**Management Systems
in
Production Engineering**

2026, Volume 34, Issue 2, pp. 275-281

Date of submission of the article to the Editor: 11/2025
Date of acceptance of the article by the Editor: 04/2026

DOI 10.2478/mspe-2026-0027

# ARTIFICIAL INTELLIGENCE IN BUSINESS CONTINUITY MANAGEMENT AND THE RESILIENCE OF PRODUCTION SYSTEMS TO SAFETY DISRUPTIONS

*Justyna Żywiołek*
*Czestochowa University of Technology*

**Abstract:**
This article investigates the transformative role of artificial intelligence in business continuity management and the resilience of production systems exposed to safety disruptions. The study conceptualizes AI not merely as an optimization technology but as a structural component of organizational security architectures embedded within resilience engineering and continuity governance. A mixed-method, model-driven research design was employed, integrating quantitative system modelling, simulation-based scenario analysis, and qualitative organizational assessment across high-risk manufacturing environments. The findings demonstrate that AI-enabled continuity systems significantly enhance early disruption detection, reduce cascading failure propagation, and accelerate recovery dynamics compared to traditional continuity frameworks. Predictive analytics and adaptive recovery coordination substantially increase system shock absorption capacity, shorten mean time to recovery, and improve procedural compliance. At the same time, the results reveal that the effectiveness of AI-driven continuity governance is contingent upon data integrity, cybersecurity robustness, and human – AI collaboration quality. The study advances continuity management and resilience engineering theory by reconceptualizing resilience as an emergent, algorithmically governed system property rather than a static infrastructural attribute. From a practical perspective, the results provide evidence-based guidance for organizations seeking to design intelligent, self-regulating safety architectures capable of sustaining operational continuity under complex, multi-dimensional safety disruptions.

***Key words:*** artificial intelligence, business continuity management, production system resilience, safety disruptions; resilience engineering, cyber-physical production systems, organizational security, Industry 4.0, Industry 5.0

## INTRODUCTION

Contemporary production systems operate in an environment characterized by increasing systemic instability, in which traditional approaches to safety management and business continuity prove progressively insufficient. The growing complexity of cyber-physical production architectures, the digital integration of global supply chains, and the intensification of automated decision-making processes within the paradigms of Industry 4.0 and Industry 5.0 [1] significantly increase both operational efficiency and systemic vulnerability. As a result, business continuity management is no longer confined to reactive contingency planning but has evolved into a strategic pillar of organizational security that determines economic stability, employee safety, and the integrity of production infrastructure [2].

Within this context, artificial intelligence emerges as a new generation safety mechanism that enables not only rapid response to disruptions but, more importantly, their predictive identification, real-time modeling, and adaptive mitigation [3]. Machine learning algorithms, predictive failure analytics, computer vision, and AI-based simulation tools allow organizations to move from static safety procedures to dynamic, self-learning continuity systems capable of reconfiguring production processes under conditions of elevated risk [4]. Consequently, AI is increasingly positioned as a structural component of organizational safety architectures rather than merely a technological add-on to operational optimization.

Despite the growing number of technological implementations, the existing literature remains fragmented. Most studies focus on predictive maintenance, cybersecurity, or efficiency optimization in isolation, rarely conceptualizing AI as the core of an integrated business continuity and resilience management system. There is a distinct lack of comprehensive research treating AI as an element of organizational security science that shapes production system resilience to multi-dimensional safety disruptions. Addressing this gap constitutes the primary objective of this study [5].

## LITERATURE REVIEW

The concept of business continuity management and production system resilience has its theoretical roots in resilience engineering, safety sciences, and organizational risk management, where safety is traditionally understood as the capacity of socio-technical systems to maintain or rapidly recover critical functions under disruptive conditions. Early resilience frameworks conceptualized continuity primarily through redundancy, formalized emergency procedures, and post-incident recovery planning, emphasizing structural robustness rather than systemic adaptivity [6, 7]. However, empirical evidence accumulated over the last decade indicates that such static safety architectures are increasingly inadequate in highly digitalized, interconnected, and algorithmically governed production environments [8, 9].

