

Smart IoT Frameworks for Real-Time Industrial Monitoring and Control

Zoran Salcic

Professor, University of Auckland, New Zealand

Abstract

The rapid development of the Industrial Internet of Things (IIoT) has transformed conventional industrial environments into interconnected, data-driven, and increasingly intelligent systems. Real-time industrial monitoring and control require frameworks capable of collecting heterogeneous operational data, processing information with low latency, identifying abnormal conditions, and supporting timely control decisions. This paper examines smart IoT frameworks for real-time industrial monitoring and control, with particular emphasis on sensing technologies, communication networks, edge computing, cloud platforms, artificial intelligence, cyber-physical systems, and intelligent control mechanisms. A conceptual literature-based methodology is adopted to examine the technological components, operational contributions, sustainability benefits, implementation challenges, and future research directions associated with smart industrial IoT frameworks. Existing research indicates that IoT-enabled manufacturing can support predictive maintenance, process monitoring, energy management, quality control, inventory visibility, and production optimization. Edge computing further strengthens real-time industrial applications by moving selected analytical processes closer to data sources, thereby reducing latency and dependence on centralized computing environments.

The analysis identifies a layered architecture consisting of physical sensing, connectivity, edge intelligence, cloud or platform services, analytics, and control applications. Such architecture enables continuous interaction between industrial assets and digital decision-support systems. However, implementation remains constrained by cybersecurity threats, interoperability problems, heterogeneous devices, data quality, network reliability, computational limitations, and workforce requirements. Recent research has emphasized the growing security requirements of IIoT environments and the importance of hierarchical security architectures for industrial edge systems. The paper concludes that effective smart IoT frameworks should combine real-time sensing, low-latency processing, intelligent analytics, secure communication, adaptive control, and human oversight. The proposed perspective provides a foundation for developing resilient and scalable industrial monitoring and control environments capable of supporting intelligent manufacturing and digitally integrated industrial operations.

Keywords: Internet of Things, Industrial IoT, Real-Time Monitoring, Industrial Control, Edge Computing, Smart Manufacturing, Cyber-Physical Systems, Intelligent Automation.

1. Introduction

The Internet of Things (IoT) has become an important technological foundation for transforming conventional industrial environments into connected and intelligent systems. Industrial machines, sensors, controllers, production equipment, and information platforms can now exchange operational information through interconnected communication infrastructures. This connectivity enables

organizations to observe industrial processes continuously rather than depending exclusively on periodic inspections or manually collected information. Industrial IoT (IIoT) therefore provides an important foundation for real-time monitoring, predictive maintenance, process optimization, quality management, and intelligent production control.

The development of smart manufacturing has accelerated the integration of IoT with artificial intelligence, cloud computing, big-data analytics, cyber-physical systems, and automation. Research on intelligent manufacturing identifies IoT, cyber-physical systems, cloud computing, big-data analytics, and information and communication technologies as major components of modern intelligent manufacturing environments. These technologies enable industrial systems to collect information from physical processes and transform it into actionable intelligence. Consequently, monitoring is increasingly evolving from simple data visualization toward prediction, anomaly detection, optimization, and automated decision-making.

Real-time industrial monitoring is particularly important in environments where small variations in temperature, vibration, pressure, speed, energy consumption, or production parameters can influence equipment performance and product quality. IoT sensors can continuously capture such variables and transmit them to analytical platforms. Industrial IoT applications have been identified in predictive maintenance, energy monitoring, asset tracking, inventory management, quality control, and production-process monitoring. Continuous monitoring can allow organizations to identify deviations earlier, reduce downtime, and improve operational visibility.

However, centralized IoT architectures can create challenges for time-sensitive industrial applications. Sending every sensor observation to a remote cloud platform may introduce communication delays and increase network dependence. Edge computing addresses this issue by placing computational resources closer to industrial data sources. Research on AI and edge computing for machine maintenance highlights the ability of edge processing to reduce latency and support faster machine-health analysis while also identifying challenges associated with deploying AI on resource-constrained edge devices.

