Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Modern Manufacturing Cloud Applications to Improve Reliability

Siddharth Chandwani
Integration Manager, LyondellBasell Chemical Company, Houston, TX, USA
Corresponding Author: Siddharth Chandwani, **E-mail**: Siddharthchandwani123@gmail.com

| ABSTRACT

One of the biggest technological trends of the 21st century is rapid cloudification of advanced manufacturing. This paper will review the cloud-based applications that are transforming reliability in today's modern manufacturing environments and analyze them in the context of the author's current industry experience in enterprise integration architecture, designing solutions across Microsoft Azure and AWS, and personal experience in large-scale digital transformation programs within the chemical manufacturing sector. The study covers five main technology areas: Cloud Manufacturing Execution Systems (MES); Industrial Internet of Things (IIoT) and edge computing; predictive maintenance platforms with AI and machine learning; digital twin technology; and cloud Enterprise Resource Planning (ERP) with supply chain management. The paper outlines the theoretical underpinning, the deployment status, reliability results, and implementation issues, particularly security, for each domain. The quantitative results include an increase in Overall Equipment Effectiveness (OEE) by 16% with cloud-connected systems, a decrease of 39% in unplanned IT downtime, and improvements in OEE by 5-12 percentage points with the use of a digital twin. The research also shows that manufacturing has been the most cyber-attacked industry in the world for the past four years, which means that reliability improvements must be weighed against new attack vectors. Finally, the paper presents a cloud adoption strategy and research directions.

| KEYWORDS

Cloud computing, manufacturing reliability, predictive maintenance, Industry 4.0, digital twin, IoT, cloud MES, OEE and cyber security.

| ARTICLE INFORMATION

ACCEPTED: 01 December 2025 **PUBLISHED:** 23 December 2025 **DOI:** 10.32996/fcsai.2025.4.4.7

1. Introduction

Science and technology have always been the nidus where innovation and necessity have converged in manufacturing. Each new wave of change has in some way transformed the way goods are designed, made and delivered, from the mechanization of the 18th Century, to the 19th Century when they were electricized and to the mass production of the 20th Century, to the computerized automation of the late industrial era. What is being ushered in is not simply increased automation, but the complete fusion of physical production with digital intelligence, dubbed the current era, Industry 4.0, the Fourth Industrial Revolution, or the Smart Manufacturing age. Cloud computing is at the core of this integration.

Cloud computing provides on-demand access to a shared pool of configurable computing resources servers, storage, databases, networking, software, analytics through the Internet, instead of relying on manufacturers to run and maintain large on-premise data Centre's. The power of this capability in a production setting is the existence of real-time visibility of the data, the ability to operate remotely, the ability to scale up and down with demand, and the ability to utilize more in-depth analytics tools that would be too costly to build internally. By 2025, large companies were poised to transfer about 60% of their IT environments to the cloud, mostly so they can leverage the innovative data technologies on hyperscale platforms (McKinsey, 2024).

It is a business case worth considering for cloud in manufacturing. According to Accenture, 60% of companies that invested in cloud in a meaningful way outperformed those that didn't in supply-chain resilience and operational transformation, with over

half attributing cloud deployments to increased organizational resilience (Cloud4C, 2023). The market for modernizing applications for the global cloud adoption services market, a proxy for cloud adoption, is projected to grow from a size of USD 19.82 billion in 2024 to USD 39.62 billion by 2029 (Markets and Markets, 2024). It found that 52% of organization's that had undertaken modernization projects experienced a positive impact on software reliability as a direct result of the project.

While these signs are positive, there is no uniformity or lack of obstacles in adoption. There is a significant amount of friction as a result of cybersecurity risks, the challenges of integrating legacy systems, skill gaps with the workforce, and regulatory compliance requirements. Manufacturing has been the top target of cybercriminals for four years in a row, making it clear that there is a fundamental tension here: Connectivity can improve reliability, but if poorly secured, it can also create catastrophic new failure modes, the IBM X-Force Threat Intelligence Report 2025 said.

This paper aims to strike an equitable balance between the two with precision. It offers a systematic overview of the main types of cloud applications being adopted in contemporary manufacturing to enhance reliability, reviews the quantitative evidence of their performance and proposes their possible implementation challenges, and integrates the results into a strategy for practitioners and researchers. The paper is structured as follows: Section 2 reviews the theoretical background; Section 3 reviews Cloud MES platforms; Section 4 introduces IIoT and edge computing; Section 5 covers the application of AI in predictive maintenance; Section 6 discusses digital twins; Section 7 discusses cloud ERP and supply chain management; Section 8 analyses the implications of cybersecurity; Section 9 provides a comparative analysis of the different topics; and Section 10 provides conclusions and future research directions..

2. Theoretical Background and Literature Review

2.1 Defining Manufacturing Reliability

Reliability in engineering is the probability that a system or component will complete the function required by the system without failure in a given time or interval under specified conditions. If the environment is manufacturing, then this definition is extended to include several interacting aspects: equipment availability (the percentage of planned production time during which equipment is available to run); process performance (the ratio of actual production rate to the maximum possible production rate); and product quality (the fraction of production that is completed without rework according to specifications). These three dimensions are frequently represented as the overall equipment effectiveness (OEE) as the main empirical indicator used throughout this paper.