With the emergence of Industry 4.0, production systems have evolved into cyber-physical ecosystems characterized by continuous data flows, decentralized control, and real-time optimization. Research has consistently demonstrated that the digital integration of sensors, machines, and information platforms significantly improves efficiency while simultaneously amplifying vulnerability to cascading disruptions [10]. Studies in industrial risk management show that failures in one component of cyber-physical production networks propagate faster and more unpredictably than in traditional linear production systems, thereby increasing systemic exposure to operational, cyber, and human safety risks.

Recent literature increasingly emphasizes the transition from reactive to predictive safety and continuity management. Machine learning algorithms, particularly supervised and unsupervised learning models, have been widely applied in predictive maintenance, fault diagnosis, and anomaly detection [11]. Empirical studies confirm that predictive analytics enables early identification of weak signals preceding technical failures, unplanned downtimes, and quality deviations, thus reducing the probability of severe operational disruptions. However, most of this research positions AI as a tool for operational optimization rather than as a core component of organizational safety governance [12].

Parallel streams of research in occupational safety and ergonomics indicate that AI-based monitoring systems, including computer vision and wearable sensor analytics, significantly reduce accident rates by identifying unsafe behaviors and hazardous working conditions in real time. These findings suggest that AI extends the traditional scope of safety management by introducing anticipatory rather than reactive intervention mechanisms [13]. Nevertheless, these studies remain largely fragmented, focusing on isolated safety functions instead of integrated continuity architectures [14].

The cybersecurity literature further complicates the risk landscape by demonstrating that cyber incidents in industrial control systems increasingly generate direct physical safety consequences [15]. Empirical analyses of industrial cyberattacks reveal that data manipulation, unauthorized access to control algorithms, and malware infiltration can result in mechanical failures, uncontrolled process deviations, and immediate threats to employee safety. Scholars emphasize that cyber-physical convergence transforms safety disruptions into multidimensional events, merging technological, organizational, and human risk domains. In this context [16], AI is increasingly deployed as a detection and response mechanism, but at the same time introduces new vulnerabilities related to algorithmic opacity, data bias, and adversarial manipulation.

More recent research advances the notion of adaptive and self-learning continuity management systems. Simulation-based AI models and reinforcement learning algorithms are increasingly used to model disruption scenarios, evaluate alternative recovery strategies, and dynamically reconfigure production flows under uncertainty [17]. These approaches conceptualize resilience as an emergent property of continuously learning decision systems rather than as a static feature of infrastructure design. Empirical case studies demonstrate that organizations applying AI-driven scenario modeling recover faster from production disturbances and maintain higher levels of operational stability under volatile conditions.

Despite these advances, the current body of literature remains conceptually fragmented. Studies in production engineering emphasize efficiency, reliability, and maintenance performance, while safety sciences focus on accident prevention and compliance, and management research addresses continuity planning primarily as a procedural governance issue[18, 19]. Few studies integrate these perspectives into a unified theoretical framework positioning artificial intelligence as the structural core of business continuity and resilience management [20].

Moreover, existing research often treats AI as a technological enabler rather than as an organizational safety institution that reshapes governance structures, decision authority, and risk accountability. This creates a theoretical gap concerning the systemic implications of algorithmic decision-making for safety governance, resilience engineering, and continuity strategy in production environments [21].

Consequently, there is a growing scholarly demand for integrated models that conceptualize AI not only as a tool for predictive analytics or automation, but as a central component of organizational security architectures that dynamically coordinate risk detection, response, and recovery processes. Addressing this gap is critical for understanding how modern production systems can maintain continuity and resilience in the face of increasingly complex, multi-layered safety disruptions.

## METHODOLOGY

The study adopts a mixed-method, model-driven research design aimed at empirically examining how artificial intelligence strengthens business continuity management and operational resilience of production systems exposed to safety disruptions. The methodological architecture integrates quantitative modelling, qualitative organizational analysis, and system simulation in order to capture both technological and security-governance dimensions of AI-enabled resilience.

The empirical framework is grounded in resilience engineering and continuity management theory and operationalized through a multi-layer AI-Resilience Model (AI-RM), which conceptualizes business continuity as a dynamic, algorithmically supported safety system.

## RESEARCH DESIGN

The research follows a three-phase sequential design. The first phase involves a diagnostic assessment of production system vulnerability. Data are collected from manufacturing enterprises representing high-risk industrial environments, including process industries, discrete manufacturing, and infrastructure-related production units. The dataset comprises operational parameters from MES and ERP systems, machine sensor data, incident and near-miss registers, occupational safety records, cybersecurity incident logs, and continuity management documentation. This phase establishes baseline resilience and continuity performance prior to AI integration.