Industrial control introduces additional requirements because monitoring information must often be translated into timely operational actions. A smart framework should therefore establish a reliable connection between sensing, communication, analytics, decision-making, and control. Smart manufacturing research has demonstrated the relevance of IoT-enabled systems for smart monitoring, smart control, scheduling, and machining. The integration of these functions creates a cyber-physical environment in which physical processes and digital intelligence continuously interact.

Security is another critical dimension of smart IoT frameworks. Increased industrial connectivity expands the attack surface and creates potential risks to data confidentiality, system integrity, availability, and physical operations. A 2024 survey of IIoT security emphasizes the importance of security requirements and cryptographic techniques in connected industrial environments. Therefore, real-time monitoring and control frameworks must incorporate security mechanisms from the architecture-design stage rather than treating cybersecurity as an additional feature.

This paper examines smart IoT frameworks for real-time industrial monitoring and control. It focuses on the architecture, technologies, operational applications, benefits, implementation challenges, and future research requirements of smart industrial IoT environments. The paper develops an integrated perspective in which sensing, connectivity, edge intelligence, cloud platforms, analytics, and control operate as interconnected components of a real-time industrial ecosystem.

2. Objectives

2.1 Examination of Smart IoT Architecture

The first objective is to examine the major architectural components required for real-time industrial monitoring and control. The study considers industrial sensors, communication networks, edge gateways, cloud platforms, data-management systems, analytics engines, and control interfaces. Particular attention is given to the relationship between these layers and their contribution to continuous industrial visibility. The objective is to identify how architectural integration can improve responsiveness, scalability, reliability, and operational intelligence.

The objective also includes examining the role of edge computing in time-sensitive industrial applications. Edge processing can reduce the amount of information transferred to centralized systems and enable selected analytical functions closer to machines and sensors. This capability is particularly important when industrial decisions require low latency. Recent research on industrial edge environments has consequently emphasized hierarchical architectures and security mechanisms across different system layers.

2.2 Assessment of Monitoring and Control Capabilities

The second objective is to assess how smart IoT frameworks improve real-time industrial monitoring and control. The assessment considers equipment health monitoring, anomaly detection, predictive maintenance, production-process optimization, quality control, energy monitoring, and adaptive control. IoT-enabled smart factories have demonstrated applications across several of these areas, including predictive maintenance, energy efficiency, quality control, and production monitoring.

The objective further considers how real-time information can support more responsive industrial decisions. Instead of relying on historical reports, organizations can use continuous data streams to identify emerging problems and modify operational parameters. This transition from reactive to predictive and adaptive management represents an important contribution of smart IoT architectures to Industry 4.0.

3. Literature Review

3.1 Industrial IoT and Smart Manufacturing

Industrial IoT extends conventional IoT concepts into industrial environments where connected devices must operate under demanding requirements related to reliability, availability, safety, and response time. IIoT connects machines, sensors, controllers, enterprise systems, and industrial applications to facilitate continuous information exchange. The resulting environment supports data-driven manufacturing and enables greater visibility into production operations.

Zhong et al. identified IoT-enabled manufacturing, cyber-physical systems, cloud computing, big-data analytics, and ICT as important technologies supporting intelligent manufacturing. Zheng et al. similarly proposed a smart manufacturing framework incorporating IoT, cloud computing, big data, AI, and CPS technologies for smart monitoring, control, scheduling, and machining. These findings indicate that IoT is not an isolated technology but a foundational communication layer within broader intelligent manufacturing architectures.

A 2023 review of IoT applications in smart factories identified predictive maintenance, asset tracking, inventory management, quality control, production-process monitoring, energy efficiency, and supply-chain optimization as important industrial applications. Such applications demonstrate the ability

of connected industrial systems to extend monitoring beyond individual machines toward broader production and operational ecosystems.

3.2 Edge Computing for Real-Time Industrial Operations

Edge computing has emerged as a complementary technology for IIoT because industrial applications frequently require rapid processing of sensor information. Traditional cloud architectures can provide significant computational capacity but may introduce communication delays when data must travel from industrial sites to remote servers. Edge architectures distribute computational capabilities closer to sensors, machines, and gateways.