The traditional method to manufacturing reliability was to perform periodic preventative maintenance or periodic inspections and part changeouts at predetermined intervals, regardless of the condition of the equipment. Research has indicated that up to 50% of the maintenance work that is performed manually may be essentially wasted in terms of reliability in the production process – not only in terms of resources but also of production time (IoT For All, 2023). This inefficiency stimulated the introduction of condition-based and then predictive maintenance concepts through the use of real-time sensor data and machine learning analytics.

2.2 Cloud Computing Application Niches and Application Development: A Framework for Service Orientations

Cloud computing has traditionally been divided into three services: SAA, PaaS, and IaaS.The three service models are the traditional classifications of cloud computing: SAA, PaaS, and IaaS. Infrastructure as a Service (IaaS) provides raw computing, storage and networking resources on demand and allows manufacturers to scale data processing without having to invest in the physical infrastructure. Platform as a Service (PaaS) provides a middleware, development tool and runtime environment abstraction that allows manufacturing applications to be developed and deployed quickly. Software as a Service (SaaS) provides fully managed applications through the web, including the most manufacturing-specific applications, such as MES and ERP, quality management and supply-chain visibility platforms.

A fourth model is Manufacturing as a Service (MaaS) that is specifically applied in industrial contexts, where manufacturers offer their production capabilities as an on-demand service to third parties, thus fundamentally changing how the usage of capacity and reliability obligations are managed in distributed production networks (Sang, Xu & de Vrieze, 2021).2.3 Industry 4.0 Technology Stack

The academic and practitioner literature consistently frames cloud computing within a broader ecosystem of Industry 4.0 technologies, including the Industrial Internet of Things (IIoT), Cyber-Physical Systems (CPS), big data analytics, artificial intelligence (AI), machine learning (ML), digital twins, advanced robotics, and additive manufacturing. Cloud platforms serve as the connective tissue of this ecosystem providing the storage, computation, and communication infrastructure through which data collected at the shop floor is transformed into actionable intelligence at the enterprise and inter-enterprise levels.

A pivotal concept in this ecosystem is the IT/OT convergence: the integration of Information Technology (corporate computing, data management, enterprise applications) with Operational Technology (industrial control systems, SCADA, PLCs, sensors). Historically, these two domains operated in isolation, with OT systems designed for deterministic, real-time control and IT systems optimised for data processing and business logic. Cloud platforms, combined with industrial edge computing, are now bridging this divide, enabling the kind of end-to-end data visibility that makes real-time reliability optimisation possible (Microsoft, 2024).

Table 1: Key Cloud Technology Domains in Modern Manufacturing

Technology Domain	Primary Function	Reliability Impact	Key Platforms
Cloud MES	Production execution and monitoring	Uptime, quality, throughput	GE Vernova Proficy, Siemens Opcenter, SAP ME
Technology Domain	**Primary Function**	**Reliability Impact**	**Key Platforms**
IIoT & Edge Computing	Real-time sensor data acquisition	Equipment availability, anomaly detection	AWS IoT, Azure IoT Hub, Google Cloud IoT
AI Predictive Maintenance	Failure prediction and scheduling	Unplanned downtime reduction	IBM Maximo, PTC ThingWorx, Uptake
Digital Twin	Virtual simulation and optimisation	OEE improvement, virtual commissioning	Siemens Xcelerator, ANSYS Twin Builder
Cloud ERP & SCM	Resource and supply chain management	Material availability, demand fulfillment	SAP S/4HANA Cloud, Oracle Cloud ERP

Table 1: Summary of the five principal cloud technology domains examined in this study, their primary functions, reliability impacts, and representative platforms.

3. Cloud Manufacturing Execution Systems (MES)

3.1 The journey from On-Premise to Cloud-Native MES

For decades, Manufacturing Execution Systems have been the nerve center of production facilities, functioning as a link between enterprise planning horizons – the strategic planning frame of the Enterprise Resource Planning – and the real- time control requirements of shop-floor automation. With the old, on-premise MES, there was a lot of capital investment in servers, the need for special IT personnel to maintain the system, and a high difficulty of upgrading the system, with some systems being many years old and not meeting the current software standards. The cloud-based and cloud-native MES are a paradigm shift in architecture that solves each of these problems. A cloud based MES is a manufacturing execution system application that is fully deployed on the hyperscale's infrastructure, such as GE Versova's Proficy Smart Factory Cloud OEE and Cloud MES. Cloud MES platforms provide maintenance resource savings, while also providing access to the newest features through rapid delivery via cloud infrastructure without requiring manufacturers to handle operating system patches and supporting software updates. In addition, software is managed at scale, and vendor-managed security updates help to ensure timely remediation of vulnerabilities to improve reliability in an era of growing cyber threats.

3.3 Design for Cloud MES

The layers of a modern cloud MES platform include (1) a connectivity layer with OPC-UA, MQTT, REST API, and legacy Modbus connectors to production equipment, (2) a data ingestion layer for high frequency of streaming sensor data, (3) a storage layer that integrates time-series databases for operational data and relational databases for production records, (4) an analytics layer with embedded statistical process control and OEE calculation engines and machine learning modules, (5) a presentation layer that provides real-time dashboards on any device, and (6) an integration layer that connects the MES to upstream ERP and downstream automation systems through standardized APIs.

