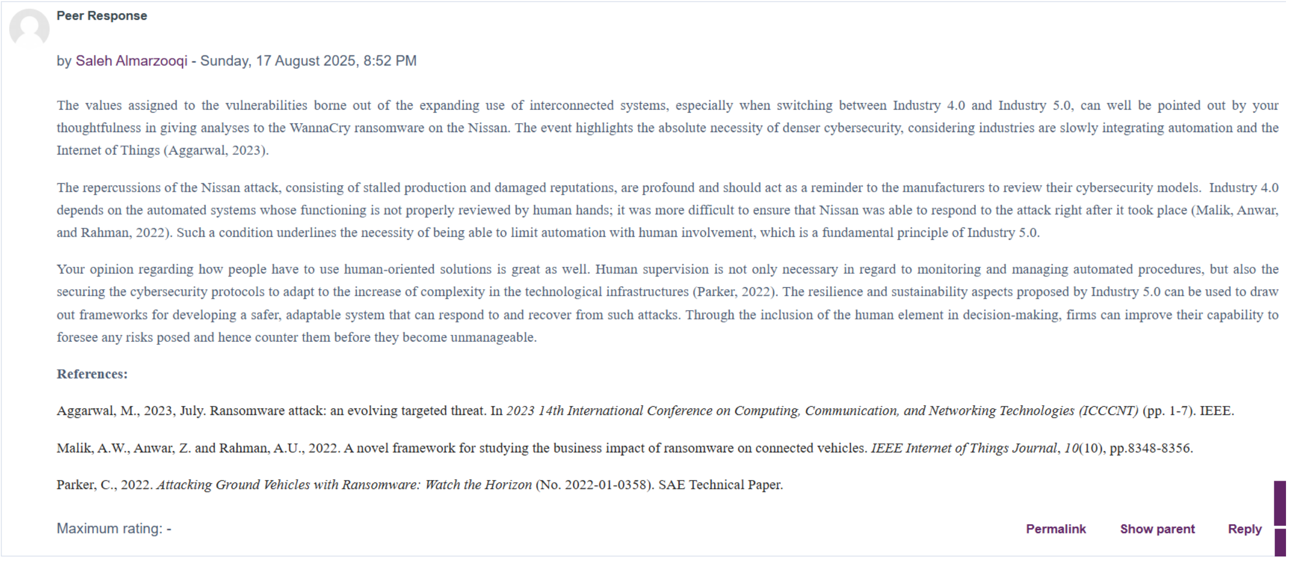


Peer Response

by Saleh Almarzooqi - Sunday, 17 August 2025, 8:52 PM

The values assigned to the vulnerabilities borne out of the expanding use of interconnected systems, especially when switching between Industry 4.0 and Industry 5.0, can well be pointed out by your thoughtfulness in giving analyses to the WannaCry ransomware on the Nissan. The event highlights the absolute necessity of denser cybersecurity, considering industries are slowly integrating automation and the Internet of Things (Aggarwal, 2023).

The repercussions of the Nissan attack, consisting of stalled production and damaged reputations, are profound and should act as a reminder to the manufacturers to review their cybersecurity models. Industry 4.0 depends on the automated systems whose functioning is not properly reviewed by human hands; it was more difficult to ensure that Nissan was able to respond to the attack right after it took place (Malik, Anwar, and Rahman, 2022). Such a condition underlines the necessity of being able to limit automation with human involvement, which is a fundamental principle of Industry 5.0.

Your opinion regarding how people have to use human-oriented solutions is great as well. Human supervision is not only necessary in regard to monitoring and managing automated procedures, but also the securing the cybersecurity protocols to adapt to the increase of complexity in the technological infrastructures (Parker, 2022). The resilience and sustainability aspects proposed by Industry 5.0 can be used to draw out frameworks for developing a safer, adaptable system that can respond to and recover from such attacks. Through the inclusion of the human element in decision-making, firms can improve their capability to foresee any risks posed and hence counter them before they become unmanageable.