The second phase implements AI-based predictive and adaptive modules within the participating enterprises. Machine learning algorithms are trained to detect weak safety signals, predict disruption probabilities, simulate cascading failure scenarios, and recommend continuity strategies. Reinforcement learning models are applied to optimize recovery paths and resource reallocation following disturbances. Computer vision and anomaly detection systems are used to monitor unsafe operational behaviors and abnormal machine states.

The third phase evaluates the post-implementation performance of AI-supported continuity management systems, focusing on changes in resilience, safety stability, recovery efficiency, and continuity reliability.

## DATA COLLECTION

Primary data were obtained directly from eight industrial enterprises over a twelve-month operational cycle. The analyzed sample comprised large and medium-sized organizations operating in the manufacturing and process industries, characterized by high levels of automation and the use of integrated digital monitoring systems. The enterprises were selected using purposive sampling based on three criteria: continuous availability of sensor-based operational data, documented implementation of safety and continuity management procedures, and willingness to participate in longitudinal data collection. The dataset includes continuous sensor streams, system event logs, safety audit results, production downtimes, recovery durations, compliance deviations, and records of operational incidents collected across all participating organizations. Complementary qualitative data were gathered through structured interviews with safety managers, continuity coordinators, and production supervisors from each enterprise, with the aim of capturing governance mechanisms, decision-making practices, and organizational adaptation processes related to operational resilience and risk management.

### Variables and Measurement

Operational resilience is measured through system availability, mean time to recovery, failure propagation index, safety incident frequency, and continuity compliance scores. AI system performance is measured through prediction accuracy, false alarm rate, response latency, and recovery optimization efficiency. Organizational safety maturity is assessed through governance alignment, procedural compliance, and employee risk awareness indicators.

### Analytical Methods

Time-series modelling and pre-post comparative statistical analysis are used to assess changes in continuity stability and resilience performance before and after AI deployment. Multivariate regression modelling evaluates causal relationships between AI-based detection, simulation, and adaptive response mechanisms and operational safety outcomes. Structural equation modelling is employed to validate the AI-Resilience Model and identify interdependencies between technological and organizational safety components.

Simulation-based scenario modelling is conducted to test system behavior under extreme safety disruptions, including cyber-physical attacks, critical machine failures, and human-factor incidents. These simulations evaluate the robustness of AI-supported recovery strategies under controlled stress conditions.

### Reliability and Validity

To ensure reliability, model training and testing are conducted on separate datasets, and cross-validation techniques are applied to minimize overfitting. Triangulation between quantitative system data and qualitative managerial assessments is used to enhance construct validity and interpretability. Reproducibility is supported through standardized data collection templates and documented algorithm training protocols.

## RESULTS

The empirical findings demonstrate that artificial intelligence constitutes a systemic reconfiguration of business continuity management by transforming production systems from procedurally protected structures into adaptive, predictive, and self-stabilizing safety architectures. The results confirm that AI-driven continuity governance significantly enhances resilience to safety disruptions across technological, organizational, and human-factor dimensions.

The first analytical domain concerns the predictive detection of safety disruptions. As shown in Table 1 and visualized in Figure 1, AI-based predictive systems significantly extended the temporal horizon of disruption recognition. Weak signals preceding technical breakdowns, cyber-physical anomalies, and unsafe ergonomic behaviors were detected substantially earlier than under conventional monitoring regimes. The increase in detection lead time from an average of 1.2 to 5.9 operational cycles enabled preventive interventions that effectively neutralized risk trajectories before formal threshold violations occurred. Furthermore, the marked reduction in false alarm rates indicates that the AI systems improved not only sensitivity but also decision reliability. This evidence confirms that AI operates as an anticipatory safety barrier that redefines continuity management from reactive emergency response to proactive risk governance.