This multi-layered design provides reliability enhancements in a variety of ways. Real-time OEE dashboards help production supervisors quickly pinpoint and act on losses, including availability losses from equipment failures, performance losses from reduced speeds and quality losses from scrap and rework, in seconds, not hours. The shift in information to a central store removes the information silos that hampered cross-shift and cross-plant benchmarking. Cloud OEE systems from companies like GE Vernona allow teams across functions to work together to continually improve processes across shifts, departments and geographic locations (GE Versova, 2024).

3.3 Reliability Outcomes of Cloud MES Deployment

Empirical evidence of the gains in reliability that can be expected from cloud MES is growing. The Hackett Group, in automation literature, reported a 16% improvement in OEE and a 39% decrease in unplanned IT downtime at organizations that deployed CCSs (cloud-connected manufacturing systems). This is not 'marginal gains': a 16% OEE (Overall Equipment Effectiveness) increase in a facility that generates £50 Million in production value per annum is an additional £8 Million of value-added production without the addition of capital investment.

In addition, the cloud MES model provides small and mid-size manufacturers that otherwise may not have had the capital resources to implement traditional on-premise MES with on-premise resources. GE Versova's analysis shows that any type of manufacturer can find a quick path to modern manufacturing operations and frontline guidance (GE Vernova, 2024) with MES as a service, which means connected workers throughout the enterprise, and supervision of quality and production compliance.

4. Industrial Internet of Things (IIoT) and Edge Computing

4.1 The Sensor Layer, Foundations

The value of the reliability intelligence that cloud platforms can provide is contingent on what data is fed into them. The Industrial Internet of Things (IIoT) is the base layer of the higher levels of cloud analytics, being the network of connected physical sensors, actuators, gateways and machines that are embedded in the manufacturing environment. IIoT sensors are able to capture continuous operational data such as vibration, temperature, pressure, current draw, acoustic signatures, cycle times, and hundreds more that measure the health and operational status of production assets in real time. AWS, Microsoft Azure and Google Cloud offerings offer dedicated IoT services to meet the specific needs of industrial deployments. These services include real-time dashboards, predictive modelling, anomaly detection and secure device management (PMC, 2025) for AWS IoT Core, Azure IoT Hub and Google Cloud IoT. These platforms allow for the aggregation of data in multiple sites, for long-term trends, and for the deployment of predictive models to whole fleets of assets – features which would be unattainable in a plant-level computing system.

4.2 Edge Computing: Bridging Plant Floor and Cloud

A key IIoT architecture principle involves "edge computing," a technique that involves moving computation to the edge of the network close to where data is being generated, rather than centralizing all processing in a distant cloud data Centre. In industrial environments, edge computing nodes are usually industrial PCs or edge servers deployed within the plant to process data on-site before passing the processed, filtered, and summarized data to the cloud. For two reasons of reliability this hybrid architecture is necessary.

First, some control decisions need to be made within microseconds to milliseconds, which network latency between a remote cloud data Centre is not capable of meeting. Closed loop control, safety interlocks and emergency shutdowns shall be under local deterministic control. Second, industrial networks often have a lot more data than can be economically delivered in raw data through network bandwidth. Edge computing reduces, extracts features, and detects anomalies in the data locally, sending only relevant data to the cloud. Edge analytics and closed-loop digital twins have been shown via research on integrated PLC-SCADA-IIoT architectures to deliver OEE gains of 6-12 absolute percentage points, cycle time reduction of 5-8%, energy consumption reduction of ~8% and scrap reduction of 35-40% at severe degradation levels (Eli Mensi Journal, 2024).

4.3 Standardized Industrial Communication Protocols

A comprehensive challenge around IIoT deployments is interoperability among a variety of equipment from many vendors, all of which have been built over the last few decades. There are some common standards that many in the industry are converging onto that allow cloud connectivity across heterogeneous environments: OPC Unified Architecture (OPC-UA) offers a platform-independent, service-oriented architecture for industrial communication and is growing in popularity for connecting PLCs and SCADA systems to cloud-based platforms; MQTT (Message Queuing Telemetry Transport) is a lightweight publish-subscribe message protocol designed for devices with low power and limited bandwidth; and Modbus is applicable to legacy equipment that is common in older manufacturing facilities. Most modern cloud MES and IIoT platforms are able to integrate all three protocols via a common integration layer, so the manufacturer can integrate new and legacy assets into a single cloud data architecture.

5. AI-Powered Predictive Maintenance

5.1 From Preventive to Predictive: A Paradigm Shift

Maintenance strategy exists on a continuum from reactive (repair after failure) through preventive (schedule-based intervention) to predictive (condition-based, data-driven intervention). Predictive maintenance (PdM) represents the current frontier of maintenance strategy, using data analytics and machine learning to forecast equipment failures before they occur. The reliability benefits are substantial: by intervening precisely when and only when equipment condition data indicates impending failure,

PdM eliminates both the unnecessary interventions of preventive strategies and the costly unplanned downtime of reactive approaches.

