Multidisciplinary | Peer-Reviewed
Open Access | Research Journal
ISSN: 3139-2954

Article ID: IRJIST-2026-050
Volume 1 | Issue 3 | 2026
DOI: https://doi.org/10.67308/irjist.050

International Research Journal of Innovation in Science and Technology

Risk Assessment and Mitigation in Smart Manufacturing Systems Using a Qualitative Risk Matrix Approach

Sharvani Jagtap[1], Aarya Chavan[2]

[1-2]Research Scholar, Vishwakarma Institute of Information Technology, Pune, India
Correspondence: [1]sharvani.22310662@viit.ac.in; [2]aarya.22310628@viit.ac.in

Abstract

Industry 4.0 technologies, including the Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), and automation, have significantly transformed modern manufacturing by improving productivity, flexibility, and operational efficiency. However, the increasing connectivity and complexity of smart manufacturing systems have also introduced new technical, operational, cybersecurity, and safety-related risks that require systematic assessment and management. This paper presents a structured framework for risk identification, assessment, and mitigation using a qualitative risk matrix approach. The proposed methodology classifies manufacturing risks into major categories and evaluates them based on their probability of occurrence and potential impact to support effective risk prioritization. Appropriate mitigation strategies, including predictive maintenance, enhanced cybersecurity measures, system redundancy, real-time monitoring, and workforce training, are discussed to improve system reliability and operational safety. The study highlights that systematic risk assessment enables early identification of critical vulnerabilities, supports informed engineering decision-making, and contributes to more resilient, reliable, and sustainable smart manufacturing systems. The proposed framework provides a practical reference for manufacturing engineers and industrial practitioners implementing risk management within Industry 4.0 environments.

Keywords: Smart Manufacturing; Industry 4.0; Risk Assessment; Risk Matrix; Risk Mitigation; Cyber-Physical Systems (CPS); Industrial Safety.

1. Introduction

Smart manufacturing has emerged as a fundamental component of the Fourth Industrial Revolution (Industry 4.0), transforming conventional production systems into intelligent, interconnected, and data-driven manufacturing environments. The integration of advanced technologies such as the Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), cloud computing, robotics, and big data analytics has enabled real-time monitoring, predictive maintenance, autonomous decision-making, and improved operational efficiency across manufacturing industries [8]–[10]. These technological advancements have significantly enhanced productivity, product quality, resource utilization, and manufacturing flexibility, enabling industries to respond rapidly to changing market demands.

Despite these advantages, the increasing complexity and connectivity of smart manufacturing systems have introduced a wide range of new challenges associated with system reliability, operational continuity, cybersecurity, and workplace safety. Unlike conventional manufacturing environments, Industry 4.0 systems rely heavily on continuous communication between physical equipment and digital platforms. Consequently, failures in sensors, communication networks, software, or control systems may propagate rapidly throughout the production process, resulting in equipment malfunction, production downtime, data loss, financial losses, and safety hazards [1], [8], [9].

In addition, cyber threats, unauthorized access, ransomware attacks, and data integrity issues have become significant concerns due to the growing dependence on interconnected industrial control systems.

Effective risk management has therefore become an essential component of modern manufacturing engineering. International standards such as ISO 31000 provide systematic principles for identifying, analysing, evaluating, and treating organizational risks, while project management frameworks and engineering reliability studies emphasize proactive planning to minimize uncertainty and improve operational resilience [1], [5]–[7]. More recently, the adoption of predictive maintenance, intelligent monitoring, digital twins, and Industrial Internet of Things (IIoT) technologies has further strengthened risk management practices by enabling early fault detection and condition-based decision-making within smart manufacturing environments [9]–[14].

Among the various qualitative risk assessment techniques, the risk matrix approach remains one of the most widely adopted methods because of its simplicity, visual interpretation, and practical applicability. By evaluating risks based on their probability of occurrence and potential impact, the qualitative risk matrix enables engineers and decision-makers to prioritize critical risks, allocate resources efficiently, and implement suitable mitigation strategies before failures occur. Its ease of implementation makes it particularly suitable for manufacturing organizations seeking structured yet practical approaches for managing operational and technological risks [1], [5].

