SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 216

CONTINUOUS IMPROVEMENT: LEVERAGING DATA SECURITY IN INDUSTRY 4.0 SETTINGS

Justyna ŻYWIOŁEK

Faculty of Management, University of Technology; justyna.zywiolek@pcz.pl, ORCID: 0000-0003-0407-0826

Purpose: This study aims to explore the critical role of data security in continuous improvement within Industry 4.0 settings. It focuses on identifying how robust data security practices enable organizations to enhance operational efficiency, foster innovation, and protect sensitive information assets. Additionally, the research highlights the interplay between technological advancements, regulatory compliance, and proactive risk management in achieving sustainable organizational growth.

Design/methodology/approach: The research adopts a mixed-method approach to investigate the role of data security in continuous improvement within Industry 4.0. A comprehensive literature review was conducted to identify key theoretical frameworks and best practices related to cybersecurity and continuous improvement. The study also incorporates case analysis of Industry 4.0 technologies, such as IoT, AI, and big data analytics, highlighting their integration with data security strategies. By analyzing real-world applications and leveraging predictive analytics and compliance audits, the research demonstrates how secure data practices can enhance organizational performance and foster innovation.

Findings: The study identifies that data security is an indispensable component of continuous improvement in Industry 4.0. Secure data practices enhance decision-making, promote operational resilience, and enable proactive risk mitigation. Moreover, they support compliance with regulatory frameworks, such as GDPR and ISO 27001, while fostering a culture of innovation and trust among stakeholders. The findings also reveal significant challenges, including technological complexity, resource constraints, and rapidly evolving cyber threats.

Research limitations/implications: The research is limited by the availability of empirical data on specific Industry 4.0 applications. Future studies could expand on the practical implementation of data security measures across diverse industries and explore the economic implications of continuous improvement strategies. Additional research on emerging technologies, such as blockchain and quantum computing, could further enrich the understanding of secure data management.

Practical implications: The study provides actionable insights for businesses seeking to integrate data security into their continuous improvement processes. It emphasizes the importance of investing in advanced security technologies, workforce training, and compliance frameworks to enhance organizational resilience. These recommendations are particularly relevant for enterprises navigating the complexities of Industry 4.0.

Originality/value: This paper contributes to the literature by linking data security directly with continuous improvement in Industry 4.0. It offers a novel perspective on the strategic importance of secure data practices, supported by both theoretical insights and practical applications. The findings are valuable to researchers, policymakers, and industry leaders focused on sustainable growth and technological innovation.
Keywords: Data Security, Continuous Improvement, Industry 4.0, Cybersecurity, Operational Resilience.
Category of the paper: Viewpoint.

1. Introduction

Continuous improvement within the framework of Industry 4.0 emphasizes the strategic use of advanced technologies to drive operational efficiency, foster innovation, and safeguard critical information assets. Industry 4.0, characterized by the integration of the Internet of Things (IoT), artificial intelligence (AI), and big data analytics, has reshaped industrial processes and information flow management (Shahin et al., 2020). Central to this evolution is the ability to secure and utilize vast amounts of data generated by interconnected systems and devices, which is essential for maintaining operational continuity and driving continuous improvement (Żywiołek, 2024c).

Data security plays a pivotal role in enabling continuous improvement in Industry 4.0 environments. As organizations increasingly depend on real-time data from sensors, production systems, customer interactions, and supply chains, ensuring the security and integrity of this information becomes fundamental. According to Żywiołek (Żywiołek, 2024b), secure data management practices not only protect organizational assets from external and internal threats but also ensure the reliability of insights derived from analytics, which are critical for informed decision-making and process optimization. Similarly, Shafig et al. (Shafiq et al., 2016) emphasize that real-time data security is critical for enabling the integration of smart systems and for maintaining the efficiency of Industry 4.0 operations.

The integration of data security into continuous improvement processes offers organizations the ability to proactively manage risks, enhance compliance with international standards such as ISO 27001, and foster trust among stakeholders (Żywiołek et al., 2023). As noted by Xu et al. (2018), the dynamic and interconnected nature of Industry 4.0 demands robust cybersecurity frameworks to mitigate vulnerabilities that can disrupt operations and compromise sensitive data. Wolniak similarly highlights that secure data practices are vital in addressing the challenges posed by an evolving cyber threat landscape, where new vulnerabilities can quickly undermine technological advancements (Wolniak et al., 2024).

