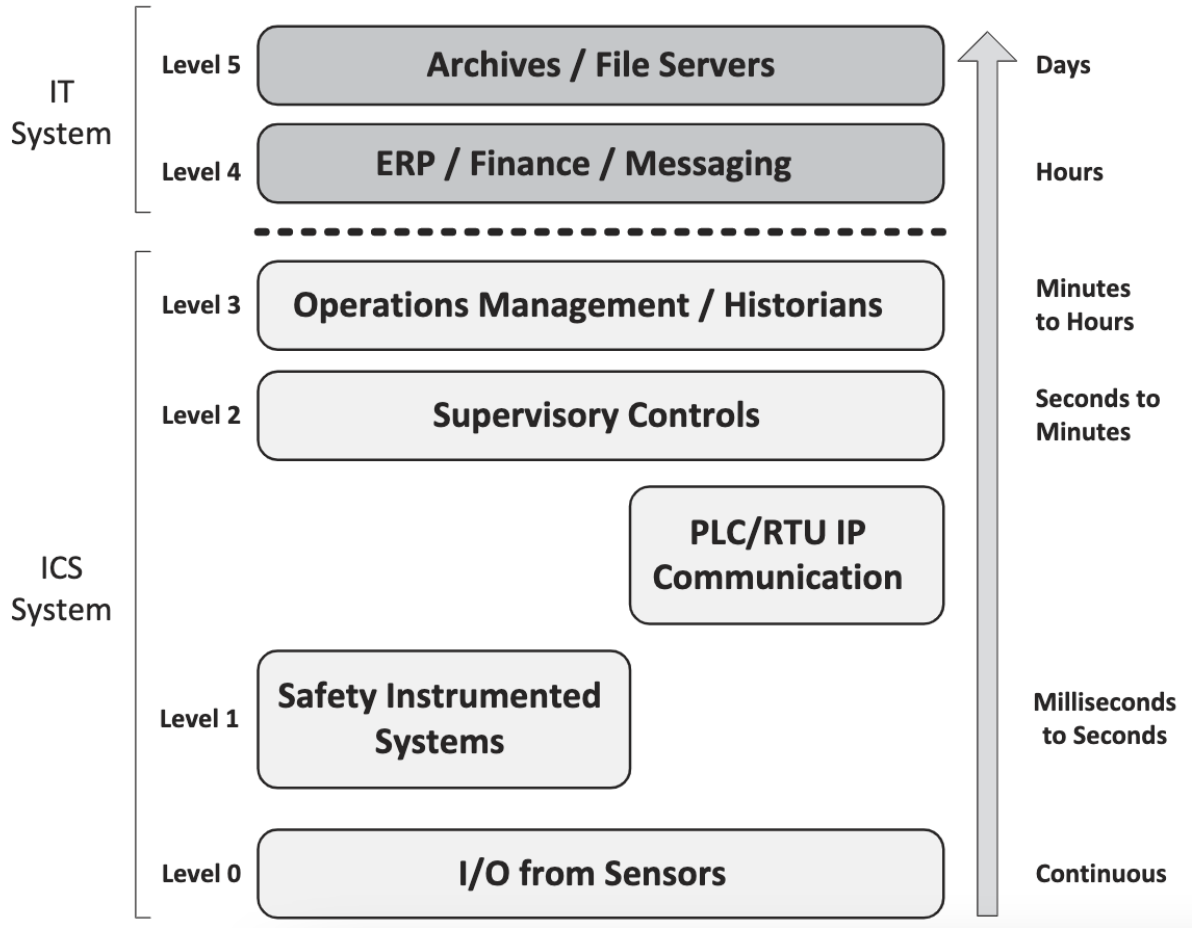
Thank you, Nisa, for your insights on Industry 4.0 and good examples of cyber attacks having a business model driven by the new technology. You highlight one of the significant risks of using this model by critical infrastructure such as the power plant in Saudi Arabia. It is one of the most considerable risks that can cause harm not only to businesses but also to the public.

As we can see, industry 4.0 is already a part of the critical infrastructure sector using technologies like big data and cloud computing (Wisniewski M. et al.,2022, p.82718). Modern systems comprise an array of both IT and industrial components interacting together to achieve a business goal (Habibi Rad et al., 2021, p.36). The figure below is also from the same paper, depicting the combination of industrial and IT components.



Industry 4.0 has opened various opportunities to automate and ease business processes. At the same time has presented us with multiple challenges where these technologies can be disrupted and cause significant loss. Therefore these Systems with critical infrastructures must be equipped with a security mechanism to prevent, detect, and recover from attacks (Habibi Rad, M, 2021, p.37). In addition, an analysis of existing threats and risks must be

conducted to make the system more rigid and have proper measures for the accepted risks (Flatt H, et al. 2016, p.3).

References

Wisniewski, M., Gladysz, B., Ejsmont, K., Wodecki, A. and Van Erp, T., 2022. Industry 4.0 solutions impacts on critical infrastructure safety and protection–a systematic literature review. IEEE Access.

Habibi Rad, M., Mojtahedi, M. and Ostwald, M.J., 2021. Industry 4.0, disaster risk management and infrastructure resilience: a systematic review and bibliometric analysis. Buildings, 11(9), p.411.

Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H. and Adamczyk, H., 2016, September. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-4). IEEE.