


Collaborative Discussion 1

Initial Response



Initial Post
by Shashank Phatak - Saturday, 30 August 2025, 3:54 PM

Kovaitė *et al.*, (2019) define 'Industry 4.0' as the fourth industrial revolution, marked by the integration of advanced digital technologies into manufacturing and business processes. This shift involves cyber-physical systems, the Internet of Things (IoT), and big data analytics, creating smart factories that enhance automation, efficiency, and customisation. Industry 4.0 enables real-time data exchange and predictive capabilities, facilitating dynamic market responses and fostering innovation.

Key technologies in Industry 4.0 include IoT, which allows autonomous machine communication to optimise production, and cloud computing, which supports scalable data storage and remote decision-making.

The authors identify six risk categories associated with Industry 4.0 adoption: technical, competence, employee acceptance, customer and partner acceptance, data privacy and security, and financial risks. Notable examples include the 2017 WannaCry ransomware attack, which disrupted operations in more than 150 countries, including companies such as Nissan (BBC News, 2017), highlighting the risks to data privacy, and the 2019-2020 protests by Amazon workers against IoT-driven automation due to concerns about job displacement (Spencer, 2019).

Luo and Zahra (2023) support these findings, emphasising similar risks in data security and workforce adaptation for multinational enterprises while noting opportunities for digital innovation amidst the challenges. Overall, while Industry 4.0 offers significant efficiency gains, it requires effective risk management for sustainable implementation.

References


BBC News (2017) Ransomware cyber-attack: Who has been hardest hit? Available from <https://www.bbc.com/news/world-39919249> [Accessed on 25th August 2025]

Kovaitė, K. et al. (2019) Industry 4.0 as the Driving Force of SME Internationalisation: A Case of Lithuania, *Economics and Business*, 33(1), pp. 192–206. Available from <https://doi.org/10.2478/eb-2019-0014>.

Luo, Y. and Zahra, S.A. (2023) Industry 4.0 in international business research, *Journal of International Business Studies*, 54(3), pp. 403–417. Available from <https://doi.org/10.1057/s41267-022-00577-9>.

Spencer D., (2023) Amazon still seems hell bent on turning workers into robots – here's a better way forward. Available from <https://theconversation.com/amazon-still-seems-hell-bent-on-turning-workers-into-robots-heres-a-better-way-forward-201221> [Accessed on 27th August 2025]

Peer Response to Mohammad Ali Okleh Harahsheh



Peer Response
by Shashank Phatak - Tuesday, 14 October 2025, 8:44 PM

Your post provides a clear and concise overview of Industry 4.0, effectively highlighting its role in integrating advanced technologies, such as IoT and cloud computing, to enhance productivity and flexibility in SMEs (Kovaitė and Stankevičienė, 2019). The examples you provide of IoT-based systems and cloud platforms illustrate their transformative potential for global operations. The risk categories technological, operational, financial, and strategic, are articulated well, with the NotPetya attack and Nokia's strategic failure serving as compelling real-world cases that underscore the vulnerabilities associated with digitalisation (dos Santos Filho et al., 2024).

To mitigate the technological and operational risks exemplified by the NotPetya attack, organisations could implement robust cybersecurity frameworks, such as zero-trust architectures and regular penetration testing, to secure interconnected systems (Tao et al., 2018). Proactive measures, such as real-time threat monitoring and patch management, could have significantly reduced disruptions for companies like Maersk. In addressing strategic risks, as illustrated by Nokia's case, firms could adopt agile innovation strategies that include continuous market scanning and R&D investments to remain ahead of technological shifts (Hermann et al., 2016). Furthermore, fostering strategic partnerships with technology providers can enhance adaptability.

The TMR-14.0 framework you referenced (dos Santos Filho et al., 2024) underlines these measures by advocating for structured risk models to address issues related to interoperability and data breaches. Additionally, Kaur et al. (2025) present a governance model that emphasises resilience through proactive threat mitigation. If implemented early, these strategies can prevent operational downtime and strategic missteps, thereby ensuring the sustainable adoption of Industry 4.0.

References

- dos Santos Filho, V. H., de Resende, L. M. M., & Pontes, J. (2024) 'Development of a theoretical model for digital risks arising from the implementation of Industry 4.0 (TMR-14.0)', *Future Internet*, 16(6), p. 215. Available at: <https://www.mdpi.com/1999-5903/16/6/215> (Accessed: 30 August 2025).
- Hermann, M., Pentek, T., & Otto, B. (2016) 'Design principles for Industrie 4.0 scenarios: A literature review', Working Paper No. 01/2015. Technische Universität Dortmund.
- Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., & Ali, S. (2025) 'Smart grid cybersecurity: A model-driven approach to risk optimization and governance for resilience and threat mitigation', *ResearchGate*. Available at: <https://www.researchgate.net/profile/Shahid-Ali-19/publication/394426368> (Accessed: 30 August 2025).
- Kovaitė, K., & Stankevičienė, J. (2019) 'Industry 4.0 as the driving force of SME internationalisation: A case of Lithuania', *Entrepreneurial Business and Economics Review*, 7(3), pp. 51–63. Available at: <https://sciendo.com/pdf/10.2478/eb-2019-0014> (Accessed: 30 August 2025).
- Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018) 'Data-driven smart manufacturing', *Journal of Manufacturing Systems*, 48, pp. 157–169. <https://doi.org/10.1016/j.jmsy.2018.01.006>

Peer Response to Peter Osifo



Peer Response

by Shashank Phatak - Tuesday, 14 October 2025, 8:45 PM

Your post effectively encapsulates the essence of Industry 4.0, emphasising its core technologies, such as IoT and robotics, along with their applications in smart homes and intelligent factories (Kovaitė and Stankevičienė, 2019). The reference to Hecklau et al. (2016) strengthens your argument regarding the necessity for comprehensive human resource management to adequately address competency risks, which represent a significant barrier to successful digital transformation. Your identification of both technical and competency risks is particularly astute, as these are critical challenges organisations face when transitioning to Industry 4.0 (Kovaitė and Stankevičienė, 2019).