Although several studies have discussed individual aspects of Industry 4.0, cybersecurity, maintenance, and manufacturing safety, comparatively fewer review-based studies have presented an integrated overview of risk identification, qualitative risk evaluation, and mitigation strategies specifically from the perspective of smart manufacturing systems. This paper addresses this need by reviewing the major categories of risks encountered in Industry 4.0 environments and presenting a structured qualitative risk matrix framework for systematic risk assessment and mitigation. The study further discusses practical mitigation strategies that support improved reliability, operational safety, and sustainable manufacturing performance, thereby providing a useful reference for researchers, manufacturing engineers, and industrial practitioners.

2. Literature Review

The rapid evolution of Industry 4.0 has significantly transformed manufacturing systems by integrating intelligent automation, cyber-physical systems, cloud computing, and Industrial Internet of Things (IIoT) technologies into conventional production environments. While these technologies have improved manufacturing efficiency and productivity, they have also increased system complexity and introduced new categories of operational, cybersecurity, and safety-related risks [8]–[10]. Consequently, researchers have devoted considerable attention to developing structured risk assessment methodologies capable of supporting safe and reliable smart manufacturing operations.

2.1. Risk Management Principles and Standards

Risk management provides a systematic framework for identifying uncertainties, evaluating their consequences, and implementing suitable control measures. ISO 31000 establishes internationally accepted guidelines for organizational risk management by emphasizing risk identification, analysis, evaluation, treatment, communication, and continuous monitoring throughout the system lifecycle [1]. Similarly, the PMBOK Guide highlights qualitative and quantitative risk assessment as essential elements of engineering and project management, supporting informed decision-making and effective resource allocation under uncertain operating conditions [5]. Reliability engineering literature further emphasizes proactive maintenance planning and systematic risk control as key contributors to improving equipment availability and operational performance [6], [7].

2.2. Smart Manufacturing and Industry 4.0 Risks

The emergence of Industry 4.0 has expanded the scope of manufacturing risk beyond conventional mechanical failures. Smart manufacturing systems integrate IoT devices, cyber-physical systems, artificial intelligence, cloud computing, and intelligent automation, enabling continuous data exchange and autonomous process control [8]–[10]. However, this high level of interconnectivity also introduces vulnerabilities related to software failures, communication network interruptions, cybersecurity breaches, sensor malfunctions, and system integration challenges. These interconnected risks may propagate across multiple manufacturing subsystems, affecting production continuity, equipment reliability, and workplace safety.

Recent studies have demonstrated that predictive maintenance, digital twins, machine learning, and intelligent monitoring systems can significantly improve equipment reliability by enabling early fault detection and condition-based maintenance [10], [14]. Nevertheless, the successful implementation of these technologies requires comprehensive risk assessment methods capable of addressing both conventional engineering failures and emerging cyber-physical threats.

2.3. Qualitative Risk Matrix and Manufacturing Applications

Among various risk assessment techniques, the qualitative risk matrix remains one of the most practical tools for evaluating manufacturing risks because of its simplicity and ease of implementation. The method classifies identified hazards according to their probability of occurrence and potential consequences, allowing organizations to prioritize corrective actions and optimize resource allocation [1], [5]. Owing to its visual representation and straightforward interpretation, the qualitative risk matrix is widely applied in manufacturing industries for operational planning, maintenance management, workplace safety, and project risk evaluation.

Recent engineering studies have further demonstrated the growing importance of integrating traditional risk assessment approaches with modern manufacturing technologies. Hybrid frameworks combining conventional risk analysis methods with intelligent monitoring, process optimization, and Industry 4.0 technologies have shown considerable potential for improving manufacturing safety, equipment reliability, and operational efficiency [11]–[14]. Similarly, investigations into advanced machining processes and manufacturing optimization have emphasized that systematic risk evaluation supports better process planning, preventive maintenance, and sustainable industrial operations [11]–[13].

