Summery post

Summery post

by Saleh Almarzooqi - Monday, 18 August 2025, 6:54 PM

Industry 5.0 is shifting towards a more robust and human-involving approach to manufacturing than Industry 4.0, dependent on automation and networked integrations (Maggioli and Cunha, 2023). A vital illustration can be proposed through introducing potential vulnerabilities into the cybersecurity of manufacturing that may be created by the rising addiction to the IoT, automation, and cyber-physical systems, as of the WannaCry ransomware attack on Nissan in the context of 2017. Through this attack, there was a massive disruption to the production, logistics, and customer trust, and Nissan incurred both financial and image losses.

Reflecting on the prompt and the responses of the peers, the transition of Industry 4.0 to Industry 5.0 should be associated with the orientation toward resiliency and human participation in the control of the automated processes. Although automation and interconnected systems are very important in boosting efficiency, the introduction of Industry 5.0 will focus on the necessity to ensure a balance of such technologies and human control (Saluja and Mongia, 2025). This solution has the potential to contribute to the mitigation of dangers as well as the stability and flexibility of infrastructures, thus decreasing the risk of damage when a cybersecurity breach occurs.

The reputation burden that the Nissan attack underlines further affirms the necessity of organisations to make investments in strong cybersecurity systems (Aggarwal, 2023). Manufacturers can make their systems less vulnerable through the introduction of human oversight and constant enhancements in aspects of security (Alhakimi, 2024). The transition is important because we now enter a new age where technological systems are becoming more dominant in the production process and in doing business. Finally, the struggles Nissan has been experiencing demonstrate that it is critical to adopt the principles of Industry 5.0 so that technologies are used to promote not only operational objectives but also the well-being and sustainable development of people.

References:

Aggarwal, M., 2023, July. Ransomware attack: an evolving targeted threat. In *2023 14th International Conference on Computing, Communication, and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

Alhakimi, A.M., 2024. The Power of Technology in Industrial Revolution 5.0. In *Utilizing Renewable Energy, Technology, and Education for Industry 5.0* (pp. 400-443). IGI Global.

Maggioli, S. and Cunha, L., 2023. A Systematic Review Discussing the Sustainability of Men and Women's Work in Industry 4.0: Are Technologies Gender-Neutral?. *Sustainability*, *15*(7), p.5615.

Saluja, A. and Mongia, A., 2025. Human-Machine Collaboration: Augmenting Human Abilities With Robotic Assistance in the Workplace. In *Technological Enhancements for Improving Employee Performance, Safety, and Well-Being* (pp. 145-170). IGI Global.

Maximum rating: -

You are logged in as Saleh Almarzooqi (Log out)

Policies

Powered by Moodle

Site Accessibility Statement
Privacy Policy