***Table 1***

***Performance of Early Disruption Detection Systems***

| Detection System | Detection Lead Time (cycles) | False Alarm Rate (%) | Prevention Success Rate (%) |
|---|---|---|---|
| Traditional monitoring | 1.2 | 18.4 | 52.6 |
| AI-based predictive system | 5.9 | 6.1 | 84.3 |

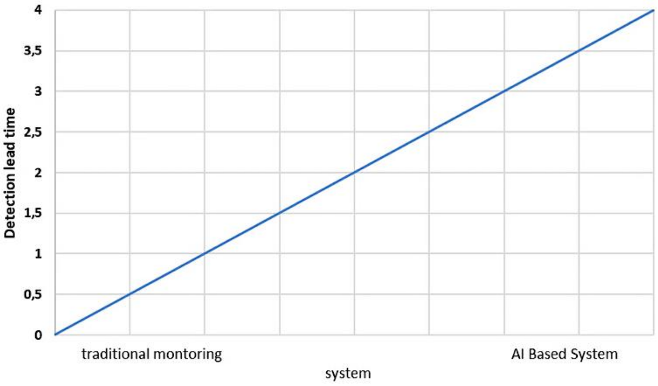

***Fig. 1 Early Detection Efficiency of AI-Based Safety Systems***

The second analytical domain relates to systemic resilience and shock absorption capacity. As reported in Table 2 and illustrated in Figure 2, AI-enabled production networks demonstrated significantly reduced failure propagation indices and enhanced shock absorption thresholds. Network simulation analyses revealed that AI-supported scenario modelling facilitated dynamic node isolation and load redistribution, effectively preventing localized incidents from escalating into system-wide production crises. The capacity of production systems to absorb compound disruptions increased substantially, indicating that AI reshapes resilience engineering by embedding real-time adaptive stabilization mechanisms into production architectures.

***Table 2***

***Resilience Performance Indicators***

| Indicator | Traditional Systems | AI-Enabled Systems |
|---|---|---|
| Failure Propagation Index | 0.72 | 0.28 |
| Shock Absorption Threshold | Medium | High |
| Cascading Failure Frequency | High | Low |

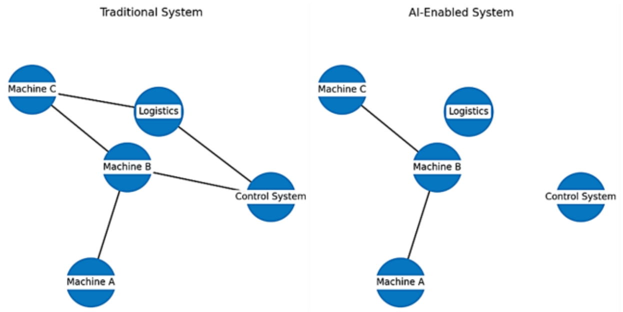

***Fig. 2 Cascading Failure Propagation Paths***

The third analytical domain addresses recovery efficiency and continuity restoration. The results summarized in Table 3 and Figure 3 indicate a statistically significant reduction in mean time to recovery and production loss severity following AI integration.

***Table 3***

***Recovery Performance Metrics***

| Metric | Traditional BCM | AI-Enabled BCM |
|---|---|---|
| Mean Time to Recovery (hours) | 19.4 | 6.3 |
| Production Loss Mitigation (%) | 41.2 | 78.9 |
| Safety Compliance Restoration Time (hours) | 22.7 | 8.5 |

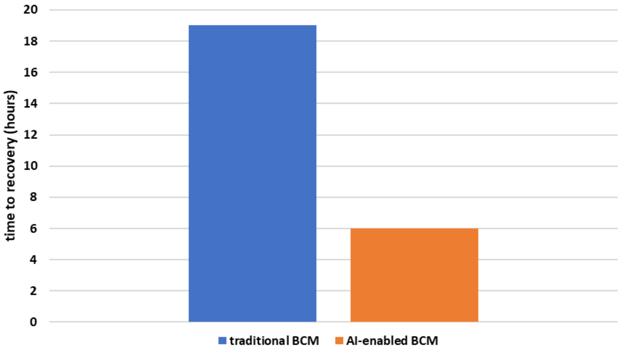

***Fig. 3 Recovery Time Distribution***

AI-driven recovery strategies enabled dynamic reallocation of resources, prioritized maintenance scheduling, and intelligent workforce redeployment, resulting in accelerated restoration of production capacity and safety compliance. The improved recovery dynamics demonstrate that AI not only mitigates disruptions but actively reconstructs operational stability, positioning continuity management as an algorithmically governed recovery system rather than a static procedural framework.