2.4. Research Gap

Although extensive research has been conducted on Industry 4.0 technologies, manufacturing automation, and engineering risk management, much of the existing literature addresses individual risk categories or focuses on specific analytical techniques. Comprehensive reviews that collectively examine technical, operational, cybersecurity, and safety risks using a practical qualitative risk matrix framework remain comparatively limited. This paper addresses this gap by presenting a structured review of risk identification, qualitative risk assessment, and mitigation strategies applicable to smart manufacturing systems, thereby providing a practical framework for improving reliability, safety, and operational resilience in Industry 4.0 environments.

3. Methodology

This study adopts a structured qualitative methodology for identifying, classifying, evaluating, and mitigating risks associated with smart manufacturing systems. The proposed framework utilizes a qualitative risk matrix approach to systematically assess potential risks based on their likelihood of occurrence and potential impact. The methodology consists of four sequential stages: risk identification, risk classification, qualitative risk assessment, and development of appropriate mitigation strategies, providing a practical framework for improving the reliability and safety of Industry 4.0 manufacturing environments.

3.1. Risk Identification

Risk identification represents the first and most important stage of the proposed methodology. The objective of this phase is to recognize potential hazards and operational challenges that may affect the performance, safety, and reliability of smart manufacturing systems. To ensure comprehensive coverage, multiple information sources are considered during the identification process, including system analysis, industrial literature, and expert knowledge.

The major approaches adopted for risk identification include:

- **System and Process Analysis:** Manufacturing workflows, machine interactions, communication networks, and data exchange mechanisms are examined to identify possible failure points, operational bottlenecks, and system vulnerabilities.
- **Review of Industrial Practices and Published Literature:** Relevant research articles, industrial case studies, technical reports, and established risk management standards are reviewed to identify commonly reported risks associated with Industry 4.0 technologies and smart manufacturing systems.
- **Expert Judgment and Industrial Experience:** Practical knowledge obtained

from manufacturing engineers, maintenance personnel, and domain experts is considered to identify operational risks that may not be adequately represented in published literature.

The integration of these information sources ensures that both technical and operational risks are comprehensively identified before proceeding to the assessment stage.

3.2. Risk Classification

Following risk identification, the identified hazards are categorized according to their origin and potential influence on manufacturing operations. This systematic classification facilitates focused analysis and enables the selection of appropriate mitigation measures for each category.

The principal risk categories considered in this study are:

- **Technical Risks:** Equipment failures, sensor malfunctions, software defects, communication failures, and system integration issues that may interrupt manufacturing processes.
- **Operational Risks:** Human errors, inadequate operator training, process inefficiencies, improper machine operation, and workflow management issues that affect production performance.
- **Cybersecurity Risks:** Unauthorized system access, malware attacks, data breaches, network vulnerabilities, and cyber threats affecting interconnected manufacturing systems.
- **Safety Risks:** Machine-related accidents, hazardous working conditions, equipment malfunction, and failure of safety mechanisms that may endanger personnel or manufacturing assets.

This classification enables systematic evaluation of different risk categories and supports the development of targeted mitigation strategies.

3.3. Qualitative Risk Assessment Using Risk Matrix

Following classification, the identified risks are evaluated using a qualitative risk matrix based on two key parameters: **Probability (P)** and **Impact (I)**. Probability represents the likelihood that a particular risk event may occur during manufacturing operations, while impact indicates the severity of its potential consequences on production continuity, equipment reliability, worker safety, and organizational performance.

Each identified risk is assessed using three qualitative levels:

- **Probability (P):** Low (P1), Medium (P2), High (P3)
- **Impact (I):** Low (I1), Medium (I2), High (I3)

The overall risk level is determined by combining the probability and impact ratings within the qualitative risk matrix. Based on this assessment, risks are classified into **Low**, **Medium**, or **High** categories, allowing decision-makers to prioritize critical risks requiring immediate corrective actions while efficiently allocating available resources.