At the same time, continuous improvement in Industry 4.0 is fundamentally about leveraging advanced data-driven approaches, such as business analytics, to refine operations and foster innovation. The vast volumes of data generated by interconnected systems reveal

patterns and trends that can inform decision-making and enhance process optimization (Tortorella et al., 2021; Rosin et al., 2020). By combining data security with predictive analytics, organizations can forecast potential vulnerabilities and proactively address them, minimizing downtime and extending the lifecycle of critical assets (Vinodh et al., 2021; Miqueo et al., 2020). Bai et al. further argue that predictive analytics in secure environments enables not only operational continuity but also strategic decision-making aligned with Industry 4.0 principles (Bai et al., 2020).

Moreover, secure data management supports a deeper understanding of customer behavior, facilitating tailored solutions and improved experiences, while fostering a culture of data-driven innovation (Frank et al., 2019). This culture, central to continuous improvement, encourages ongoing refinements and iterative enhancements that are essential for maintaining competitiveness and achieving sustained growth (Da Costa et al., 2019). Rossini underscores the role of secure data analytics in driving innovation while ensuring compliance with regulatory frameworks, which is critical in the context of global Industry 4.0 adoption (Rossini et al., 2019).

Despite its transformative potential, implementing data security within Industry 4.0 is not without challenges. Technological complexity, high implementation costs, and the rapid evolution of cyber threats require organizations to adopt a strategic and proactive approach (Żywiołek, 2024a; Valamede, 2020). Additionally, regulatory compliance with frameworks such as GDPR and ISO standards imposes administrative and operational burdens, further underscoring the need for a skilled workforce and robust risk management practices.

This publication explores the critical role of data security in supporting continuous improvement within Industry 4.0 settings. By highlighting the interplay between technological advancements, regulatory compliance, and organizational resilience, this study underscores the necessity of leveraging data security to drive innovation, maintain competitiveness, and achieve sustained operational excellence.

2. Selected aspects of using business analytics to ensure the security of information resources

Business analytics plays a pivotal role in ensuring the security of information resources by enabling organizations to proactively identify vulnerabilities, detect threats, and implement robust security measures. By leveraging advanced analytical tools, organizations can analyze vast amounts of data in real time, uncovering patterns and anomalies that may indicate potential security breaches (Mrugalska, Wyrwicka, 2017). Predictive analytics, for example, can forecast emerging cyber threats by analyzing historical data and identifying trends, allowing organizations to adopt preemptive measures to mitigate risks before they materialize (Mayr et al., 2018).

One critical application of business analytics in information security is monitoring network activity to detect and respond to potential intrusions. Analytical tools can continuously assess traffic patterns, identifying deviations from normal behavior that may signify malicious activity (Meister et al., 2019). For instance, if a sudden surge in data access requests from a particular IP address is detected, analytics can flag this anomaly for further investigation, helping to prevent data breaches. Similarly, machine learning algorithms can differentiate between legitimate user behavior and unauthorized access attempts, enhancing authentication processes and safeguarding sensitive information (Taylor et al., 2019).

Another significant aspect is the use of business analytics to evaluate the effectiveness of existing security protocols. By analyzing data related to past incidents, organizations can identify gaps in their defenses and optimize their security strategies (Tuominen, 2016). For example, root cause analysis of security breaches enables organizations to pinpoint weaknesses in their infrastructure and implement targeted improvements, such as updating outdated software or strengthening encryption methods. Business analytics also supports compliance with information security standards, such as ISO 27001 and GDPR (Żywiołek et al., 2022). Analytical tools can streamline the process of tracking and reporting on compliance metrics, ensuring that organizations adhere to regulatory requirements. This not only minimizes the risk of legal penalties but also enhances stakeholder trust in the organization's commitment to safeguarding information resources.

In addition, the integration of business analytics within Industry 4.0 and digital transformation initiatives fosters a culture of proactive information security. Employees across all organizational levels can access real-time insights into security risks and recommended actions, enabling a more collaborative and responsive approach to information protection. This democratization of data empowers teams to make informed decisions that align with the organization's broader security objectives.

Lastly, the iterative nature of continuous improvement in information security is well-supported by business analytics. Analytical tools enable organizations to measure the impact of implemented changes, refine their strategies based on new data, and adapt to evolving threats. This cyclical process ensures that information security remains dynamic and resilient in the face of emerging challenges.

