Industry 4.0 refers to the fourth industrial revolution, which combines machines, people, and physical assets into an integrated digital ecosystem that creates, analyses, and transmits data without human interaction, and occasionally takes action based on that data. It places a strong emphasis on connection, automation, machine learning, and real-time data. The Industrial Internet of Things (IIoT) and smart manufacturing are components of Industry 4.0. It integrates physical production and operations with intelligent digital technology, machine learning, and big data to build more linked systems for manufacturing and supply chain management-focused businesses.

Industry 4.0 is anticipated to change the industrial world, much as steam power did in the 1800s. The number of networked devices in use today is a chance to gather data and enable enhanced management and technological decision-making, which will significantly enhance output. Industry 4.0 facilitates the actionability of data. If used correctly, the availability of information across a system or systems may become a potent weapon.

Four Key Areas of Industry 4.0

* Cyber-Physical Systems (CPS) and Cobots
* Internet of Things (IoT) and Big Data
* Cloud Manufacturing (CMfg)
* Automation

Communications and cybersecurity cannot be seen as separate processes with Industry 4.0. To fully benefit from the possibilities that Industry 4.0 presents, firms of all sizes will need to comprehend its capabilities and possible dangers.

The risks that industry 4.0 would face would be those directly of the IT infrastructure and more. Notable attacks would be attacks on Web & Application, Network & Infrastructure, and direct threat to internet connected devices (IIoT)

**References**

Industry 4.0 and cybersecurity Managing risk in an age of connected production A Deloitte series on digital manufacturing. (n.d.). [online] Available at: https://www2.deloitte.com/content/dam/insights/us/articles/3749\_Industry4-0\_cybersecurity/DUP\_Industry4-0\_cybersecurity.pdf [Accessed 15 Sep. 2022].

Nurse, J.R.C., Creese, S. and De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. IT Professional, [online] 19(5), pp.20–26. doi:10.1109/mitp.2017.3680959.

Toth, P. (2022). Cybersecurity and Industry 4.0 – What You Need to Know. NIST. [online] Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-and-industry-40-what-you-need-know [Accessed 15 Sep. 2022].