Impact \ Probability	Low (P1)	Medium (P2)	High (P3)
High (I3)	Machine overheating (rare but severe)	Cyber-attack on database	System-wide network failure, Major safety accident
Medium (I2)	Minor sensor calibration error	Operator error, Data processing delay	Frequent sensor malfunction, Software bugs
Low (I1)	Minor UI glitch	Routine maintenance delay	Frequent small data packet loss

Figure 1: *Qualitative risk matrix illustrating the relationship between probability and impact for risk prioritization.*

3.4. Risk Mitigation Strategy

After the risks have been prioritized, suitable mitigation measures are proposed according to their severity and operational significance. Higher-priority risks are addressed through preventive and corrective measures aimed at reducing either the likelihood of occurrence or the potential impact on manufacturing operations.

Typical mitigation strategies include predictive maintenance, continuous equipment monitoring, enhanced cybersecurity measures, workforce training, preventive maintenance scheduling, process optimization, and implementation of appropriate safety protocols. The selection of these measures supports improved system reliability, operational continuity, and workplace safety while

contributing to sustainable smart manufacturing practices.

The complete sequence of the proposed qualitative risk assessment methodology is illustrated in Figure 2.

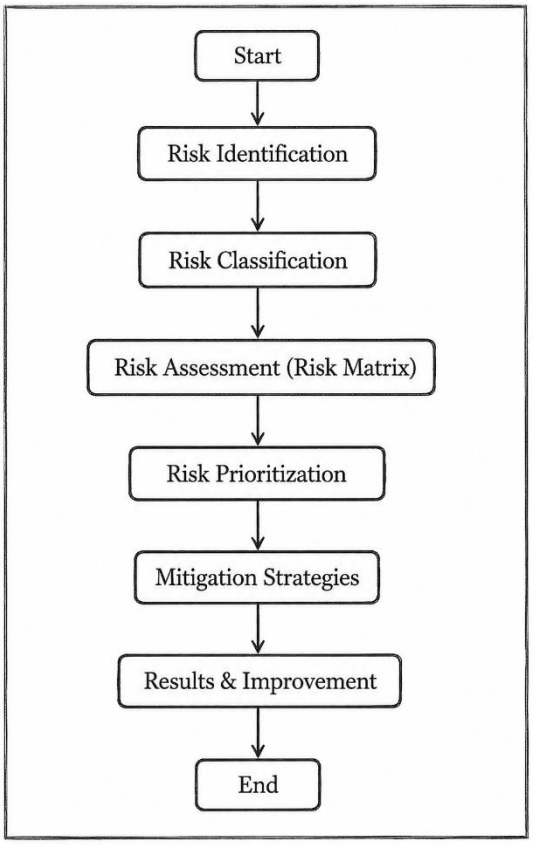

Figure 2: *Methodological flowchart for qualitative risk assessment and mitigation in smart manufacturing systems.*

4. Risk Analysis in Smart Manufacturing Systems

4.1. Identified Risks

Smart manufacturing systems integrate advanced digital technologies, intelligent automation, and interconnected production networks, making them susceptible to a wide range of technical, operational, cybersecurity, and safety-related risks. The identification and classification of these risks provide the foundation for effective risk assessment and the development of suitable mitigation strategies. Based on the proposed qualitative risk assessment framework, the principal risks considered in this study are summarized in Table 1.

Table 1: *Identified risks in smart manufacturing systems*

Risk Type	Description
Technical	Sensor failure, machine breakdown, system errors
Operational	Human error, lack of training, process inefficiency
Cybersecurity	Data breach, hacking, unauthorized system access
Safety	Injury due to automation, machine-related hazards

The identified risks represent some of the most common challenges encountered in Industry 4.0 manufacturing environments. Because modern manufacturing systems operate through interconnected machines, communication networks, sensors, and control platforms, a failure in one subsystem may propagate to other components, resulting in production interruptions, reduced operational efficiency, and increased safety concerns. Therefore, systematic identification of these risks is essential for improving system reliability and supporting informed engineering decisions.

4.2. Risk Matrix Evaluation

Following risk identification, each risk is evaluated using the qualitative risk matrix described in the methodology. The assessment considers both the probability of occurrence and the potential operational impact to determine the overall level of risk. This approach enables risks to be prioritized according to their severity, thereby assisting organizations in allocating resources and implementing appropriate preventive measures.