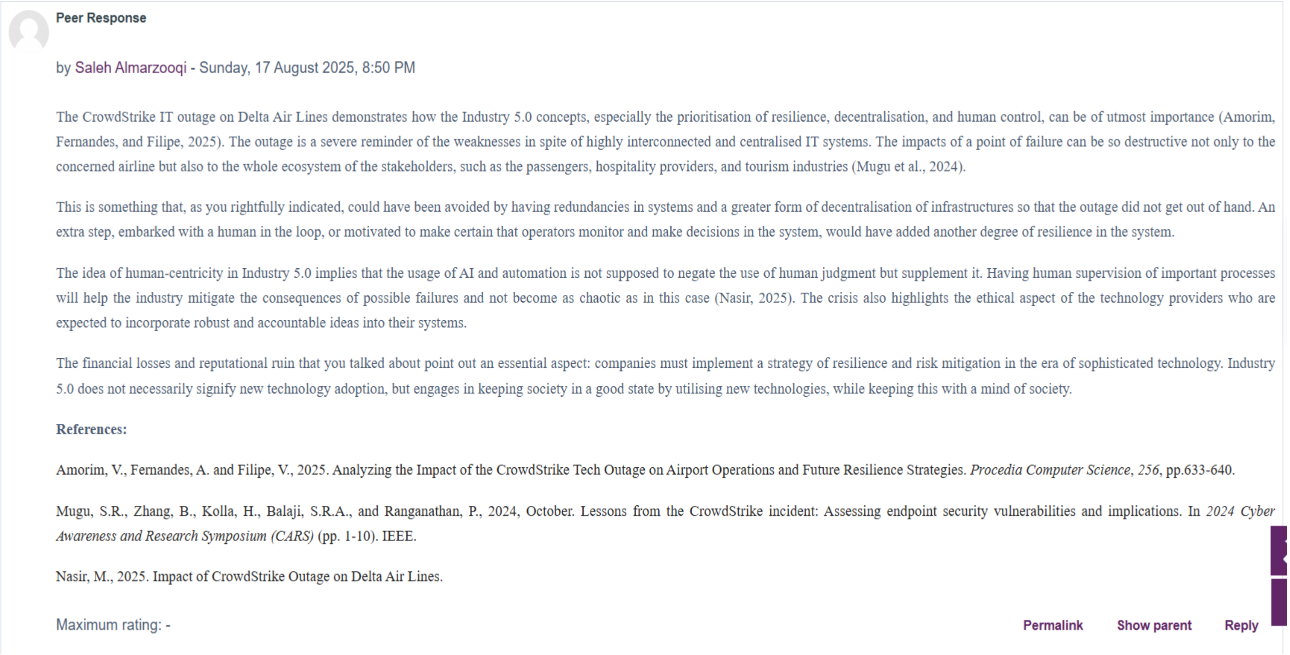
References:

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.

Malik, A.W., Anwar, Z. and Rahman, A.U., 2022. A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet of Things Journal*, *10*(10), pp.8348-8356.

Parker, C., 2022. *Attacking Ground Vehicles with Ransomware: Watch the Horizon* (No. 2022-01-0358). SAE Technical Paper.

Maximum rating: -



Peer Response

by Saleh Almarzooqi - Sunday, 17 August 2025, 8:50 PM

The CrowdStrike IT outage on Delta Air Lines demonstrates how the Industry 5.0 concepts, especially the prioritisation of resilience, decentralisation, and human control, can be of utmost importance (Amorim, Fernandes, and Filipe, 2025). The outage is a severe reminder of the weaknesses in spite of highly interconnected and centralised IT systems. The impacts of a point of failure can be so destructive not only to the concerned airline but also to the whole ecosystem of the stakeholders, such as the passengers, hospitality providers, and tourism industries (Mugu et al., 2024).

This is something that, as you rightfully indicated, could have been avoided by having redundancies in systems and a greater form of decentralisation of infrastructures so that the outage did not get out of hand. An extra step, embarked with a human in the loop, or motivated to make certain that operators monitor and make decisions in the system, would have added another degree of resilience in the system.

The idea of human-centricity in Industry 5.0 implies that the usage of AI and automation is not supposed to negate the use of human judgment but supplement it. Having human supervision of important processes will help the industry mitigate the consequences of possible failures and not become as chaotic as in this case (Nasir, 2025). The crisis also highlights the ethical aspect of the technology providers who are expected to incorporate robust and accountable ideas into their systems.

The financial losses and reputational ruin that you talked about point out an essential aspect: companies must implement a strategy of resilience and risk mitigation in the era of sophisticated technology. Industry 5.0 does not necessarily signify new technology adoption, but engages in keeping society in a good state by utilising new technologies, while keeping this with a mind of society.

References:

Amorim, V., Fernandes, A. and Filipe, V., 2025. Analyzing the Impact of the CrowdStrike Tech Outage on Airport Operations and Future Resilience Strategies. *Procedia Computer Science*, *256*, pp.633-640.

Mugu, S.R., Zhang, B., Kolla, H., Balaji, S.R.A., and Ranganathan, P., 2024, October. Lessons from the CrowdStrike incident: Assessing endpoint security vulnerabilities and implications. In *2024 Cyber Awareness and Research Symposium (CARS)* (pp. 1-10). IEEE.

Nasir, M., 2025. Impact of CrowdStrike Outage on Delta Air Lines.

Maximum rating: -