To mitigate the technical risks you've outlined, such as the need for new capabilities within intelligent factories, organisations could adopt robust system integration frameworks. For example, implementing standardised IoT protocols like MQTT or OPC UA can enhance interoperability and reduce system failures (Brettel et al., 2014). Additionally, conducting regular system audits and stress testing can further ensure reliability during the implementation process.

In terms of addressing competency risks, proactive measures such as tailored training programs and digital literacy workshops are essential. Hecklau et al. (2016) advocate for continuous learning systems to upskill employees, which could help prevent skill gaps in organisations adopting Industry 4.0 technologies. Moreover, cultivating a culture of adaptability through change management initiatives, as suggested by Hermann et al. (2016), could alleviate resistance and align workforce capabilities with technological demands. If these strategies are implemented early on, they could minimise disruptions and facilitate the adoption of intelligent systems in factories, ensuring smoother transitions to Industry 4.0.

References

- Brettel, M., Friedrichsen, N., Keller, M., & Rosenberg, M. (2014) 'How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 perspective', *International Journal of Mechanical, Industrial Science and Engineering*, 8(1), pp. 37–44.
- Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016) 'Holistic approach for human resource management in Industry 4.0', *Procedia CIRP*, 54, pp. 1–6.
- Hermann, M., Pentek, T., & Otto, B. (2016) 'Design principles for Industrie 4.0 scenarios: A literature review', *Working Paper No. 01/2015*. Technische Universität Dortmund.
- Kovaitė, K., & Stankevičienė, J. (2019) 'Risks of digitalisation of business models', *Contemporary Issues in Business, Management and Economics Engineering 2019*. Available at: <https://doi.org/10.3846/cibmee.2019.039> (Accessed: 30 August 2025).

Summary Post



Summary Post

by Shashank Phatak - Tuesday, 14 October 2025, 8:59 PM

Reflecting on the initial post and the peer responses provided to peers Peter Osifo and Mohammad Ali Okleh Harahsheh, we can recognise that Industry 4.0 represents a transformative shift driven by technologies such as IoT, cloud computing, and big data analytics. These advancements are facilitating the emergence of smart factories and the internationalisation of SMEs (Kovaitė and Stankevičienė, 2019). In the initial post, it has been outlined how these technologies enhance automation and efficiency while also identifying associated risks, including data privacy concerns (e.g., the WannaCry attack) and employee resistance (e.g., protests at Amazon). In the peer responses to Peter and Mohammad, there is a strong emphasis on proactive risk mitigation strategies to address the risks they highlighted, thereby enriching the discussion on the challenges and opportunities presented by Industry 4.0.

In response to Peter's post, which addressed technical and competency risks, it has been suggested to implement standardised IoT protocols (e.g., MQTT) and continuous learning systems to mitigate potential system failures and skill gaps (Brettel et al., 2014; Hecklau et al., 2016). For Mohammad's post, which focused on the NotPetya attack and Nokia's strategic shortcomings, it was suggested to employ cybersecurity frameworks such as zero-trust architectures and agile innovation strategies to minimise operational disruptions and prevent strategic missteps (Tao et al., 2018). These suggestions align with the views of Luo and Zahra (2023), who advocate for adaptive governance to balance innovation with risk. The course material further emphasised the necessity for robust risk management frameworks.

The engagement with peers has deepened the understanding of how risks can vary between different contexts, particularly between SMEs and larger firms. This experience has highlighted the importance of tailored training, strong cybersecurity measures, and cultural adaptability to ensure the sustainable adoption of Industry 4.0.

References

- Brettel, M., Friedrichsen, N., Keller, M., & Rosenberg, M. (2014) 'How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 perspective', *International Journal of Mechanical, Industrial Science and Engineering*, 8(1), pp. 37–44.
- Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016) 'Holistic approach for human resource management in Industry 4.0', *Procedia CIRP*, 54, pp. 1–6.
- Kovaitė, K., & Stankevičienė, J. (2019) 'Industry 4.0 as the driving force of SME internationalisation: A case of Lithuania', *Entrepreneurial Business and Economics Review*, 7(3), pp. 51–63. Available at: <https://sciendo.com/pdf/10.2478/eb-2019-0014> (Accessed: 30 August 2025).
- Luo, Y., & Zahra, S. A. (2023) 'Industry 4.0 in international business research', *Journal of International Business Studies*, 54(3), pp. 403–417. Available at: <https://doi.org/10.1057/s41267-022-00577-9> (Accessed: 30 August 2025).
- Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018) 'Data-driven smart manufacturing', *Journal of Manufacturing Systems*, 48, pp. 157–169. <https://doi.org/10.1016/j.jmsy.2018.01.006>