The results of the qualitative risk assessment are presented in Table II, where each identified risk is classified according to its probability, impact, and corresponding risk level.

Table 2: *Risk Matrix Evaluation*

Risk	Probability	Impact	Risk Level
Sensor failure	High	High	Critical
Cyber attack	Medium	High	High
Operator error	Medium	Medium	Medium
Equipment failure	Low	High	Medium

The evaluation indicates that risks with higher probability and greater operational impact require immediate attention, while moderate and low-risk events can be managed through routine monitoring and preventive maintenance. This structured assessment assists manufacturing organizations in establishing priorities for risk reduction and supports systematic decision-making within smart manufacturing environments.

4.3. Analysis

The qualitative risk assessment indicates that sensor failure represents the most critical risk in smart manufacturing systems because sensors serve as the primary source of operational data for automated monitoring, process control, and decision-making. A sensor malfunction can interrupt data acquisition, reduce automation efficiency, and affect the overall stability of interconnected manufacturing processes.

Cybersecurity threats also represent a significant concern due to the increasing connectivity of Industry 4.0 environments. Although their probability of occurrence may be lower than certain operational failures, cyberattacks can result in unauthorized access, data breaches, production interruptions, and substantial financial losses. Consequently, cybersecurity remains a high-priority risk requiring continuous monitoring and robust protective measures.

Operator errors and equipment failures are categorized as moderate risks because their occurrence can generally be reduced through proper workforce training, preventive maintenance, standardized operating procedures, and continuous equipment monitoring. While these risks may not always result in catastrophic failures, inadequate management can adversely affect production efficiency, product quality, and workplace safety.

Overall, the analysis demonstrates that the qualitative risk matrix provides a practical and systematic approach for prioritizing manufacturing risks based on their likelihood and potential consequences. By identifying critical risk areas at an early stage, manufacturing organizations can implement appropriate mitigation strategies that improve operational reliability, reduce downtime, and enhance the safety and resilience of smart manufacturing systems.

5. Mitigation Strategies

Smart manufacturing systems are exposed to various technical, operational, cybersecurity, and safety-related risks. Therefore, implementing effective mitigation strategies is essential to reduce the likelihood of failures, minimize their potential impact, and improve the overall reliability, safety, and efficiency of manufacturing operations. Appropriate preventive measures, corrective actions, and continuous monitoring contribute significantly to the successful operation of Industry 4.0 manufacturing systems.

5.1. Technical Risk Mitigation

Technical risks such as sensor malfunctions, machine failures, and software-related issues can significantly affect manufacturing performance. The following measures can help minimize these risks:

- Implement predictive maintenance using real-time monitoring and data analytics to identify potential equipment failures before they occur.
- Select high-quality sensors, controllers, and other critical system components to improve system reliability and operational stability.
- Conduct periodic inspection, calibration, and preventive maintenance to identify and rectify faults before they develop into major system failures.

5.2. Operational Risk Mitigation

Operational risks are primarily associated with human error, inadequate training, and inefficient manufacturing processes. These risks can be reduced through the following measures:

- Provide comprehensive training programs to ensure that operators are familiar with manufacturing processes, equipment operation, and safety procedures.
- Develop and implement standardized operating procedures (SOPs) to maintain consistency and minimize operational errors.
- Perform regular supervision and continuous monitoring of manufacturing activities to identify process deviations and implement corrective actions at an early stage.

5.3. Cybersecurity Risk Mitigation

As smart manufacturing systems rely on

interconnected digital networks, effective cybersecurity measures are essential to protect manufacturing infrastructure and sensitive production data. Recommended measures include:

- Deploy firewalls, secure communication protocols, and data encryption techniques to protect manufacturing networks.
- Regularly update and patch software applications to reduce system vulnerabilities and defend against emerging cyber threats.
- Implement robust authentication and access control mechanisms to prevent unauthorized system access and protect critical manufacturing information.