AI-enabled edge computing is particularly relevant for machine maintenance. Research indicates that edge-based processing can address some of the latency, privacy, and availability limitations associated with centralized computing. Edge intelligence can support anomaly detection, equipment-health assessment, local optimization, and rapid response while sending only selected information to cloud platforms.

Edge computing can also reduce network traffic by filtering and aggregating sensor data before transmission. However, edge devices typically have more limited computational and storage capabilities than centralized data centers. Therefore, efficient algorithms, lightweight models, resource allocation, and distributed intelligence remain important research requirements.

3.3 IoT-Based Monitoring and Intelligent Control

Real-time monitoring provides the information foundation for intelligent control. Industrial sensors can capture variables such as temperature, pressure, vibration, current, speed, humidity, flow, and machine-state indicators. Analytical systems can then transform these observations into operational information. Smart manufacturing research identifies smart monitoring and smart control as important scenarios within Industry 4.0 environments.

Smart production planning and control research has also examined how Industry 4.0 technologies create new capabilities for planning and control activities. A systematic review of 102 studies identified numerous smart capabilities and performance indicators associated with Industry 4.0 production planning and control. These findings demonstrate that IoT-based monitoring can contribute to both operational visibility and higher-level production decision-making.

4. Methodology

4.1 Research Design

This study adopts a conceptual and literature-based research design to examine smart IoT frameworks for real-time industrial monitoring and control. The research synthesizes existing academic literature on IIoT, smart manufacturing, edge computing, industrial automation, cyber-physical systems, intelligent analytics, and industrial cybersecurity. The literature is organized according to technological architecture, monitoring capability, control functionality, performance contribution, implementation challenge, and future research requirements. This approach enables the study to integrate findings from different technological perspectives into a unified framework.

The research focuses on the relationship between connected industrial assets and intelligent decision-making. Particular attention is given to the flow of information from sensors through communication networks and computational layers toward monitoring dashboards, analytics platforms,

and control mechanisms. Existing literature indicates that IoT, CPS, cloud computing, and data analytics form interconnected foundations for intelligent manufacturing.

4.2 Smart IoT Framework Components

The proposed conceptual framework consists of six interconnected layers: physical industrial assets, sensing, communication, edge intelligence, cloud or platform intelligence, and application/control. The physical layer includes machines and production equipment. The sensing layer captures operational conditions, while the communication layer transfers information. Edge intelligence provides low-latency processing, and cloud platforms provide scalable storage and advanced analytics. The application layer supports monitoring, prediction, visualization, and control.

The architecture is designed around a continuous feedback process. Sensor data are collected from industrial assets, processed at appropriate computational levels, analyzed to identify operational conditions, and transformed into decisions or control actions. The resulting system response generates new operational data that can be used for further analysis. This feedback mechanism enables continuous adaptation and supports the transition from static monitoring toward intelligent industrial control.

Key Framework Components

- **Industrial assets:** Machines, production lines, equipment, robots, and infrastructure.
- **Sensors and actuators:** Data collection and physical-system interaction.
- **Communication layer:** Industrial Ethernet, wireless networks, gateways, and protocols.
- **Edge layer:** Local filtering, anomaly detection, and low-latency analytics.
- **Cloud/platform layer:** Data storage, large-scale analytics, and model management.
- **AI analytics:** Prediction, classification, optimization, and anomaly detection.
- **Monitoring layer:** Dashboards, alerts, and operational visualization.
- **Control layer:** Automated or human-supervised system intervention.
- **Security layer:** Authentication, encryption, access management, and threat detection.

4.3 Analytical Dimensions

The framework is evaluated according to real-time responsiveness, monitoring accuracy, control effectiveness, scalability, reliability, cybersecurity, and resource efficiency. Real-time responsiveness considers whether information can be processed rapidly enough for industrial decision-making. Monitoring accuracy considers the quality and reliability of sensor information and analytical models. Control effectiveness examines whether monitoring outputs can be translated into appropriate operational actions.

Scalability and reliability are important because industrial environments can contain thousands of connected devices. Cybersecurity evaluates the ability of the framework to protect industrial information and operations from unauthorized access or manipulation. Resource efficiency considers network bandwidth, computational requirements, energy consumption, and storage. These dimensions provide a multidimensional basis for evaluating smart IoT frameworks.

