Cyber Manufacturing

Matthew N. O. Sadiku[1], Philip O. Adebo[1],
Sarhan M. Musa[1]
[1]Roy G. Perry College of Engineering
Prairie View A&M University
Prairie View, TX 77446

Abayomi Ajayi-Majebi[2]
[2]Department of Manufacturing Engineering
Central State University
P.O. Box 1004
Wilberforce, OH 45384-1004

***Abstract*:- Cyber manufacturing is a kind of transformative system that translates data from interconnected system into predictive. It is a modern manufacturing approach that utilizes cyber-physical systems, which are smart systems that include co-engineered interacting networks of physical and computational components. This paper provides an introduction on cyber manufacturing.**

Key Words: Cyber manufacturing, manufacturing systems, cyber-physical systems, big data

INTRODUCTION

Manufacturing is the process of creating a product out of raw materials. The manufacturing industry includes many sectors such chemical industry, automotive industry, metal machinery industry, and electronics industry. Manufacturing has been noted as one of the largest industries globally [1].

Manufacturing is a national priority in many nations, both developed and developing. They are investing heavily in strategic, manufacturing-technology areas. In the past, the manufacturing industry has been in a continuous struggle to produce high-quality goods at the reasonable price that consumers can afford. The industrial era has allowed machines to resolve the quantity issue of manufacturing. Today's manufacturing operations integrate resources in a more complex manner, which requires extensive collaboration.

Cyber manufacturing may be regarded as the convergence of cyber-physical systems (CPSs), systems engineering, and manufacturing innovation. CPSs are enabling technologies which bring the virtual and physical worlds together to create a truly networked world in which intelligent objects communicate and interact without human intervention. They are essentially the upgraded version of embedded systems. They are the heart of industry 4.0. They are expected to bring about radical changes and revolution in the interaction between the physical and virtual worlds [2]. Cyber manufacturing system (CMS) is a vision for future advanced manufacturing systems integrated with technologies. It offers a blueprint for future manufacturing systems in which physical components are fully integrated with computational processes in a connected environment. Figure 1 typically shows cyber manufacturing system [3].

ENABLING TECHNOLOGIES

Several technologies are needed in developing cyber-manufacturing solutions. The enabling technologies include cyber-physical systems (CPSs), Internet of things (IoT), cloud computing, digital twin, sensors network, and machine learning.

- *Cyber-Physical Systems* (CPSs) are essentially integrations of computation, networking, and physical processes and they are increasingly finding applications in manufacturing. CPS usually refers to systems of collaborating computational elements that control physical entities. In CPS, computation and networking technologies interact with physical systems. CPSs are collaborating computational entities which are in intensive connection with the surrounding physical, providing and using data-accessing and data-processing services available on the Internet. They can be found in many applications including smart healthcare wearable devices, smart grid, smart water, smart manufacturing, smart factory, gas and oil pipelines monitoring and control, unmanned aerial, and autonomous underwater vehicles, and hybrid electrical vehicles. Figure 2 illustrates the **g**eneral representation of CPS [4].

- *Internet of Things* (IoT): Although there are similarities between CPS and IoT, they are not the same. The Internet of things (IoT) is a network of physical objects (sensors, machines, cars, buildings, etc.) that allows interaction and cooperation of these objects to reach common objective. Wireless sensor networks (WSNs) are a key enabling technology for IoT in manufacturing. While the IoT paradigm does not include the idea of information analytics, CPS is based on connectivity and run complex analytics. However, it is possible to view the IoT as the infrastructure that makes CPS possible. By increasing the amount of automation at multiple levels within a factory and across the enterprise, cyber-physical manufacturing systems enable higher productivity, higher quality, and lower costs. The real value of the IoT for manufacturers will be in the analytics arising from CPSs. Characteristically, IoT will make everything in our lives "smart." IoT has the potential to accurately track people, equipment, or even service animals and analyze the data captured [5].

- *Big Data Analytics:* The volume of data has exploded to unimaginable levels in the past decade. Big data comes from different sources such as sensors, devices, computer networks, machines, IoT, GPS, RFID, ecommerce transactions, web, weather data, medical data, insurance records, and social media. As we capture terabytes of data, our major challenge is making sense of this gigantic amount of data. This is where big data analytics fits into the picture. Big data analytics deals with examining massive amounts of data to uncover hidden patterns, market trends, customer preferences, and other useful information that can help in making informed decisions. The massive amount of raw data available from the manufacturing process creates opportunities to add intelligence to the process. Cyber manufacturing intertwines industrial big data and smart analytics to discover and comprehend invisible issues for decision making. Big data analytics is a technology that aims to support manufacturers to extract knowledge from data, which can be used for future prediction, increasing profits, and enhancing customer service [6, 7].