5.4. Safety Risk Mitigation

Maintaining workplace safety remains a fundamental requirement in automated manufacturing environments. The following safety measures contribute to reducing occupational hazards:

- Install appropriate machine guarding systems to prevent accidental contact with moving or hazardous machine components.
- Provide emergency stop mechanisms that enable rapid shutdown of equipment during abnormal operating conditions.
- Ensure the use of appropriate personal protective equipment (PPE), including safety helmets, gloves, eye protection, and other protective devices required for specific manufacturing operations.

5.5. Schedule and Reliability Improvements

Proper production planning and maintenance scheduling play an important role in improving manufacturing reliability and minimizing unexpected downtime. The following practices are recommended:

- Establish preventive maintenance schedules to ensure timely inspection and servicing of manufacturing equipment.
- Develop backup systems for critical manufacturing operations to maintain production continuity during equipment failures.
- Introduce redundancy for essential system components wherever feasible to improve operational reliability and reduce the impact of unexpected failures.

Key Insight: The implementation of these mitigation strategies collectively reduces the high-priority risks identified through the qualitative risk assessment process. Their adoption contributes to improved system stability, reduced production downtime, enhanced workplace safety, and greater operational reliability in smart manufacturing environments.

6. Results and Discussion

The application of the qualitative risk matrix provides a systematic approach for identifying, evaluating, and prioritizing the major risks associated with smart manufacturing systems. By assessing each identified risk according to its probability of occurrence and potential impact, the proposed framework enables critical risks to be distinguished from lower-priority events, thereby supporting effective decision-making and resource allocation. The assessment identified sensor failures and cybersecurity threats as high-priority risks due to their significant influence on production continuity, system reliability, and operational safety.

The analysis highlights that although Industry 4.0 technologies have considerably improved manufacturing efficiency, productivity, and automation, they have also introduced additional technical and operational challenges. The increasing integration of intelligent machines, communication networks, and digital technologies requires systematic risk management to prevent disruptions that may affect manufacturing performance and workplace safety.

The mitigation strategies presented in Section 5 demonstrate practical approaches for reducing the identified risks. Predictive maintenance, continuous condition monitoring, preventive maintenance scheduling, and backup system implementation support early detection of potential failures and contribute to improved operational reliability. Similarly, operator training, standardized operating procedures, and effective human-machine coordination help reduce operational errors and improve process consistency. The adoption of machine guarding, emergency stop mechanisms, and appropriate personal protective equipment further strengthens workplace safety in automated manufacturing environments.

Effective risk management also contributes to reducing maintenance requirements, minimizing unexpected production

interruptions, and supporting efficient utilization of manufacturing resources. By identifying potential failures at an early stage and implementing appropriate mitigation measures, organizations can improve production continuity, enhance equipment reliability, and establish a safer and more resilient manufacturing environment.

The comparative analysis of the identified risk levels is presented in Figure 3, illustrating the relative priority assigned to each risk category based on the qualitative risk assessment framework.

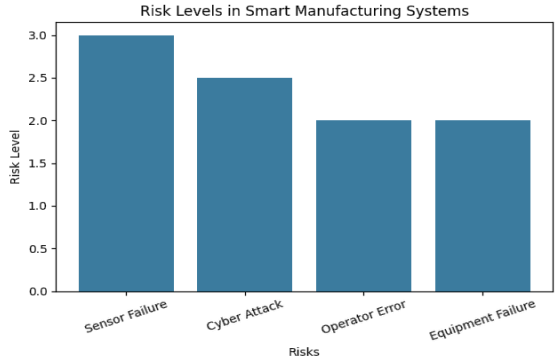

Figure 3: *Risk level comparison of identified risks in smart manufacturing systems.*

7. Conclusion

This paper presented a qualitative risk assessment framework for smart manufacturing systems using a risk matrix approach to identify, classify, and prioritize technical, operational, cybersecurity, and safety-related risks. The proposed framework provides a structured and practical method for evaluating potential manufacturing risks based on their likelihood of occurrence and operational impact, enabling organizations to prioritize critical issues and implement appropriate mitigation measures.

The study highlights that effective risk management plays an important role in improving manufacturing reliability, operational continuity, and workplace safety. The adoption of strategies such as predictive maintenance, cybersecurity enhancement, workforce training, preventive maintenance, and continuous monitoring supports the development of more resilient and sustainable Industry 4.0 manufacturing environments. Overall, the proposed framework serves as a practical reference for supporting risk-informed decision-making in modern smart manufacturing systems.