5. Analysis

5.1 Architecture of Smart IoT Frameworks

A smart IoT framework for industrial monitoring and control should provide continuous communication between physical assets and digital intelligence. Sensors generate operational observations, gateways aggregate information, and edge devices process time-sensitive data. Cloud or platform-level systems

then provide broader analytics, historical storage, and model management. Monitoring applications present processed information to engineers and operators, while control systems use analytical results to modify operational parameters.

The layered architecture reduces the risk of placing all processing responsibilities on one computational environment. Edge systems can address immediate decisions, while cloud platforms can support computationally intensive analytics and long-term analysis. This hybrid approach is consistent with the increasing integration of IIoT and edge computing for continuous industrial monitoring and management.

Table 1: Architectural Layers of Smart IoT Frameworks for Industrial Monitoring and Control

Layer	Main Components	Primary Function	Industrial Contribution
Physical Layer	Machines, robots, equipment	Industrial operation	Executes production processes
Sensing Layer	Sensors, meters, actuators	Data collection	Captures real-time conditions
Connectivity Layer	Gateways, Ethernet, wireless networks	Data transmission	Enables device communication
Edge Layer	Edge gateways, local processors	Local analytics	Low-latency processing
Platform Layer	Cloud, databases, IoT platforms	Storage and analytics	Large-scale information processing
Intelligence Layer	AI, ML, analytics	Prediction and optimization	Intelligent decision support
Application Layer	Dashboards, alerts, control systems	Visualization and action	Monitoring and industrial control
Security Layer	Encryption, authentication, access control	Protection	Secures industrial operations

Interpretation: Table 1 demonstrates that effective industrial IoT frameworks depend on the coordinated operation of multiple architectural layers. The sensing layer establishes visibility, connectivity enables information exchange, and edge computing provides localized processing. Cloud and platform services provide broader computational capabilities, while AI transforms collected information into predictions and recommendations. The application and control layers convert intelligence into operational action. Security must operate across all layers because IIoT environments expose interconnected industrial systems to broader cybersecurity risks.

5.2 Real-Time Monitoring Capabilities

Real-time monitoring is one of the central functions of smart IoT frameworks. Continuous sensor streams can reveal changes in equipment conditions, production quality, energy consumption, environmental parameters, and process performance. Instead of relying on periodic inspections, operators can receive continuous information and automated alerts when predefined thresholds or learned patterns indicate potential problems.

IoT-enabled smart factories have demonstrated applications in production monitoring, quality control, energy efficiency, predictive maintenance, inventory management, and asset tracking. These capabilities can improve operational visibility and allow industrial organizations to respond more rapidly to abnormal conditions. When combined with AI, monitoring systems can move beyond threshold-based alerts toward predictive identification of emerging failures.

Table 2: Real-Time Industrial Monitoring and Control Applications

Application	IoT Data Sources	Intelligent Function	Expected Outcome
Equipment Monitoring	Vibration, temperature, current	Condition assessment	Reduced equipment failure
Predictive Maintenance	Machine-health indicators	Failure prediction	Reduced downtime
Quality Monitoring	Product and process sensors	Anomaly detection	Improved product quality
Energy Monitoring	Smart meters and equipment sensors	Consumption analysis	Improved energy efficiency
Process Control	Pressure, flow, speed, temperature	Adaptive optimization	Stable production
Safety Monitoring	Environmental and equipment sensors	Hazard detection	Improved workplace safety
Inventory Monitoring	RFID and tracking sensors	Real-time tracking	Improved inventory visibility
Production Monitoring	Machine and line data	Performance analytics	Improved productivity

Interpretation: Table 2 shows that smart IoT frameworks support multiple industrial functions through continuous data collection and intelligent analysis. Equipment monitoring and predictive maintenance focus on reliability, while quality and process monitoring support production performance. Energy and safety applications extend IoT capabilities toward operational sustainability and risk reduction. The integration of monitoring with control mechanisms is particularly important because industrial value is generated when information can be translated into timely and appropriate actions.