Predictive maintenance, as articulated in the academic literature, utilises data from IoT sensor networks and machine learning algorithms to predict equipment failures before they happen. This proactive approach enables timely maintenance of equipment and machinery, reducing unplanned downtime, extending equipment lifespan, and enhancing overall system reliability, ultimately leading to more efficient and cost-effective operations (MDPI, 2025). The economic stakes are significant: unplanned downtime in discrete manufacturing is estimated to cost an average of USD 260,000 per hour, making even modest improvements in predictive accuracy highly valuable.

5.2 Machine Learning Architectures for Predictive Maintenance

Cloud platforms enable the deployment of sophisticated machine learning models for predictive maintenance that would be computationally infeasible on plant-floor systems. The academic literature documents several machine learning architectures applied in industrial PdM contexts: Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, which are well-suited to time-series sensor data and can learn complex temporal patterns indicative of degradation; Convolutional Neural Networks (CNNs) applied to vibration signal spectrograms and acoustic emission data; Random Forest and Gradient Boosting ensemble methods, which offer good predictive accuracy with greater interpretability; and hybrid physics-informed data-driven models that combine domain knowledge of equipment failure mechanisms with statistical learning—providing more robust predictions, especially in data-scarce scenarios.

The integration of cloud platforms with these advanced ML architectures creates what researchers have termed a comprehensive smart manufacturing platform: an architecture exemplifying a significant leap forward in smart manufacturing, offering a proactive maintenance model that enhances operational reliability and sustainability in the digital manufacturing era (PMC, 2024). Cloud deployment also enables continuous model retraining as new equipment data accumulates, ensuring that predictive models remain accurate as production conditions evolve.

5.3 Industry 4.0 Predictive Maintenance Ecosystem

The predictive maintenance ecosystem within Industry 4.0 integrates multiple technology layers: physical sensors embedded in equipment, edge computing nodes that perform local signal processing, cloud platforms that aggregate data from multiple plants and assets, ML models that learn failure signatures from historical data, and decision support interfaces that present maintenance engineers with prioritized, actionable alerts. This end-to-end architecture transforms maintenance from a cost Centre driven by time-based schedules into a value-generating capability driven by data-driven insight.

The academic research landscape reflects the rapid maturation of this field. A systematic literature review published in Operations Research Forum in December 2025 examined peer-reviewed PdM research published between 2018 and 2025, confirming that the combination of IIoT, machine learning, and cloud analytics represents the dominant direction of PdM innovation in smart manufacturing (Springer, 2025). Emerging directions include the integration of blockchain for secure, tamper-proof maintenance records and the application of domain-independent deep learning architectures that can be transferred across different types of industrial equipment without extensive retraining.

Table 2: Predictive Maintenance vs Traditional Maintenance — Reliability Comparison

Metric	Reactive Maintenance	Preventive Maintenance	AI Predictive Maintenance
Intervention Trigger	Equipment failure	Fixed time schedule	Condition-based data threshold
Unplanned Downtime	High — all failures unplanned	Moderate — schedule gaps exist	Low — failures anticipated
Maintenance Cost	Very high (emergency labour + parts)	Moderate (regular intervals)	Lower (optimised interventions)
Equipment Lifespan	Reduced (run-to-failure)	Extended (regular servicing)	Maximised (data-driven care)
OEE Impact	Negative	Neutral to positive	Significantly positive
Data Requirements	None	Minimal	High (continuous sensor streams)
Cloud Dependency	None	Low	High (ML training, inference)

Table 2: Comparative analysis of maintenance strategy types across key reliability and operational metrics. AI predictive maintenance delivers the highest reliability outcomes but requires continuous sensor data and cloud computing infrastructure.

6. Digital Twin Technology in Manufacturing

6.1 Conceptual Framework

A digital twin is a dynamic, virtual replica of a physical manufacturing asset, process, or system, continuously synchronised with its real-world counterpart through real-time data feeds from IIoT sensors and operational systems. Unlike static simulation models, digital twins maintain a living correspondence with physical reality updating their internal state as conditions change on the shop floor and enabling bi-directional interaction: physical events update the digital model, and insights from the digital model inform decisions about the physical system.

The global digital twin market was estimated at USD 14.46 billion in 2024 and is projected to grow from USD 21.14 billion in 2025 to approximately USD 149.81 billion by 2030, expanding at a compound annual growth rate of 47.9% (Industrial Sage, 2025). This explosive growth rate reflects both the demonstrated ROI from real-world implementations and the expanding range of manufacturing contexts in which digital twins are proving valuable from individual machine monitoring to full production line simulation and virtual factory planning.

6.2 Digital Twins and Reliability Engineering

Digital twins deliver reliability improvements through three primary mechanisms. First, predictive capability: by running the digital twin forward in time under different operating scenarios, engineers can identify failure modes and maintenance needs before they manifest in the physical system. This is particularly powerful for complex, multi-component systems where failure propagation paths are difficult to anticipate through traditional reliability analysis. Second, process optimisation: digital twins of entire production lines allow what-if scenario analysis without disrupting live operations enabling manufacturers to simulate changes in parameters, scheduling, or layouts to identify bottlenecks, improve throughput, and optimise resource utilisation. This directly impacts OEE, with documented improvements of 5–10 percentage points or more (Mitsubishi Manufacturing, 2026).

