University of Essex
MSc Artificial Intelligence
Module: ML_PCOM7E July 2025 B
Unit 3: Collaborative Discussion – The 4th Industrial Revolution

Initial Discussion

At my company, I develop a variety of internal software systems for tracking work orders, vendor payments, and media asset files, including integrations between software platforms built by other company work groups and by outside vendors.

The resilience and human centricity aspects of Industry 5.0 are consistently relevant to my work, especially where data input is concerned. Resilience in this context, in particular, refers to the ability of a software system to adapt to changing usage patterns and to respond appropriately to unexpected behavior by human users (Alves, Lima and Gaspar, 2023).

For example, a form field may appear to a non-technical end user to allow any alphanumeric character or special character available on a standard keyboard. From the end user's perspective, that's an entirely reasonable assumption to make. What the end user doesn't typically know is that depending on the type of data being processed, and the disparate software platforms that data may need to pass through, what appears to be a valid input instead can cause system integration breakdowns.

A good example from recent experience involved an end user of a billing software platform entering greater than (">") and less than ("<") symbols into a text field in a form. Those special characters, however, were not recognized by the secondary software that ingested the form into an archiving system, which – in turn – acted as one of the data sources for several other asset management platforms. What appeared to the end user as an unremarkable bit of data entry was, instead, the cause of a ripple effect of derivative system errors.

In this example, there was no loss and no damage done – the error was caught and remediated right away – but it highlights the fragility of interconnected data processing systems that the concept of resilience in Industry 5.0 is intended to ameliorate.

Reference

Alves, J., Lima, T.M. and Gaspar, P.D. (2023). Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes*, 11(1), p.193. doi:https://doi.org/10.3390/pr11010193.

Peer Response No. 1

I think the discussion raises an interesting point: that entry points for ransomware attacks frequently rely on email or other human-information system points of interaction (Nagar, 2024).

If the goal of Industry 5.0 is to better align human factors with how information systems are built and operated (Alves, Lima and Gaspar, 2023), I think it would be reasonable to say that ransomware mitigation in this context should rely on not only employee training (addressing human factors directly via business processes), but also a kind of system-level “training” of the platforms themselves, i.e., building the systems to anticipate how people will use them ahead of time.

For example, phishing and other malicious email-based attacks often rely on readily identifiable indicators that a call to user action in a message is not legitimate. A phishing email may have an unusual return address pointing to a domain name that has no obvious connection to the employee’s company domain name.

Put briefly, an Industry 5.0 software platform might proactively look for – and attempt to remediate – such signs of a malicious actor in the course of its regular operation, additional to training end users to follow preventative measures out of their own volition. Both system-level and business-level processes then align to better respond to how human users act in practice in real world scenarios.

References

Alves, J., Lima, T.M. and Gaspar, P.D. (2023). Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes*, 11(1), p.193. doi:https://doi.org/10.3390/pr11010193.

Nagar, G., 2024. The evolution of ransomware: tactics, techniques, and mitigation strategies. *International Journal of Scientific Research and Management (IJSRM)*, *12*(06), pp.1282-1298.

Peer Response No. 2

I think that this discussion is a good illustration of the “resilience” factor of Industry 5.0 systems, or the ability of Industry 5.0 systems to respond to unforeseen events without (or with minimal) loss of functionality, and to restore impaired functioning without (or with minimal) human intervention (Alves, Lima and Gaspar, 2023).
As noted in the original post, resilience is a critical factor in infrastructure such as energy management utilities. A power outage not only has the potential to cause temporary economic losses from cessation of labor, insurance claims, and similar derivative consequences, it can – in severe cases – also lead to damaging the capacity of the system itself to function at needed levels in the future and/or cause otherwise avoidable injury or loss of human life (Introna, Santolamazza and Vittorio, 2024).

In that sense, an Industry 5.0 system should be built with resilience as a foreground principle. Such a system would not only be built to do what it was intended to do as well as it possibly can per the Industry 4.0 paradigm (Alves, Lima and Gaspar, 2023), but also be built with multiple layers of automated defenses against events that could cause impaired functionality, along with multiple avenues for automated damage mitigation and self-repair in the event of deleterious incidents (Introna, Santolamazza and Vittorio, 2024).

References

Alves, J., Lima, T.M. and Gaspar, P.D. (2023). Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes*, 11(1), p.193. doi:https://doi.org/10.3390/pr11010193.

Introna, V., Santolamazza, A. and Vittorio Cesarotti (2024). Integrating Industry 4.0 and 5.0 Innovations for Enhanced Energy Management Systems. *Energies*, 17(5), pp.1222–1222. doi:https://doi.org/10.3390/en17051222.

Discussion Summary

The discussion at hand revolves around the concepts of resilience and human centricity in Industry 5.0 as applied to data input in software systems. Specifically, “resilience” in this context addresses the capacity of a software system to recognize patterns of user interaction and respond appropriately, meaning, the system is capable of adapting to unexpected data inputs that otherwise could lead to runtime errors, unprovisioned downtime, and/or lapses in data security (Alves, Lima and Gaspar, 2023).

I described an example taken from my workplace in which an end user of a billing software platform, acting in the normal course of business, entered greater than (“>”) and less than (“<”) symbols into a text field in a form. These special characters, however, were not recognized by a derivative system that needed to parse the input data from one format to another, which, in turn, caused unexpected errors and loss of functionality in a downstream dependent software platform.

Peer feedback focused on the human centricity aspect of this scenario, referring to the human factors element of non-technical users interacting with a software system. A proposal for ameliorating such incidents was made to the effect that a fully resilient and human centric system would have mechanisms in place for identifying common user behaviors that could cause performance errors, and actively prevent the user from engaging in them while additionally educating them, within the software itself, as to how to avoid similar errors in the future.

An additional and insightful comment was made that the implementation of resilient systems does not occur in a vacuum, and software-based measures cannot be the first or last or only measures taken: the organizational culture in which the software operates and users interact with it also needs to deliberately cultivate a mindset of fostering adherence to best practices, whether business process or software-based, that minimize deleterious software usage patterns as a routine practice (Pina et al, 2024).

References

Alves, J., Lima, T.M. and Gaspar, P.D. (2023). Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes*, 11(1), p.193. doi:https://doi.org/10.3390/pr11010193.

Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., Abbasi, M. and Martins, P. (2024). Data Privacy and Ethical Considerations in Database Management. *Journal of Cybersecurity and Privacy*, [online] 4(3), pp.494–517. doi:https://doi.org/10.3390/jcp4030024.