5.3 Intelligent Control and Decision Support

Monitoring alone does not constitute a complete smart industrial framework. The information generated by IoT systems must support decisions and, where appropriate, automated control. AI and machine-learning models can analyze sensor data to detect anomalies, predict machine conditions, forecast production requirements, and recommend operational changes. Control systems can then apply approved changes to industrial processes.

Smart production planning and control literature indicates that Industry 4.0 technologies provide new smart capabilities across planning and control activities. Intelligent control can therefore operate at multiple levels, ranging from automatic adjustment of machine parameters to higher-level optimization of production schedules.

A hybrid human-machine approach is especially valuable in safety-critical industrial environments. Automated control can respond rapidly to predefined conditions, while human operators retain responsibility for complex decisions, exceptional situations, and system supervision. This balance can improve reliability while reducing the risks associated with fully autonomous decision-making.

6. Discussion

6.1 Real-Time Intelligence and Industrial Performance

The findings indicate that smart IoT frameworks can significantly improve industrial visibility and responsiveness by establishing continuous connections between physical operations and digital analytical systems. Traditional monitoring methods often provide delayed information, whereas IoT-based frameworks generate continuous streams of operational data. This allows organizations to identify deviations earlier and initiate corrective actions before minor problems become major operational failures.

The integration of AI further strengthens this capability. Instead of simply identifying whether a parameter exceeds a threshold, intelligent systems can learn relationships between multiple variables and estimate future equipment or process conditions. This enables predictive maintenance and proactive control. Research on smart factories confirms the broad application of IoT in predictive maintenance, process monitoring, energy management, and quality control.

6.2 Edge-Cloud Integration

Edge-cloud integration provides an effective approach for balancing real-time responsiveness with computational scalability. Edge systems can process time-sensitive information locally, while cloud platforms can store historical data and perform computationally intensive analysis. This architecture can reduce latency and network dependence without eliminating the benefits of centralized data management.

Research on AI and edge computing for machine maintenance emphasizes that centralized computing may face latency, privacy, and availability challenges and identifies edge processing as an important response. Similarly, research on industrial monitoring in the crude-oil sector highlights the potential of integrating IIoT and edge computing for continuous monitoring and management.

6.3 Security and Reliability

The increasing connectivity of industrial environments creates a direct relationship between operational intelligence and cybersecurity. A compromised IoT device can potentially become a pathway toward

other industrial components. Consequently, security mechanisms must be distributed across sensing, connectivity, edge, platform, and application layers.

The 2024 IIoT security literature emphasizes the importance of cryptographic mechanisms and systematic security requirements in industrial IoT environments. Hierarchical industrial edge security research similarly emphasizes architecture-level approaches for identifying and addressing threats across different layers. These findings indicate that cybersecurity should be incorporated into the framework from the beginning rather than added after deployment.

7. Challenges

7.1 Interoperability and Heterogeneous Industrial Devices

Industrial environments contain machines and devices from different manufacturers and generations. Legacy equipment may use proprietary interfaces or communication protocols, while newer equipment may support modern IoT connectivity. Integrating these systems into a unified monitoring framework can therefore be technically difficult. Data formats, communication protocols, naming conventions, and device capabilities may differ substantially.

Interoperability problems can also affect analytics. If information from different devices cannot be combined consistently, the resulting dataset may be incomplete or difficult to interpret. Standardized interfaces, middleware, gateways, semantic models, and interoperable communication protocols are therefore important for scalable smart IoT implementation.

7.2 Cybersecurity and Privacy

Cybersecurity is a major challenge because IIoT environments connect operational technology with digital communication networks. Increasing connectivity expands the potential attack surface and may expose industrial systems to unauthorized access, malware, denial-of-service attacks, data manipulation, and other threats. Research specifically focused on IIoT security confirms the importance of security requirements and cryptographic approaches.

Privacy and data governance are also relevant where industrial data are shared across cloud services, suppliers, or external analytics platforms. Organizations need strong identity management, encryption, secure authentication, access controls, continuous monitoring, and incident-response mechanisms. Security must also account for resource constraints on edge devices.