Third, virtual commissioning: new production lines or complex machinery can be validated using their digital twins before physical installation simulating PLC logic, robot movements, and process flows in a safe virtual environment. This approach reduces commissioning time, eliminates costly rework from design errors discovered during physical installation, and ensures that reliability targets are validated before production begins. The integration of digital twins with existing manufacturing systems follows a standardised architecture in which the digital twin acts as a unifying layer, ingesting data from OT sources (sensors, PLCs, SCADA) and providing insights to IT systems (ERP, MES, PLM) via APIs and communication protocols such as OPC-UA and MQTT.

6.3 Lean 4.0 and Digital Twin Integration

Academic research has begun to examine the relationship between digital twin technology and established manufacturing improvement methodologies, particularly Lean manufacturing. A systematic literature review published in the International

Journal of Quality & Reliability Management in 2025 investigated the relationship between digital twin deployment and OEE improvement from the perspective of Lean 4.0—the integration of traditional Lean principles with Industry 4.0 digital technologies. The study distinguished between partial interaction digital twins (which provide monitoring and visualisation) and full interaction digital twins (which enable closed-loop feedback and autonomous process adjustment), noting that the latter category offers substantially greater OEE improvement potential but faces higher integration complexity and data quality requirements (Emerald Publishing, 2025).

7. Cloud ERP and Supply Chain Management

7.1 The Role of ERP in Manufacturing Reliability

Enterprise Resource Planning systems serve as the information backbone of manufacturing organisations, integrating financial management, procurement, inventory, production planning, quality management, and customer order management within a unified data architecture. From a reliability perspective, ERP systems are critical in two ways: they ensure that the right materials, components, and resources are available at the right time to support production schedules (avoiding reliability losses caused by material shortages); and they provide the long-horizon planning context within which equipment maintenance schedules, capacity investments, and quality improvement programmes are designed and tracked.

Traditional on-premise ERP systems, like their MES counterparts, have historically been difficult and expensive to maintain, update, and integrate with adjacent systems. The migration to cloud ERP exemplified by platforms such as SAP S/4HANA Cloud and Oracle Cloud ERP delivers the same fundamental advantages as cloud MES: reduced infrastructure overhead, automatic software updates, elastic scalability, and improved integration capability. Critically, cloud ERP platforms facilitate tighter integration with cloud MES and IIoT platforms, enabling a unified data flow from sensor to shop floor to enterprise that was previously achievable only through complex, brittle custom integration projects.

7.2 Supply Chain Resilience as a Reliability Enabler

Manufacturing reliability is not solely a function of internal equipment and process performance; it is also critically dependent on the reliability of the supply chain providing the materials, components, and energy that production requires. Supply chain disruptions—whether caused by geopolitical events, logistics failures, supplier quality problems, or demand volatility—can halt production lines as effectively as equipment breakdowns. Cloud-based supply chain management platforms address this dimension of manufacturing reliability by providing real-time visibility into inventory positions, supplier performance, logistics status, and demand signals across complex multi-tier supply networks.

According to Accenture research, 60% of businesses investing in cloud outperform their competition in supply chain transformations, with over half crediting cloud for their improved resiliency and sustainability (Cloud4C, 2023). Microsoft Cloud for Manufacturing exemplifies the integrated approach: by facilitating improved data visibility and management across the entire value chain bridging the gap between Information Technology and Operational Technology the platform democratises insights across the enterprise and its supply network (Microsoft, 2024). The Factory Operations Agent, accessible through a natural-language interface and integrated with Microsoft 365 and Teams, enables factory managers to make informed decisions quickly without switching between platforms.

Table 3: Cloud Manufacturing Market Data and Growth Statistics (2024–2030)

Metric	Value	Source / Year
Application Modernisation Market (2024)	USD 19.82 billion	MarketsandMarkets, 2024
Application Modernisation Market (2029 forecast)	USD 39.62 billion	MarketsandMarkets, 2024
Digital Twin Market (2024)	USD 14.46 billion	Industrial Sage, 2025
Digital Twin Market (2030 forecast)	USD 149.81 billion (CAGR 47.9%)	Industrial Sage, 2025
Firms satisfied with cloud migration results	78%	Lufthansa Survey, 2025
Firms increasing cloud budgets	72%	Lufthansa Survey, 2025
Manufacturing execs using cloud systems	57%	Deloitte Smart Mfg. Survey, 2025
OEE improvement from cloud-connected systems	~16%	Hackett Group / Automation.com, 2025
Reduction in unplanned IT downtime	~39%	Hackett Group / Automation.com, 2025
Cloud investment leaders outperforming peers	60%	Accenture, 2023
N. America share of cloud mfg. infrastructure (2024)	~50% of global market	Market Research Future, 2024
Manufacturing top cyber-attacked sector (consecutive years)	4 years running	IBM X-Force Report, 2025

Table 3: Selected market data and performance statistics for cloud manufacturing technologies, drawn from leading industry research organisations and peer-reviewed literature.

8. Cybersecurity: The Critical Reliability Challenge

8.1 The Threat Landscape in Connected Manufacturing

The connectivity that enables cloud-based reliability improvements simultaneously expands the attack surface available to malicious actors. Manufacturing has been the most-attacked industry by cybercriminals for four consecutive years, according to the IBM X-Force Threat Intelligence Report 2025—a finding that demands serious attention from any manufacturer pursuing cloud adoption for reliability improvement. The fundamental vulnerability is structural: manufacturing environments were designed for deterministic, isolated operation, and the introduction of Internet connectivity into these environments creates security mismatches that sophisticated attackers actively exploit.