By leveraging the capabilities of business analytics, organizations can ensure the security of their information resources, fostering trust, compliance, and operational excellence in an increasingly data-driven world.

Table 1.
The Usage of Business Analytics in Ensuring the Security of Information Resources

Aspect	Description of Usage of Business Analytics
Threat Detection	Business analytics tools monitor and analyze network activity in real-time to identify anomalies or suspicious patterns indicative of cyber threats.
Vulnerability Analysis	Predictive analytics assess historical security data to identify potential system vulnerabilities, enabling proactive mitigation measures.
Compliance Monitoring	Analytics tools track compliance with regulations like GDPR or ISO 27001, providing reports and alerts to ensure adherence to legal standards.
Incident Response	Business analytics provides real-time insights into security incidents, enabling rapid response and containment of potential breaches.
Access Control	Analytical tools assess user behavior to detect unauthorized access attempts, enhancing identity verification and access management processes.
Data Encryption Optimization	Analytics evaluate data encryption protocols and usage to ensure robust security measures are in place for sensitive information.
System Health Monitoring	Predictive analytics monitor the performance and health of IT systems, identifying risks of hardware or software failures that could compromise security.
Employee Behavior Analysis	Analytics tools evaluate patterns of employee activity to detect insider threats or unintentional security lapses, promoting a secure organizational environment.
Incident Root Cause Analysis	Post-incident analytics identify the root cause of breaches, guiding the improvement of security policies and preventive measures.
Security Training Assessment	Data analytics evaluate the effectiveness of cybersecurity training programs, ensuring employees are equipped to handle potential threats.

3. Software used in continuous improvement analysis for information security in enterprises

Analytical software plays a crucial role in the process of continuous improvement in ensuring the security of information resources in enterprises operating under Industry 4.0 conditions. The application of advanced analytical tools enables the transformation of raw data into actionable insights that support decision-making, process monitoring, and the identification of potential (Khan et al., 2024; Iuga, Rosca, 2017; Ito, 2020). Tools such as Tableau, Power BI, Qlik Sense, and SAS Analytics are particularly significant in processes related to the analysis of data concerning information security.

Tableau, as an advanced data visualization tool, enables the creation of interactive dashboards, allowing real-time monitoring of information security metrics. With real-time updates, enterprises can promptly respond to emerging threats by identifying trends and deviations in data (Maarof, Mahmud, 2016; Li et al., 2016). Power BI offers similar capabilities and integrates seamlessly with Microsoft's ecosystem, making it ideal for organizations utilizing its suite of products. Its AI-powered features facilitate advanced threat analysis, which is critical for strategic planning and ensuring information security (Manuri, 2018; Gomes Leite et al., 2018).

Qlik Sense stands out with its intuitive interface and associative data model, enabling users to freely explore data and uncover hidden threats. This functionality is particularly valuable for risk management and anomaly detection in information systems (Hambach et al., 2017). SAS Analytics, on the other hand, provides advanced tools for predictive and statistical analysis, enabling the forecasting of threats and identifying patterns related to security incidents. Its high-performance capabilities allow for processing large volumes of data, which is essential for organizations with extensive IT structures (Mora, 2017).

IBM Cognos Analytics supports organizations in data management and generating reports related to performance and information security. Its ad hoc reporting and interactive dashboards allow users to analyze compliance with regulations such as GDPR and ISO 27001 standards in real time, thereby supporting effective risk management (Pekarčíková et al., 2019). Similarly, with its cloud-based architecture, facilitates real-time data monitoring and collaboration among teams responsible for information security (Cavdur et al., 2019). Tools such as Google Data Studio and SAP BusinessObjects offer intuitive interfaces and integration capabilities with various data sources, making them attractive solutions for enterprises of all sizes (Dallasega et al., 2017).

The application of these analytical tools enables effective monitoring of security incidents, risk analysis, and optimization of information management processes. Additionally, they support compliance with legal regulations and industry standards, which is a key element of strategies to protect information resources in the digital era. The aforementioned software allows enterprises to create an environment of continuous improvement that fosters a data-driven culture of security management and supports the achievement of operational excellence (Gattullo et al., 2019).