8. Future Scope

Future research may focus on integrating the proposed qualitative framework with quantitative risk assessment techniques to improve the accuracy of risk evaluation. The application of Industrial Internet of Things (IIoT), digital twins, artificial intelligence, and machine learning can further strengthen predictive risk analysis and real-time decision-making. In addition, validation of the proposed framework across diverse manufacturing sectors and industrial environments would enhance its practical applicability and support the development of intelligent, adaptive, and sustainable manufacturing systems.

References

[1] ISO 31000:2018, Risk Management: Guidelines. International Organization for Standardization, Geneva, Switzerland, 2018.

[2] IEC 60812:2018, Failure Modes and Effects Analysis (FMEA and FMECA). International Electrotechnical Commission, Geneva, Switzerland, 2018.

[3] IEC 61025:2006, Fault Tree Analysis (FTA). International Electrotechnical Commission, Geneva, Switzerland, 2006.

[4] IEC 61882:2016, Hazard and Operability Studies (HAZOP Studies): Application Guide. International Electrotechnical Commission, Geneva, Switzerland, 2016.

[5] PMI, A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 7th ed. Newtown Square, PA, USA: Project Management Institute, 2021.

[6] S. O. Duffuaa, A. Raouf, and J. D. Campbell, Planning and Control of Maintenance Systems: Modeling and Analysis. New York, NY, USA: Wiley, 1999.

[7] E. Zio, An Introduction to the Basics of Reliability and Risk Analysis. Singapore: World Scientific, 2007.

[8] K. Schwab, The Fourth Industrial Revolution. Geneva, Switzerland: World Economic Forum, 2016.

[9] L. Monostori, “Cyber-physical production systems: Roots, expectations and R&D challenges,” Procedia CIRP, vol. 17, pp. 9–13, 2014.

[10] F. Tao, Q. Qi, L. Wang, and A. Y. C. Nee, “Digital Twins and Cyber-Physical Systems toward Smart Manufacturing,” Engineering, vol. 5, no. 4, pp. 653–661, 2019.

[11] A. Somatkar and S. Mhatre, “Risk Analysis and Process Optimization in Toy

Manufacturing Using FMEA, Six Sigma, and Statistical Process Control," International Research Journal of Innovation in Science and Technology (IRJIST), vol. 1, no. 2, pp. 39–46, 2026.
[12] G. Sanap, V. Sanap, T. Patil, and A. Kadu, "Integrated Analytical Modeling of Material Removal Rate and Surface Roughness in Magnetic Levitation EDM of Ti-6Al-4V," International Research Journal of Innovation in Science and Technology (IRJIST), vol. 1, no. 2, pp. 32–38, 2026.
[13] K. U. Kotkar and V. V. Chahare, "Optimization of Roller Burnishing Parameters for Al7075 Using Hybrid Nanofluids: A Comparative Performance Study," International Research Journal of Innovation in Science and Technology (IRJIST), vol. 1, no. 2, pp. 180–188, 2026.
[14] V. D. Singare and A. A. Somatkar, "Design and Development of an Autonomous Machine Vision-Based Weed Detection and Removal Robot for Agriculture 4.0 Applications," International Research Journal of Innovation in Science and Technology (IRJIST), vol. 1, no. 2, pp. 80–86, 2026.
[15] B. S. Dhillon, Engineering Risk Management. London, UK: Springer, 2017.
[16] H. Kagermann, W. Wahlster, and J. Helbig, Recommendations for Implementing the Strategic Initiative Industrie 4.0. Frankfurt, Germany: Acatech, 2013.
[17] A. Hale and M. Guldenmund, "The application of safety management systems in manufacturing industries," Safety Science, vol. 44, no. 8, pp. 739–755, 2006.
[18] E. Hollnagel, Safety-I and Safety-II: The Past and Future of Safety Management. Farnham, UK: Ashgate Publishing, 2014.

Publisher's Note & Copyright