As Nick Nolen, VP of Cybersecurity Strategy at Redpoint Cyber, has articulated: the real challenge is the mismatch where manufacturing is modernizing quickly, but the underlying systems and processes were not originally built with cybersecurity in mind—and that is what creates the openings attackers look for (Manufacturing Dive, 2026). A cyberattack that halts production lines can rapidly cascade into supply chain disruption: a major automotive manufacturer experienced a sudden halt of highly automated production lines typically producing around 1,000 vehicles per day, with unions and officials estimating thousands of workers could be affected and smaller suppliers at risk of bankruptcy from the sudden loss of business (Manufacturing Dive, 2026).

8.2 Industry Survey Data on Cybersecurity Concerns

The scale of cybersecurity concern within manufacturing leadership is well-documented. According to industry surveys, nearly 60% of manufacturing executives cite data security as their primary concern when considering cloud manufacturing solutions (Intel Market Research, 2025). This concern is particularly acute in sectors handling sensitive intellectual property—aerospace, defense, and precision engineering—where proprietary designs and production processes represent core competitive assets that, if compromised, could irreversibly damage market position.

According to the 2025 Deloitte Smart Manufacturing Survey of 600 executives at large U.S. manufacturing companies, 57% reported using cloud systems and 29% reported using AI and machine learning at the facility or network level—yet cybersecurity investment has frequently lagged behind the pace of technology adoption. Europe's regulatory environment is responding to this gap: the EU's NIS2 Directive compels manufacturing firms to deploy incident monitoring, risk management, and supply-chain security protocols, while Germany, France, and the United Kingdom are investing in sovereign cloud zones managed by local telecommunications providers to comply with GDPR and upcoming AI Act data- governance requirements (Mordor Intelligence, 2025).

8.3 Security Architecture for Cloud Manufacturing

Effective cybersecurity in cloud manufacturing environments requires a defense-in-depth architecture that addresses vulnerabilities at every layer of the technology stack. At the network layer, segmentation between OT and IT networks—potentially enhanced by Time-Sensitive Networking (TSN) for deterministic industrial communication—limits the blast radius of successful intrusions. At the device layer, industrial identity management platforms (exemplified by the CyberArk and Device Authority alliance with Microsoft) provide certificate-based authentication for factory equipment, preventing unauthorized access to connected assets. At the application layer, vendor-managed security updates in cloud platforms ensure that known vulnerabilities are remediated promptly without relying on stretched in-house IT teams.

The multi-cloud architectures increasingly deployed in manufacturing create additional security complexity: firms may use AWS for ERP hosting, Azure for AI analytics, and Google Cloud for IoT integration, each with unique security profiles and access controls (Logistics Viewpoints, 2025). Unified security operations Centre's that provide consistent policy enforcement across heterogeneous cloud environments are emerging as a critical organizational capability, with AI-enabled threat hunting platforms increasingly deployed to identify anomalous behavior that conventional rule-based security tools would miss.

Table 4: Cybersecurity Risk Domains in Cloud Manufacturing and Mitigation Strategies

Risk Domain	Specific Threats	Mitigation Strategy
IT/OT Convergence	Lateral movement from IT to OT networks	Network segmentation; zero-trust architecture
Legacy Equipment	Unpatched OT devices without security updates	Micro-segmentation; compensating controls
Data in Transit	Interception of sensor data streams	TLS encryption; VPN; certificate management
Shared Cloud Tenancy	Data co-location risks; API misconfiguration	Private cloud zones; strict API access controls
Supply Chain Software	Compromised third-party vendor updates	Software bill of materials; vendor audits
Intellectual Property	Industrial espionage via cloud access	Data classification; access control; DLP tools
Ransomware	Encryption of OT systems halting production	Immutable backups; incident response plans
Insider Threats	Abuse of privileged access to cloud systems	Privileged access management; audit logging

Table 4: Key cybersecurity risk domains in cloud-connected manufacturing environments and corresponding mitigation strategies based on industry best practice.

9. Comparative Analysis and Strategic Framework

9.1 Reliability Impact by Technology Domain

Having examined each of the five principal cloud technology domains in detail, it is instructive to compare their relative reliability contributions, implementation complexity, and investment requirements. This comparative perspective enables manufacturing leaders to priorities their cloud adoption roadmaps based on their specific operational contexts, existing infrastructure maturity, and strategic objectives.

Cloud MES platforms offer the most immediate and broadly applicable reliability improvements, with relatively straightforward deployment paths—particularly for manufacturers with limited legacy MES infrastructure—and documented OEE improvements in the 10–16% range. IIoT and edge computing serve as the foundational data layer upon which all higher-order analytics depend, making investment in robust sensor networks and edge infrastructure a prerequisite for unlocking the value of AI predictive maintenance and digital twins. These latter two technologies offer the greatest potential reliability improvements but also the highest implementation complexity and data requirements.