Table 2.
Examples of Software and Applications Used in the Continuous Improvement Process for Information Security

Software Name	Description	Application
Tableau	A data visualization tool that enables the creation of interactive dashboards.	Real-time monitoring of security metrics, identifying trends and anomalies in data.
Power BI	Microsoft's business intelligence software that integrates seamlessly with its ecosystem.	Visualization of system logs, threat analysis using artificial intelligence, and generating compliance reports.
Qlik Sense	A self-service data analytics platform with an intuitive interface.	Identifying hidden threats, analyzing dependencies in information systems, and creating interactive reports.
SAS Analytics	Advanced software for predictive and statistical analysis.	Forecasting potential threats, identifying patterns in security incidents, and optimizing information security processes.
IBM Cognos Analytics	An analytics platform offering ad-hoc reporting and interactive dashboards.	Analyzing compliance with regulations (e.g., GDPR, ISO 27001), generating performance and security-related reports.
Domo	A cloud-based analytics tool enabling real-time data integration.	Real-time data monitoring, team collaboration in security management, and strategy analysis in real-time.

Cont. table 2.

Google Data Studio	A free data visualization tool with integration capabilities for other Google products.	Creating intuitive reports on security status and real-time monitoring of security-related data.
SAP BusinessObjects	A comprehensive suite of tools for reporting and data analysis.	Managing large data sets, integration with SAP systems, and supporting security-related analyses.
Looker	A platform for data exploration and visualization, focusing on real-time analytics.	Cloud data analysis, creating custom reports, and modeling and managing data in the context of security.
MicroStrategy	Enterprise-grade software for advanced analytics and data visualization.	Generating detailed reports, analyzing trends related to security, and mobile access to analytical data.

4. Advantages and Challenges of Using Data Security in Continuous Improvement for Industry 4.0

Data security plays a crucial role in the process of continuous improvement within the context of Industry 4.0, characterized by advanced automation, system integration, and intensive data utilization. Securing information supports organizations in improving decision-making quality by enabling reliance on accurate and reliable data. This approach eliminates the risk of errors caused by incomplete or uncertain information, leading to better process management and higher operational efficiency (Karlovits, 2017; Ghobakhloo, Fathi, 2020). Additionally, data security prevents operational disruptions resulting from cyberattacks, system failures, or the loss of critical information. In the highly interconnected systems of Industry 4.0, ensuring data integrity minimizes the risk of downtime and ensures business continuity (Dogan, 2018).

Another significant aspect is the ability to monitor data security in real time. Advanced analytical tools allow organizations to quickly detect potential threats and respond immediately, enhancing flexibility and enabling faster preventive actions (Greasley, 2019). Data security solutions also foster innovation by protecting information related to markets, customers, and technological processes. This protection enables organizations to safely explore new areas of development while minimizing the risks associated with the loss of valuable data (Arica, Powell, 2017; Bibby, Dehe, 2018). An important outcome of implementing these solutions is building customer trust. The use of advanced data protection technologies and compliance with legal regulations, such as GDPR, increases customer confidence and strengthens organizational reputation (Beifert et al., 2018).

At the same time, implementing data security systems poses several challenges. One of the primary issues is technological complexity and the integration of modern solutions with existing systems, which often involves high costs and time-consuming processes. Organizations also face a shortage of highly skilled cybersecurity professionals, limiting their capacity to manage this area effectively (Dombrowski et al., 2017). Internal threats, such as unintentional

employee errors or deliberate actions leading to data theft, are another significant concern. Furthermore, the rapid evolution of new cyber threats outpaces the capabilities of current security technologies, requiring organizations to continually update systems and procedures (Meesublak, Klinsukont, 2020). Lastly, the dynamically changing legal regulations surrounding data protection, such as GDPR and national laws, impose additional administrative and financial burdens that can be challenging for many businesses to address.

Despite these challenges, data security remains an indispensable element of continuous improvement strategies in Industry 4.0. Its integration with operational processes creates an environment conducive to innovation and long-term development, while simultaneously supporting the protection of critical informational assets. Moreover, it fosters a culture of continuous improvement and adaptation to the evolving technological landscape, ensuring sustainable growth and resilience in a competitive environment.

Table 3 lists the benefits of using continuous improvement in an Industry 4.0 environment for data security, along with descriptions of each benefit.