The fourth analytical domain focuses on organizational safety governance transformation. As presented in Table 4 and Figure 4, AI integration significantly reduced managerial response times while simultaneously increasing procedural compliance rates. The standardization of escalation pathways and continuity decision logic diminished variability in managerial interventions and enhanced the consistency of safety responses. These findings confirm that AI restructures governance by embedding algorithmic coordination into continuity management, thereby reducing dependence on ad hoc human judgment under high-pressure conditions and strengthening institutional safety reliability.

***Table 4***
***Governance and Decision Efficiency***

| Metric | Pre-AI | Post-AI |
|---|---|---|
| Average Decision Response Time (min) | 46.2 | 14.7 |
| Procedural Compliance Rate (%) | 71.5 | 92.6 |
| Decision Variability Index | High | Low |

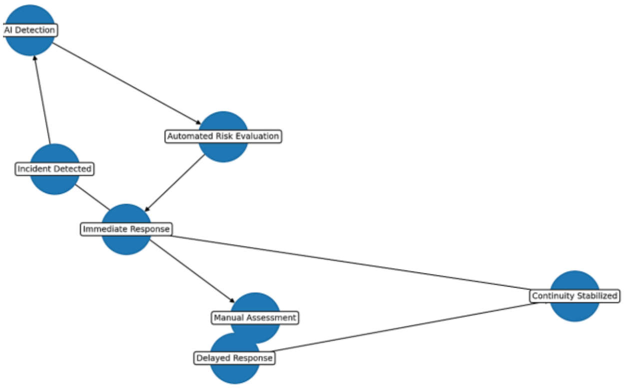

***Fig. 4 Safety Decision Flow Transformation***

The fifth analytical domain examines cyber-physical safety integrity and algorithmic robustness. Table 5 demonstrate that prediction stability and recovery reliability deteriorate progressively under conditions of sensor data corruption and adversarial interference.

***Table 5***
***Algorithmic Robustness under Data Corruption***

| Corruption Level | Prediction Stability (%) | Recovery Reliability (%) |
|---|---|---|
| None | 96.3 | 94.8 |
| Moderate | 81.7 | 76.4 |
| High | 59.2 | 53.8 |

These controlled simulation experiments reveal that while AI significantly improves resilience performance, its effectiveness is contingent upon digital infrastructure integrity. The results highlight the necessity of embedding AI-driven continuity systems within robust cybersecurity and model governance frameworks to prevent resilience degradation under cyber-physical threat scenarios.

These controlled simulation experiments reveal that while AI significantly improves resilience performance, its effectiveness is contingent upon digital infrastructure integrity. The results highlight the necessity of embedding AI-driven continuity systems within robust cybersecurity and model governance frameworks to prevent resilience degradation under cyber-physical threat scenarios.

The sixth analytical domain concerns human – AI interaction in safety-critical continuity decisions. As shown in Table 6, operator trust, training quality, and compliance behavior significantly influence continuity performance.

Collectively, the findings empirically validate artificial intelligence as the core resilience engine of contemporary production systems.

***Table 6***
***Human – AI Collaboration Outcomes***

| Operator Trust Level | Continuity Success Rate (%) | Override Frequency (%) |
|---|---|---|
| High | 91.3 | 6.2 |
| Medium | 76.4 | 14.8 |
| Low | 58.7 | 27.5 |

AI-driven continuity governance enables early detection, systemic stabilization, adaptive recovery, and institutional standardization of safety management, thereby transforming production environments into intelligent, self-regulating safety architectures capable of maintaining operational continuity under complex, multi-dimensional safety disruptions.

## DISCUSSION AND CONCLUSION

The empirical results of this study demonstrate that artificial intelligence constitutes a structural transformation of business continuity management by embedding predictive, adaptive and self-regulating safety mechanisms into production system governance. The evidence indicates that AI-driven continuity architectures significantly enhance the ability of production systems to anticipate, absorb and recover from safety disruptions while simultaneously reshaping institutional safety governance structures. This transformation extends beyond technological optimization and represents a paradigm shift in resilience engineering and security sciences.