7.3 Latency, Reliability, and Scalability

Real-time industrial control requires predictable communication and processing performance. Network congestion, unreliable wireless connections, overloaded edge devices, or cloud-service interruptions can reduce system responsiveness. A monitoring framework that cannot provide timely information may be unsuitable for critical control applications.

Scalability presents another challenge. As the number of connected sensors and machines increases, data volumes can grow rapidly. Organizations must therefore design distributed architectures capable of managing large data streams without excessive network and computational requirements. Edge computing can help by processing selected information locally, but resource limitations on edge devices must also be addressed.

8. Future Research

8.1 AI-Enabled Autonomous IoT Control

Future research should investigate advanced AI techniques capable of supporting more adaptive industrial control. Reinforcement learning, deep learning, anomaly detection, and hybrid analytical models could allow IoT frameworks to learn from changing operational conditions. However, future systems should incorporate safety constraints, uncertainty estimation, explainability, and human oversight before being applied to safety-critical industrial processes.

8.2 Edge AI and Distributed Intelligence

Future research should develop lightweight AI models specifically designed for industrial edge environments. Current edge devices may have limited processing power, memory, and energy resources. Model compression, federated learning, efficient neural architectures, and adaptive computation could enable sophisticated intelligence without requiring continuous communication with centralized cloud platforms.

Edge-based industrial intelligence should also be studied as a distributed ecosystem rather than as isolated devices. Multiple edge nodes could collaboratively process information from different production areas while sharing selected analytical outputs with central platforms. This could improve scalability and reduce unnecessary network traffic.

8.3 Secure and Resilient Industrial IoT

Future research should integrate cybersecurity directly into smart IoT architecture. Secure-by-design frameworks should combine device authentication, cryptographic protection, intrusion detection, anomaly detection, secure firmware, and continuous security assessment. Hierarchical security models for industrial edge environments provide a useful direction for protecting different architectural layers.

Research should also examine resilience against simultaneous cyber and physical disruptions. Industrial IoT systems should be capable of detecting abnormal behavior, isolating compromised devices, maintaining essential operations, and recovering safely. This requires stronger integration between cybersecurity, fault tolerance, and industrial control research.

9. Limitations

This study has several limitations. First, it uses a conceptual and literature-based methodology rather than conducting experiments within a physical industrial facility. Therefore, the identified benefits of smart IoT frameworks represent synthesized research findings rather than direct measurements from a particular production environment. Actual performance may vary according to industrial sector, network architecture, equipment age, sensor quality, control requirements, and organizational capabilities.

Second, industrial IoT technologies are highly diverse, and different sectors have different real-time requirements. A framework appropriate for conventional manufacturing may not be directly transferable to chemical processing, energy systems, mining, or other safety-critical environments. Differences in latency requirements, regulatory conditions, communication infrastructure, and cybersecurity requirements can influence implementation outcomes.

Third, the study does not experimentally quantify the costs associated with IoT deployment, edge infrastructure, cybersecurity, device maintenance, data storage, and workforce training. Future empirical research should therefore evaluate smart IoT frameworks through real-world deployments, controlled industrial experiments, quantitative performance benchmarks, and long-term cost-benefit analyses.

10. Conclusion

Smart IoT frameworks provide an important technological foundation for real-time industrial monitoring and control. By connecting industrial machines, sensors, communication networks, edge devices, cloud platforms, analytical systems, and control applications, these frameworks create continuous interaction between physical operations and digital intelligence. The analysis demonstrates that IoT can support equipment monitoring, predictive maintenance, quality control, energy management, process optimization, safety monitoring, and production management. Existing research confirms the growing role of IoT in smart factories and Industry 4.0 environments.

The integration of edge computing is particularly important for industrial environments where low latency and rapid response are required. Edge processing can reduce communication delays and allow selected analytical tasks to occur close to machines and sensors, while cloud platforms can provide large-scale storage and advanced analytics. However, the effectiveness of such frameworks depends on reliable connectivity, interoperability, data quality, computational resources, and appropriate system architecture. Industrial IoT also introduces significant cybersecurity requirements because increased connectivity can expand the attack surface.