Table 3.
Benefits of Continuous Improvement in an Industry 4.0 Environment for Data Security

Benefit	Description
Enhanced Decision-Making	Continuous improvement enables organizations to base decisions on accurate and reliable data, reducing errors and improving strategic planning.
Operational Resilience	Securing data and identifying risks proactively ensures business continuity by minimizing the impact of cyberattacks or system failures.
Real-Time Threat Monitoring	Advanced tools provide real-time insights into potential threats, allowing immediate responses and improved risk management.
Innovation Support	Protecting critical information fosters innovation by enabling the safe exploration of new technological and market opportunities.
Increased Customer Trust	Adherence to data protection standards like GDPR builds trust and strengthens customer loyalty by safeguarding personal and business information.
Cost Reduction	Identifying inefficiencies and addressing vulnerabilities reduces the financial impact of data breaches and operational disruptions.
Regulatory Compliance	Continuous monitoring and improvement help meet evolving legal and regulatory requirements, minimizing penalties and reputational risks.
Improved Collaboration	Secure data sharing across departments facilitates better coordination and alignment in addressing data security challenges.
Adaptability to New Threats	Regular updates to systems and processes ensure organizations remain resilient to emerging cyber threats and technological advancements.
Promotes a Culture of Excellence	Continuous improvement fosters a proactive mindset focused on refining data security practices and achieving long-term operational excellence.

This table highlights the multifaceted advantages of adopting a continuous improvement approach to data security within Industry 4.0, emphasizing its importance in achieving sustainability and competitiveness. Table 4 outlines the various challenges associated with implementing data security in continuous improvement processes within the context of Industry 4.0. It highlights key issues such as technological complexity, integration difficulties, compliance with evolving regulations, and resource constraints. These challenges underscore the importance of addressing both technical and organizational aspects to ensure

effective and sustainable data security practices. By understanding these issues, organizations can develop strategies to mitigate risks and enhance their ability to safeguard critical information in an increasingly digital and interconnected environment.

Table 4.
Challenges of Using Data Security in Continuous Improvement within Industry 4.0 Conditions

Challenge	Description
Technological Complexity	Implementing advanced data security systems in interconnected Industry 4.0 environments is often complicated and resource-intensive.
Integration Difficulties	Ensuring seamless integration of new security measures with legacy systems and diverse platforms can be challenging.
High Implementation Costs	Acquiring, maintaining, and updating data security technologies involve significant financial investment, especially for smaller enterprises.
Evolving Cyber Threats	The rapid evolution of cyber threats often outpaces the development and implementation of effective countermeasures.
Shortage of Skilled Workforce	The lack of qualified professionals in cybersecurity hinders the deployment and management of robust data security measures.
Compliance with Regulations	Adhering to complex and ever-changing data protection regulations, such as GDPR, adds administrative and operational burdens.
Internal Threats	Employee errors or intentional misuse of data can undermine security efforts and lead to significant vulnerabilities.
Data Volume and Complexity	The massive and complex data generated in Industry 4.0 environments can overwhelm traditional security measures and analytics tools.
Resistance to Change	Organizational reluctance to adopt new data security practices can delay implementation and reduce overall effectiveness.
Cost of Continuous Updates	Maintaining up-to-date security systems and processes to counter emerging threats requires ongoing investment and resource allocation.

This table highlights the key challenges organizations face in integrating data security into continuous improvement strategies within Industry 4.0, emphasizing the need for proactive measures, skilled personnel, and strategic resource management to address these issues effectively.

5. Conclusion

The integration of robust data security measures into continuous improvement efforts within Industry 4.0 settings represents a transformative approach to enhancing operational resilience, strategic decision-making, and overall business sustainability. By ensuring the integrity, availability, and confidentiality of data, organizations can drive efficiency, foster innovation, and build trust among stakeholders. Data security facilitates the identification and mitigation of risks in real time, enabling businesses to adapt swiftly to emerging threats and maintain operational continuity in highly interconnected environments.

Moreover, secure data management supports predictive capabilities, allowing organizations to anticipate potential vulnerabilities and address them proactively. This not only minimizes downtime and protects critical assets but also promotes a culture of continuous improvement

where data-driven insights guide strategic refinements and operational excellence. By safeguarding sensitive information and complying with regulatory requirements, companies can enhance customer confidence and strengthen their competitive position in the market.

However, leveraging data security in continuous improvement is not without challenges. Issues such as technological complexity, integration difficulties, high implementation costs, and the rapidly evolving cyber threat landscape demand strategic planning and resource allocation. Overcoming these obstacles requires a skilled workforce, effective change management, and a commitment to continuous updates and innovation.