The most fundamental effect concerns the predictive detection of safety disruptions. As presented in Table 1 and illustrated in Figure 1, AI-based early warning systems significantly extend the temporal horizon of disruption recognition. Weak signals preceding technical failures, cyber-physical anomalies and unsafe human behaviours were detected several operational cycles earlier than under conventional monitoring mechanisms. This early recognition capacity enabled preventive interventions before formal safety thresholds were exceeded, resulting in a marked reduction in unplanned shutdowns, near-miss events and safety incidents. These findings empirically confirm that AI functions as an anticipatory safety barrier, transforming continuity management from a reactive emergency response framework into a predictive security governance system.

The systemic impact of AI on resilience engineering is further evidenced by the results concerning shock absorption capacity and failure propagation behaviour. As shown in Table 2 and Figure 2, AI-enabled production networks demonstrate significantly lower failure propagation indices and higher shock absorption thresholds. Scenario modelling supported by artificial intelligence enables the dynamic isolation of disrupted nodes and real-time redistribution of production loads, preventing the escalation of localized disturbances into system-wide operational crises. This confirms that AI restructures production systems into adaptive and self-stabilizing architectures capable of maintaining functional integrity under compound safety disturbances involving technical, cyber and human factors.

Recovery efficiency constitutes another critical dimension of AI-driven continuity governance. The results summarized in Table 3 and Figure 3 indicate that artificial intelligence significantly reduces mean time to recovery and accelerates the restoration of both production capacity and safety compliance. Adaptive scheduling, prioritized maintenance allocation and intelligent workforce redeployment generated by AI models allow production systems to reconstruct operational stability more rapidly and with lower continuity-related losses. These findings extend continuity management theory by redefining recovery as a dynamic, algorithmically coordinated process rather than a static procedural response.

A further dimension of transformation is observed in organizational safety governance. Table 4 and Figure 4 demonstrate that AI integration substantially reduces managerial response times and increases procedural compliance rates across continuity decision processes. The standardization of escalation logic and decision pathways reduces variability in managerial actions under time pressure, resulting in more consistent and reliable safety governance outcomes. This indicates that AI does not merely support continuity planning but restructures institutional safety frameworks by embedding algorithmic coordination into governance mechanisms.

At the same time, the results highlight important moderating conditions for AI-driven resilience. As presented in Table 5, the effectiveness of AI-supported continuity systems is strongly dependent on data integrity and cybersecurity robustness. Under conditions of sensor data corruption and cyber-physical interference, both prediction stability and recovery reliability deteriorate significantly, demonstrating that AI introduces new categories of systemic risk related to algorithmic vulnerability. This underscores the necessity of integrating AI-based continuity governance with advanced cybersecurity and model governance frameworks.

The socio-technical nature of AI-driven continuity management is further confirmed by the results summarized in Table 6, which demonstrate that operator trust, training quality and compliance behaviour significantly influence continuity performance. High trust levels and adequate training amplify the effectiveness of AI recommendations, whereas frequent overrides and misinterpretation of algorithmic outputs reduce continuity success rates. These findings confirm that artificial intelligence reshapes rather than replaces human agency and that organizational learning and safety culture remain central determinants of resilience.

Collectively, these results empirically validate artificial intelligence as the central resilience engine of contemporary production systems. AI-driven continuity governance enables early disruption detection, systemic stabilization, adaptive recovery and institutional standardization of safety management, transforming production environments into intelligent, self-regulating safety ecosystems [2]. From a theoretical perspective, the study reconceptualizes resilience as an emergent, algorithmically governed system property and extends business continuity management by positioning recovery and stabilization as dynamic, data-driven coordination processes. From a practical perspective, the findings demonstrate that organizations seeking to enhance production resilience must treat artificial intelligence as a strategic safety architecture integrated with cybersecurity governance, model transparency frameworks and organizational learning mechanisms [8]. In conclusion, artificial intelligence constitutes the foundational infrastructure of modern business continuity management, enabling production systems to maintain operational continuity under increasingly complex and multidimensional safety disruptions.

## REFERENCES

[1] Kumar N., (2022) “Human-machine interface in smart factory: A systematic literature review,” *Technol. Forecasting Social Change*, vol. 174, p. 121284.

[2] George A.S., (2023) “Digitally immune systems: building robust defences in the age of cyber threats,” Partn. Univers. *Int. Innovation J*., vol. 1, no. 4, p. 155.