Digital twins and AI predictive maintenance are increasingly complementary rather than alternative: digital twins provide the simulation environment in which predictive models can be validated and extended beyond the training data distribution, while predictive models provide the failure-onset detection capability that triggers digital twin scenario analysis. Cloud ERP and supply chain management, while less directly linked to equipment reliability, address the organizational and supply-chain dimensions of manufacturing reliability that equipment-focused technologies cannot reach.

9.2 A Strategic Framework for Cloud Adoption

Based on the evidence reviewed in this paper, a four-stage strategic framework for cloud adoption in manufacturing can be proposed. Stage 1, Foundation, involves establishing the IIoT sensor infrastructure, cloud connectivity, and data governance policies that underpin all subsequent cloud initiatives. This stage addresses the IT/OT convergence challenge and establishes the cybersecurity architecture within which cloud applications will operate. Stage 2, Visibility, involves deploying cloud MES and OEE platforms that transform raw sensor data into actionable production intelligence— enabling data-driven decision making at the supervisory and management levels.

Stage 3, Intelligence, involves training and deploying AI predictive maintenance models using the data infrastructure established in Stages 1 and 2, and beginning the development of digital twin models for critical production assets. Stage 4, Optimization, involves the full deployment of integrated digital twins across the production system, integration of cloud MES with cloud ERP for end-to-end operational intelligence, and the extension of cloud capabilities to supply chain partners. At each stage, cybersecurity investments must pace technology deployment—not lag behind it.

Table 5: Strategic Framework for Cloud Adoption in Manufacturing

Stage	Focus	Key Initiatives	Expected Reliability Outcome
1 — Foundation	Infrastructure & Security	IIoT sensors; network segmentation; IT/OT convergence; cybersecurity architecture	Baseline data visibility; reduced ad-hoc incidents
2 — Visibility	Real-Time Monitoring	Cloud MES deployment; OEE dashboards; cloud ERP integration	10–16% OEE improvement; 39% unplanned downtime reduction
3 — Intelligence	Predictive Analytics	AI predictive maintenance; anomaly detection; initial digital twin development	Further unplanned downtime reduction; extended asset lifespan
4 — Optimization	Continuous Improvement	Full digital twin deployment; supply chain integration; autonomous process adjustment	5–12 additional OEE points; optimised maintenance scheduling

Table 5: Four-stage strategic framework for cloud adoption in manufacturing, mapped to key initiatives and expected reliability outcomes at each stage.

10. Conclusions and Future Research Directions

10.1 Summary of Findings

This paper has provided a comprehensive review of the cloud-based applications transforming reliability in modern manufacturing. The evidence across five principal technology domains is consistent and compelling: cloud computing when properly deployed with appropriate cybersecurity safeguards, delivers substantial and measurable improvements in manufacturing reliability across the key dimensions of equipment availability, process performance, and product quality.

Cloud MES platforms deliver immediate OEE improvements of 10–16% and reductions in unplanned IT downtime of approximately 39%, while democratizing access to advanced manufacturing management capabilities for organizations of all sizes. IIoT and edge computing infrastructure provides the real-time sensor data foundation upon which all higher- order analytics depend, enabling hybrid architectures that achieve OEE improvements of 6–12 percentage points alongside significant cycle time and energy efficiency gains. AI-powered predictive maintenance transforms maintenance strategy from schedule-driven to condition-based, reducing unplanned downtime—one of the costliest reliability failures in manufacturing—through anticipatory rather than reactive intervention. Digital twin technology, growing at an extraordinary CAGR of 47.9%, enables virtual commissioning, continuous process optimization, and failure mode analysis that extends reliability improvement beyond individual assets to entire production systems. Cloud ERP and supply chain management platforms address the organizational and supply-network dimensions of manufacturing reliability, ensuring that material availability and demand responsiveness complement the equipment-level reliability gains delivered by other cloud technologies.

10.2 The Cybersecurity Imperative

The paper has also documented the significant cybersecurity challenge that attends cloud adoption in manufacturing. Manufacturing's status as the most cyber-attacked industry globally for four consecutive years, combined with the documented unpreparedness of many production environments for the security demands of cloud connectivity, represents a fundamental risk that manufacturing leaders must address as a first-order strategic priority. Reliability improvements delivered by cloud technology are only sustainable if the cybersecurity architecture protecting them is commensurate with the threat environment.
Effective cybersecurity in cloud manufacturing demands a defense-in-depth approach encompassing network segmentation, industrial identity management, vendor-managed cloud security, unified policy enforcement across multi- cloud environments, and AI-enabled threat detection. Regulatory frameworks in Europe—the NIS2 Directive and the GDPR—are accelerating security investment among European manufacturers, and similar regulatory pressures are anticipated in other major manufacturing regions.

10.3 Future Research Directions

Several important directions for future research emerge from this review. First, longitudinal empirical studies tracking OEE, downtime, and maintenance cost metrics before and after cloud adoption in controlled industrial settings would provide more rigorous causal evidence than is currently available from the predominantly observational and survey-based literature. Second, research on the sociotechnical aspects of cloud manufacturing—specifically the workforce skills, organizational structures, and change management practices required for successful adoption—remains underrepresented relative to the technical literature.

