2023.3296894
11. Yang, Y., Chen, Y., Chen, N., & Chen, J. (2025). ESFMTO: A reliable task offloading strategy based on edge server failure model in IIoT. *Ad Hoc Networks, 176*, 103887. https://doi.org/10.1016/j.adhoc.2025.103887
12. "Industrial IoT embedded devices fault detection and classification: A case study." (2024). *Internet of Things, 25*, 101042. https://doi.org/10.1016/j.iot.2023.101042
13. "Industrial IoT regulated by Software-Defined Networking platform for fast and dynamic fault tolerance application." (2024). *Simulation Modelling Practice and Theory, 135*, 102963. https://doi.org/10.1016/j.simpat.2024.102963
14. "Machine Learning-driven Quality Control Strategies for Industrial IoT Applications." (2024). *2024 4th Asian Conference on Innovation in Technology*. https://doi.org/10.1109/ASIANCON62057.2024.10837745

15. "An adaptive backoff algorithm for enhanced MAC-layer security and operational efficiency in IoT and cyber–physical systems." (2025). *Internet of Things, 32,* 101641. https://doi.org/10.1016/j.iot.2025.101641
16. "Collaborative fault tolerance for cyber–physical systems: The detection stage." (2025). *Computers in Industry, 166,* 104253. https://doi.org/10.1016/j.compind.2025.104253
17. "A literature review framework and open research challenges for predictive maintenance in Industry 4.0." (2025). *Computers & Industrial Engineering, 206,* 111193. https://doi.org/10.1016/j.cie.2025.111193
18. "Application-wise review of machine learning-based predictive maintenance: Trends, challenges, and future directions." (2025). *Applied Sciences, 15*(9), 4898. https://doi.org/10.3390/app15094898
19. "Techniques in reliability of Internet of Things (IoT)." (2025). *Procedia Computer Science, 256,* 55–62. https://doi.org/10.1016/j.procs.2025.02.095
20. "An asynchronous federated learning based zero trust architecture for the next generation industrial control systems." (2025). *Computer Networks, 269,* 111459. https://doi.org/10.1016/j.comnet.2025.111459
21. "Alpha-Net: A dependable and trustworthy deep learning framework for securing industrial internet of things networks against botnet attacks." (2026). *Computers & Electrical Engineering, 131,* 110919. https://doi.org/10.1016/j.compeleceng.2025.110919

Publisher's Note:
IRPG remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of IRPG and/or the editor(s). IRPG disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.