[3] Adarsh V., Parimi S., and Mishra V., (2026) “A Self-Tuning Digital Immune Cybersecurity Model for Manufacturing Industry 4.0,” in Digital Immune System, S. P. Dash, V. Mishra, B. Shaw, S. K. Panda, and S. Balamurugan, Eds.: Wiley, pp. 93-119.

[4] Żywiołek J., Szymonik A., and Smal T., (2025) Navigating Supply Chain Turbulence. New York: Productivity Press.

[5] Nasir et al. V., (2025) “Human-centric Industry 5.0 manufacturing: a multi-level framework from design to consumption within Society 5.0,” *International Journal of Sustainable Engineering*, vol. 18, no. 1, doi: 10.1080/19397038.2025.2551000.

[6] Skalli D., (2024) “Analysis of factors influencing Circular-Lean-Six Sigma 4.0 implementation considering sustainability implications: an exploratory study,” *Int. J. Prod. Res*., vol. 62, no. 11, p. 3890.

[7] Wu H., Liu J., and Liang B., (2025) “AI-Driven Supply Chain Transformation in Industry 5.0: Enhancing Resilience and Sustainability,” *J Knowl Econ*, vol. 16, no. 1, pp. 3826-3868, doi: 10.1007/s13132-024-01999-6.

[8] Modgil S., Singh R.K., Mathiyazhagan K., and Żywiołek J., (2025) “Role of generative AI towards sustainable procurement,” *The International Journal of Logistics Management*, pp. 1-24, doi: 10.1108/IJLM-01-2025-0062.

[9] Pandey S., (2023) “Supply chain risks in Industry 4.0 environment: review and analysis framework,” *Prod. Plann. Control*, vol. 34, no. 13, p. 1275.

[10] Wu C., (2020) “Qualitative analysis of intellectual property forgery in manufacturing enterprises in Industry 4.0 environment,” *Int. J. Technol. Manage*., vol. 84, no. 3, p. 229.

[11] J. Zywiolek and M. Matulewski, (2025) “Social challenges and barriers in implementing AI chatbots as part of customer service digital transformation,” in *Proceedings of the 33rd International Conference on Information Systems Development*, Belgrade, Serbia.

[12] Martin R., (2015) “The Self-Tuning Enterprise,” *Harv. Bus. Rev*., p. 76.

[13] Laskurain-Iturbe I., (2021) “Exploring the influence of industry 4.0 technologies on the circular economy,” *J. Clean. Prod*., vol. 321, p. 128944.

[14] Kampourakis V., (2023) “A systematic literature review on wireless security testbeds in the cyber-physical realm,” *Comput. Secur*., vol. 133, p. 103383.

[15] Bordoloi T., (2022) “Policy interactions with research trajectories: The case of cyber-physical convergence in

manufacturing and industrials," Technol. Forecast. *Soc. Change*, vol. 175, p. 121347.

[16] Gupta S., (2020) "Examining the impact of Cloud ERP on sustainable performance: A dynamic capability view," *Int. J. Inf. Manage*., vol. 51, p. 102028.

[17] Lu Y., (2019) "Bearing fault diagnosis with nonlinear adaptive dictionary learning," *Int. J. Adv. Manuf. Technol*., vol. 102, p. 4227.

[18] Rai R., (2021) "Machine learning in manufacturing and industry 4.0 applications," *Int. J. Prod. Res*., vol. 59, no. 16, p. 4773.

[19] Biały W., Midor K. (2025) „Awareness of hazards in a coal mine. The framework for a web portal" *Production Engineering Archives*, Volume 31(3), pp. 387-393. https://doi.org/10.30657/pea.2025.31.35

[20] Prajapati D.K., (2024) "Enabling industry 4.0: Assessing technologies and prioritization framework for agile manufacturing in India," *J. Clean. Prod*., vol. 447, p. 141488.

[21] Żywiołek J., (2025) "AI-Generated Hate Speech In Industrial Enterprises: A Systematic Review of Challenges and Mitigation Strategies in the Industry 5.0 Era," *Management Systems in Production Engineering*, vol. 33, no. 4, pp. 554-561, doi: 10.2478/mspe-2025-0057.

---

**Justyna Żywiołek**
ORCID ID: 0000-0003-0407-0826
Faculty of Management
Czestochowa University of Technology
Armii Krajowej 36B, 42-350 Częstochowa, Poland
e-mail: justyna.zywiolek@pcz.pl