Future smart IoT frameworks should therefore move beyond simple device connectivity toward secure, intelligent, adaptive, and resilient industrial ecosystems. AI-enabled analytics, distributed edge intelligence, secure communication, predictive maintenance, and human-supervised control can collectively improve industrial responsiveness and operational efficiency. Security should be integrated across every architectural layer, while interoperability and scalable data management should be treated as fundamental design requirements. When these capabilities are combined within a carefully designed architecture, smart IoT frameworks can provide a strong foundation for intelligent industrial monitoring, adaptive control, and sustainable digital transformation.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
2. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of Things (IIoT): An analysis framework. *Computers in Industry*, 101, 1–12. <https://doi.org/10.1016/j.compind.2018.04.015>
3. Da Xu, L., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), 2233–2243. <https://doi.org/10.1109/TII.2014.2300753>
4. Farooq, M. S., Abdullah, M., Riaz, S., Alvi, A., Rustam, F., López Flores, M. A., Castanedo Galán, J., Samad, M. A., & Ashraf, I. (2023). A survey on the role of Industrial IoT in manufacturing for implementation of smart industry. *Sensors*, 23(21), 8958. <https://doi.org/10.3390/s23218958>
5. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
6. Kaur, J., & Kaur, P. (2021). Industrial Internet of Things (IIoT): Architecture, enabling technologies, security and applications. *Journal of Ambient Intelligence and Humanized Computing*, 12, 10497–10517.
7. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23. <https://doi.org/10.1016/j.mfglet.2014.12.001>

8. Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, 6, 1–10. <https://doi.org/10.1016/j.jii.2017.04.005>
9. Nkerabahizi, N. J., Wei, M., Wang, P., & Rafiq, A. (2024). A look into smart factory for Industrial IoT driven by SDN technology: A comprehensive survey of taxonomy, architectures, issues and future research orientations. *Journal of King Saud University—Computer and Information Sciences*, 36(5), 102069. <https://doi.org/10.1016/j.jksuci.2024.102069>
10. O'Donovan, P., Leahy, K., Bruton, K., & O'Sullivan, D. T. J. (2018). An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities. *Journal of Big Data*, 5, 25. <https://doi.org/10.1186/s40537-018-0123-4>
11. Pang, Z., Chen, Q., Han, W., & Zheng, L. (2015). Value-centric design of the Internet-of-Things solution for food safety in supply chains. *International Journal of Distributed Sensor Networks*, 11(3), 137085. <https://doi.org/10.1155/2015/137085>
12. Qin, J., Liu, Y., & Grosvenor, R. (2016). A categorical framework of manufacturing for Industry 4.0 and beyond. *Procedia CIRP*, 52, 173–178. <https://doi.org/10.1016/j.procir.2016.08.005>
13. Schlemitz, A., & Mezhyuev, V. (2024). Approaches for data collection and process standardization in smart manufacturing: Systematic literature review. *Journal of Industrial Information Integration*, 39, 100578. <https://doi.org/10.1016/j.jii.2024.100578>
14. Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11), 4724–4734. <https://doi.org/10.1109/TII.2018.2805515>
15. Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems*, 48, 157–169. <https://doi.org/10.1016/j.jmsy.2018.01.006>
16. Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, 56(8), 2941–2962. <https://doi.org/10.1080/00207543.2018.1444806>
17. Yang, C., Shen, W., & Wang, X. (2018). The Internet of Things in manufacturing: Key issues and potential applications. *IEEE Systems, Man, and Cybernetics Magazine*, 4(1), 6–13. <https://doi.org/10.1109/MSMC.2017.2702391>
18. Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wireless Communications*, 24(3), 10–16. <https://doi.org/10.1109/MWC.2017.1600421>
19. Visconti, P., Rausa, G., Del-Valle-Soto, C., Velázquez, R., Cafagna, D., & De Fazio, R. (2024). Machine learning and IoT-based solutions in industrial applications for smart manufacturing: A critical review. *Future Internet*, 16(11), 394. <https://doi.org/10.3390/fi16110394>
20. Wang, W., Fadlullah, Z. M., Lu, R., & Li, X. (2022). Fusion of federated learning and Industrial Internet of Things: A survey. *Computer Networks*, 212, 109048. <https://doi.org/10.1016/j.comnet.2022.109048>