Despite these challenges, the benefits of integrating data security into continuous improvement processes far outweigh the difficulties. Organizations that prioritize data security as a core element of their Industry 4.0 strategies are better positioned to achieve long-term success. By fostering agility, protecting critical information assets, and ensuring compliance with evolving standards, businesses can maintain their resilience, drive innovation, and sustain growth in an increasingly digital and interconnected world.

References

1. Arica, E., Powell, D.J. (2017). *Status and future of manufacturing execution systems*, pp. 2000-2004. IEEE.
2. Bai, C., Dallasega, P., Orzes, G., Sarkis, J. (2020). Industry 4.0 technologies assessment: A sustainability perspective. *International Journal of Production Economics, 229,* 107776.
3. Beifert, A., Gerlitz, L., Prause, G., Beifert, A., Gerlitz, L., Prause, G. (2018). Industry 4.0 – For Sustainable Development of Lean Manufacturing Companies in the Shipbuilding Sector. *Springer International Publishing, 36,* 563-573.
4. Bibby, L., Dehe, B. (2018). Defining and assessing industry 4.0 maturity levels – case of the defence sector. *Production Planning & Control, 29*, 1030-1043.
5. Cavdur, F., Yagmahan, B., Oguzcan, E., Arslan, N., Sahan, N. (2019). Lean service system design: a simulation-based VSM case study. *BPMJ, 25*, 1802-1821.
6. Da Costa, M.B., Dos Santos, Leonardo Moraes Aguiar Lima, Schaefer, J.L., Baierle, I.C., Nara, E.O.B. (2019). Industry 4.0 technologies basic network identification. *Scientometrics, 121*, 977-994.
7. Dallasega, P., Rojas, R.A., Rauch, E., Matt, D.T. (2017). Simulation Based Validation of Supply Chain Effects through ICT enabled Real-time-capability in ETO Production Planning. *Procedia Manufacturing, 11*, 846-853.
8. Dogan (2018). Data perspective of lean six sigma in industry 4.0 era: A guide to improve quality. *Proc. Int. Conf. Ind. Eng. Oper. Manag.*, 943.
9. Dombrowski, U., Richter, T., Krenkel, P. (2017). Interdependencies of Industrie 4.0 & Lean Production Systems: A Use Cases Analysis. *Procedia Manufacturing, 11*, 1061-1068.

10. Frank, A.G., Dalenogare, L.S., Ayala, N.F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics, 210*, 15-26.
11. Gattullo, M., Scurati, G.W., Fiorentino, M., Uva, A.E., Ferrise, F., Bordegoni, M. (2019). Towards augmented reality manuals for industry 4.0: A methodology. *Robotics and Computer-Integrated Manufacturing, 56*, 276-286.
12. Ghobakhloo, M., Fathi, M. (2020). Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing. *Journal of Manufacturing Technology Management, 31*, 1-30.
13. Gomes Leite, D., Estombelo Montesco, R.A., Sakuraba, C.S. (2018). Increasing a gas distributor net profit through Lean Six Sigma. *Quality Engineering, 30*, 359-370.
14. Hambach, J., Kümmel, K., Metternich, J. (2017). Development of a Digital Continuous Improvement System for Production. *Procedia CIRP, 63,* 330-335.
15. Ito (2020). Digital Twin Technology for Continuous Improvement at Manufacturing Sites. *Digit. Solut. Better Futur. Soc., 69*, 66.
16. Iuga, M.V., Rosca, L.I. (2017). Comparison of problem solving tools in lean organizations. *MATEC Web Conf., 121*, 2004.
17. Karlovits (2017). Technologies for using big data in the paper and printing industry. *J. Print Media Technol. Res., 6*, 75.
18. Khan, M.A., Kumar, N., Alsamhi, S.H., Barb, G., Zywiołek, J., Ullah, I., Noor, F., Shah, J.A., Almuhaideb, A.M. (2024). Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review. *IEEE Trans. Netw. Serv. Manage., 1*.
19. Li, Z., Wang, K., He, Y. (2016). *Industry 4.0 - Potentials for Predictive Maintenance*. Atlantis Press.
20. Maarof, M.G., Mahmud, F. (2016). A Review of Contributing Factors and Challenges in Implementing Kaizen in Small and Medium Enterprises. *Procedia Economics and Finance, 35*, 522-531.
21. Manuri (2018). Augmented Reality in Industry 4.0. *Am. J. Comput. Sci. Inf. Technol., 6*, 17.
22. Mayr, A., Weigelt, M., Kühl, A., Grimm, S., Erll, A., Potzel, M., Franke, J. (2018). Lean 4.0 - A conceptual conjunction of lean management and Industry 4.0. *Procedia CIRP, 72*, 622-628.
23. Meesublak, K., Klinsukont, T. (2020). *A Cyber-Physical System Approach for Predictive Maintenance*. IEEE, 337-341.
24. Meister, M., Beßle, J., Cviko, A., Böing, T., Metternich, J. (2019). Manufacturing Analytics for problem-solving processes in production. *Procedia CIRP, 81*, 1-6.
25. Miqueo, A., Torralba, M., Yagüe-Fabra, J.A. (2020). Lean Manual Assembly 4.0: A Systematic Review. *Applied Sciences, 10*, 8555.
26. Mora (2017). Exploiting lean benefits through smart manufacturing: A comprehensive perspective. *IFIP Adv. Inf. Commun. Technol., 513*, 127.