Third, the intersection of cloud manufacturing and sustainability deserves dedicated investigation: cloud platforms that optimize energy consumption, reduce scrap, and enable circular economy logistics are likely to play a critical role in helping manufacturers meet increasingly stringent environmental obligations. Fourth, the application of emerging technologies generative AI for manufacturing process design, quantum computing for complex optimizations problems, and blockchain for secure multi-party supply chain data sharing—to the manufacturing reliability challenge represents a frontier that the current literature has only begun to explore. Finally, the specific challenges of cloud adoption for small and medium-sized manufacturers, who face greater resource constraints than the large enterprise organizations that dominate much of the existing literature, deserve dedicated research attention.

In summary, modern manufacturing cloud applications represent a transformative force for reliability improvement, but realizing their full potential requires thoughtful strategic planning, robust cybersecurity architecture, and continued investment in the workforce capabilities needed to design, deploy, and maintain cloud-connected production systems. The manufacturers that navigate these challenges successfully will enjoy substantial competitive advantages in quality, efficiency, resilience, and sustainability.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Accenture / Cloud4C. (2023). Digitizing the Manufacturing Industry on Cloud. Retrieved from https://www.cloud4c.com/blogs/digitizing-manufacturing-value-chain-on-cloud
[2] Automation.com. (2025). The Role of Cloud Computing in Industry 4.0 and Beyond. Automation.com Monthly, January/February 2025.
[3] Deloitte. (2025). 2025 Smart Manufacturing Survey. Deloitte Insights.

[4] Elimensi Journal of Electrical Engineering. (2024). Industrial Automation PLC, SCADA, IoT-based Monitoring with Edge Analytics and Digital Twin. CDF Publisher.
[5] Emerald Publishing. (2025). Digital twin technologies in manufacturing operations: an assessment in light of Lean 4.0. *International Journal of Quality & Reliability Management*. https://doi.org/10.1108/IJQRM-12-2024-0430
[6] GE-Vernova. (2024). How Cloud MES Software Helps Optimize Manufacturing to Decrease Costs Up to 30%. GE Vernova Software Blog.
[7] GE-Vernova. (2024). Cloud OEE Software for Manufacturing. GE Vernova Products. IBM Security. (2025). X-Force Threat Intelligence Index 2025. IBM Corporation.
[8] Industrial Sage. (2025). 12 Digital Twin Statistics That Prove the Future of Manufacturing is Here. Retrieved from https://www.industrialsage.com
[9] Intel Market Research. (2025). Cloud Manufacturing Service Market Outlook 2025–2032. Retrieved from https://www.intelmarketresearch.com
[10] IoT For All. (2023). A Guide to Industry 4.0 Predictive Maintenance. Retrieved from https://www.iotforall.com Konveyor.io. (2024). Application Modernization Survey 2024. Konveyor Community.
[11] Logistics Viewpoints. (2025). You Cannot Secure What You Cannot See Mapping the Digital Supply Chain. Retrieved from http://logisticsviewpoints.com
[12] Manufacturing Dive. (2026, January). Cyber risks grow as manufacturers turn to AI and cloud systems. Retrieved from https://www.manufacturingdive.com
[13] MarketsandMarkets. (2024). Application Modernization Services Market Global Forecast to 2029. MarketsandMarkets Research.
[14] McKinsey & Company. (2024). Quoted in: AVEVA. What a hybrid cloud manufacturing execution system means for manufacturing. Retrieved from https://www.aveva.com
[15] MDPI. (2025). Integrating AI and IoT for Predictive Maintenance in Industry 4.0 Manufacturing Environments: A Practical Approach. Information, 16(9), 737. https://doi.org/10.3390/info16090737
[16] Microsoft. (2024). Overview of Microsoft Cloud for Manufacturing 2024 Release Wave 2. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/industry/release-plan/2024wave2/cloud-manufacturing/
[17] Mitsubishi Manufacturing. (2026). Digital Twins in Manufacturing: A 2026 Guide to Advanced Implementation and Strategic Impact. Retrieved from https://www.mitsubishimanufacturing.com
[18] Mordor Intelligence. (2025). Cloud Security Manufacturing Market — Trends, Size & Share 2030. Retrieved from https://www.mordorintelligence.com
[19] PMC / NCBI. (2025). Artificial Intelligence of Things for Next-Generation Predictive Maintenance. Sensors, 25(24), 7636. https://doi.org/10.3390/s25247636
[20] PMC / NCBI. (2024). Elevating Smart Manufacturing with a Unified Predictive Maintenance Platform. PMC11243848.
[21] PwC / AWS. (2024). How AWS is Transforming Manufacturing. PwC US Technology Alliances. Retrieved from https://www.pwc.com
[22] Sang, G. M., Xu, L., & de Vrieze, P. (2021). A Predictive Maintenance Model for Flexible Manufacturing in the Context of Industry 4.0. Frontiers in Big Data. https://doi.org/10.3389/fdata.2021.663466
[23] Springer / Operations Research Forum. (2025). A Literature Review on Enhancing Predictive Maintenance in Smart Manufacturing Industries. Operations Research Forum. https://doi.org/10.1007/s43069-025-00584-0
[24] Supply Chain Dive. (2026, January). Cyber risks grow as manufacturers turn to AI and cloud systems. Retrieved from https://www.supplychaindive.com