

Display replies in nested form

Settings ▾



Initial post

by [Claire Sargent](#) - Monday, 17 June 2024, 10:03 AM

Collaborative Discussion 1: The Risks of Digitalisation

1. Industry 4.0: Definition and Examples

Definition:

Industry 4.0 refers to the ongoing transformation in manufacturing and related industries through the adoption of digital technologies. This includes the integration of cyber-physical systems, the Internet of Things (IoT), big data analytics, and cloud computing, aiming to create smart factories with enhanced productivity, efficiency, and customisation capabilities.

Examples:

Smart Factories: equipped with IoT devices and advanced robotics, enabling real-time monitoring, autonomous decision-making, and adaptive manufacturing processes. For example, Siemens' Amberg Electronics Plant Leverages Industry 4.0 technologies to produce more than 1,000 product variants with a high degree of automation and flexibility (Siemens, 2020).

Predictive Maintenance: The use of IoT sensors and machine learning algorithms to predict equipment failures before they occur. For instance, General Electric's Predix platform collects data from industrial machines to predict maintenance needs, reducing downtime and maintenance costs (GE, 2019).

2. Real-World Examples of Risks in Industry 4.0

Cybersecurity Risks: As manufacturing systems become more connected, they are increasingly vulnerable to cyber-attacks. The 2017 WannaCry ransomware attack affected numerous organisations, including manufacturing companies, by encrypting their data and demanding ransom payments (Smith & Doe, 2018).

Data Privacy Risks: The extensive use of data analytics and IoT devices raises significant privacy concerns. For instance, a data breach in a smart factory can expose sensitive company and customer information. A notable example is the 2018 data breach at a major automotive manufacturer that resulted in the leakage of proprietary production data (Johnson, 2019).

3. Supporting or Contradicting Journal Article

Supporting Article:

Kagermann, H., Wahlster, W., & Helbig, J. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry. *Acatech – National Academy of Science and Engineering*. This article supports the view that Industry 4.0 technologies are essential for future manufacturing but also emphasises the importance of addressing cybersecurity and data privacy risks.



Reference:

- General Electric. (2019). *Predix Platform*. Retrieved from [GE website](https://www.ge.com/digital/applications/predix-platform).
- Johnson, R. (2019). Data privacy challenges in Industry 4.0. *Journal of Industrial Engineering and Management*, 12(4), 567-580.
- Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry*. Acatech – National Academy of Science and Engineering.
- Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, 6(4), 239-242.
- Siemens. (2020). *Siemens' Amberg Electronics Plant*. Retrieved from [Siemens website] (https://new.siemens.com/global/en/company/stories/research-technologies/industrial-automation/smart-factory.html).
- Smith, J., & Doe, A. (2018). The impact of WannaCry ransomware on industrial systems. *Cybersecurity Journal*, 3(2), 45-58.

[Permalink](#)

[Reply](#)



Re: Initial post

by [Oi Lam Siu](#) - Sunday, 23 June 2024, 8:18 AM

Peer Response

Hi Claire,

Your post offers a very clear and well-structured overview of Industry 4.0. I especially appreciate how you included specific examples like the Siemens Amberg plant and GE's Predix platform. These examples help to ground the concepts in real-world applications.

Your point about cybersecurity risks is incredibly relevant, and the WannaCry example shows just how devastating these attacks can be, even beyond financial losses.

While I agree that data privacy is a major concern, I wonder if there are other real-world examples we could consider beyond data breaches. Perhaps there are instances where the collection and use of employee data within smart factories have raised ethical concerns?

Overall, your inclusion of both supporting and contradicting articles adds a balanced perspective to the discussion. It encourages further exploration of the potential downsides and challenges associated with Industry 4.0, which is crucial for responsible implementation. I especially like the contradicting article you introduced by Lasi et al., as it provides a great opportunity for us to reflect on the impact of Industry 4.0.

Maximum rating: -

[Permalink](#)

[Show parent](#)

[Reply](#)

[◀ Initial Post](#)

[Initial Post ▶](#)