27. Mrugalska, B., Wyrwicka, M.K. (2017). Towards Lean Production in Industry 4.0. *Procedia Engineering, 182*, 466-473.
28. Pekarčíková, M., Trebuňa, P., Kliment, M. (2019). Digitalization effects on the usability of lean tools. *AL, 6*, 9-13.
29. Rosin, F., Forget, P., Lamouri, S., Pellerin, R. (2020). Impacts of Industry 4.0 technologies on Lean principles. *International Journal of Production Research, 5*, 1644-1661.
30. Rossini, M., Costa, F., Tortorella, G.L., Portioli-Staudacher, A. (2019). The interrelation between Industry 4.0 and lean production: an empirical study on European manufacturers. *The International Journal of Advanced Manufacturing Technology, 102*, 3963-3976.
31. Shafiq, S.I., Velez, G., Toro, C., Sanin, C., Szczerbicki, E. (2016). Designing Intelligent Factory: Conceptual Framework and Empirical Validation. *Procedia Computer Science, 96*, 1801-1808.
32. Shahin, M., Chen, F.F., Bouzary, H., Krishnaiyer, K. (2020). Integration of Lean practices and Industry 4.0 technologies: smart manufacturing for next-generation enterprises. *Int. J. Adv. Manuf. Technol., 107*, 2927-2936.
33. Taylor, S.J.E., Anagnostou, A., Kiss, T., Taylor, S.J.E., Anagnostou, A., Kiss, T. (2019). *High Speed Simulation Analytics.* Springer International Publishing, 167-189.
34. Tortorella, G., Sawhney, R., Jurburg, D., Paula, I.C. de, Tlapa, D., Thurer, M. (2021). Towards the proposition of a Lean Automation framework. *JMTM, 32*, 593-620.
35. Tuominen, V. (2016). The measurement-aided welding cell—giving sight to the blind. *The International Journal of Advanced Manufacturing Technology, 86*, 371-386.
36. Valamede (2020). Lean 4.0: A new holistic approach for the integration of lean manufacturing tools and digital technologies. *Int. J. Math. Eng. Manag. Sci., 5*, 854.
37. Vinodh, S., Antony, J., Agrawal, R., Douglas, J.A. (2021). Integration of continuous improvement strategies with Industry 4.0: a systematic review and agenda for further research. *TQM, 33*, 441-472.
38. Wolniak, R., Dolata, M., Hadryjańska, B., Wysokińska-Senkus, A. (2024). *Employing business analytics in industry 4.0 settings for human resource analytics*. SPSUTOM, 629-640.
39. Żywiołek, J. (2024a). Building Trust in AI-Human Partnerships: Exploring Preferences and Influences in the Manufacturing Industry. *Management Systems in Production Engineering, 32*, 244-251.
40. Żywiołek, J. (2024b). Knowledge-Driven Sustainability: Leveraging Technology for Resource Management in Household Operations. *ECKM, 25*, 974-982.
41. Żywiołek, J. (2024c). Trust-Building in AI-Human Partnerships Within Industry 5.0. *System Safety: Human - Technical Facility - Environment, 6.*
42. Żywiołek, J., Trigo, A., Rosak-Szyrocka, J., Khan, M.A. (2022). Security and Privacy of Customer Data as an Element Creating the Image of the Company. *Management Systems in Production Engineering, 30*, 156-162.