Summary Post: When Technology Fails - Industry 4.0 Risks

by Natali Nikolic - Monday, 11 November 2024, 10:02 PM

https://www.my-course.co.uk/mod/forum/discuss.php?d=266564#p501111

Industry 4.0 has significantly increased productivity through interconnected digital systems but has also exposed industries to substantial risks, as seen in the July 2024 Microsoft outage, which disrupted multiple sectors and resulted in billions of dollars in losses for U.S. companies. This event underscores Industry 4.0's vulnerability to system failures, highlighting the critical need for resilience to manage such risks effectively (Robins-Early, 2024; Sabbagh, 2024; Schwab, 2016).

In my initial post, I discussed Chaos Engineering as a proactive approach to reduce future outages by deliberately testing system weaknesses, thereby strengthening resilience (Rosenthal et al., 2020).

Similarly, my peer Pëllumb Dalipi proposed simulating failures to uncover vulnerabilities, though he also noted the high complexity and costs involved, particularly for rare but high-impact events. He emphasized that achieving resilience demands both thorough testing and a commitment from organizations to invest in these methods (Ale et al., 2021; Hollnagel, 2018).

Another perspective by Rodrigo Pereira Cruz highlights trustworthiness when designing resilient security systems (Henschke & Ford, 2017); without user trust, even the most advanced and cost-effective systems lose value, emphasizing the need to prioritize this aspect in mitigating Industry 4.0 risks.

In conclusion, while Industry 4.0 enhances productivity, its dependence on digital systems poses significant risks, as described in this instance. Strategies like Chaos Engineering, along with a focus on resilience and trust, emphasize the importance of proactive strategies and dedicated efforts to maintain system stability.

References

- Ale, B.J.M., Hartford, D.N.D., & Slater, D.H., 2021. Prevention, precaution and resilience: Are they worth the cost? Safety Science.
- Henschke, A. & Ford, S.B. (2017) Cybersecurity, trustworthiness and resilient systems: guiding values for policy. Journal of cyber policy 2(1): 82-95. DOI: https://doi.org/10.1080/23738871.2016.1243721.
- Hollnagel, E., 2018. Safety-II in Practice: Developing the Resilience Potentials.
- Robins-Early, N. (2024) 'CrowdStrike global outage to cost US Fortune 500 companies $5.4bn', The Guardian. Available at: https://plus.lexis.com/api/permalink/934f29a5-0366-48c4-abe2-28fdebf5f3a9/?context=1001073 (Accessed: 27 October 2024).
- Rosenthal, C. and Jones, N. (2020) Chaos engineering: system resiliency in practice. 1st edn. Sebastopol, CA: O'Reilly Media.
- Sabbagh, D. (2024) 'Is the UK resilient enough to withstand a major cyber-attack? Microsoft's IT outage reveals the fragility of our software systems and the risks of a more serious technology collapse', The Guardian. Available at: https://plus.lexis.com/api/permalink/2746aabc-07cf-4a5e-9839-862c97a68b7e/?context=1001073 (Accessed: 27 October 2024).
- Schwab, K. (2016) 'The Fourth Industrial Revolution: what it means, how to respond'. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (Accessed: 25 October 2024).