CHALLENGES

The applications of CPS in many domains such as manufacturing will have disruptive effects on technology, business, law, and ethics. The increased use of CPS brings some threats that could have significant consequences for users. CPS are prone to information leakage from the physical domain. They are prone to a wider range of attacks and design flaws [8].

Cyber-physical attacks are becoming common across a wide range of industries including manufacturing. Manufacturing is a significant target for cyber-criminals and manufacturers must take appropriate actions to protect themselves in the face of cyber-related risks. Cyber security is one of the major hurdles in implementing cyber manufacturing since CMS opens a door for cyber–physical attacks on manufacturing systems. The attacks may cause physical damages to physical components (such as machines, equipment, parts, products, etc.) through unintended over-wearing, breakage, scrap parts. Cyber-physical attacks are new and unique risks to CMSs. The four most dangerous cyber risks are identity theft, compromised websites, spam, and employees [9].

Although there is no mandated regulatory standards for governing cyber-security in manufacturing, the cybersecurity communities have developed a variety of standards, which address weaknesses and vulnerabilities. Different standards contribute in different ways to realize cyber manufacturing. Developing standards tends to motivate the adoption of new technologies and accelerates the adoption of new manufactured products and manufacturing methods. Standards allow a more dynamic and competitive marketplace. They are a critical tool for leveling the playing field for small businesses by reducing the cost barriers. They enable low cost applications which are suitable for small manufacturers [10].

These challenges are critical to cyber manufacturers' abilities to capture the value associated with this new frontier of technology while appropriately addressing the dynamic cyber risks. Many technologies, such as big data analytics, communication protocols, and cyber-security, still need a lot of research and development before cyber manufacturing can reach their full potential [11].

CONCLUSION

CPS has made great strides into manufacturing systems. Cyber manufacturing is a transformative concept that involves the translation of data from interconnected systems into predictive and prescriptive operations. As IoT and CPS technologies advance, cyber manufacturing realization will be facilitated through standardization and more reliable cyber security.

The most important part of any manufacturing operation is its people. To help in the attraction of cyber talent, manufacturers should work to become allies with higher educational institutions and build the talent pool they need. While attracting and retaining talented cyber professionals, manufacturers should provide training for the rest of the company's employees. More information about cyber manufacturing can be found in the books in [10,12] and related journal: *Manufacturing Letters.*

REFERENCES

[1] M. N. O. Sadiku, T. J. Ashaolu, A. Ajayi-Majebi, and S. M. Musa, "Emerging technologies in manufacturing," *International Journal of Scientific Advances*, vol. 1, no.2, Sept.-Oct., 2020.

[2] A. R. Al-Ali, R. Gupta, and A. A. Nabulsi, "Cyber physical systems role in manufacturing technologies," *AIP Conference Proceedings,* April 2018, https://aip.scitation.org/doi/pdf/10.1063/1.5034337

[3] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," *Manufacturing Letters,* vol. 8, 2016, pp. 11–15.

[4] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, "Cyber-physical systems: A brief survey," *International Journal of Trend in Research and Development,* vol. 7, no. 3, 2020.

[5] M. N. O. Sadiku, and S. M. Musa, and S. R. Nelatury, "Internet of things: An introduction," *International Journal of Engineering Research and Advanced Technology,* vol. 2, no.3, March 2016, pp. 39-43.

[6] M. N. O. Sadiku, J. Foreman, and S. M. Musa, "Big data analytics: A primer," International *Journal of Technologies and Management Research,* vol. 5, no. 9, September 2018, pp. 44-49.

[7] C. M. M. Kotteti, M. N. O. Sadiku, S. M. Musa, "Big data analytics," *Invention Journal of Research Technology in Engineering & Management*, vol. 2, no. 10, Oct. 2018, pp. 2455-3689.

[8] M. N. O. Sadiku, Y. Wang, S. Cui, and S. M. Musa, "Cyber-physical systems: A primer," *European Scientific Journal*, vol. 13, no. 36, 2017, pp. 52-58.

[9] G. Iltis, "The 4 Most dangerous manufacturing cybersecurity threats," January 2020, https://www.tech-pointe.com/blog/manufacturing-cybersecurity-threats

[10] A. B. Feeney, S. Frechette, and V. Srinivasan, "Cyber-physical systems engineering for manufacturing," in *Springer Series in Wireless Technology, Industrial Internet of Things: Cyber manufacturing Systems,* chapter 4, 2017.

[11] Deloitte, "Cyber risk in advanced manufacturing," https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf

[12] L. Wang and X. V. Wang, *Cloud-Based Cyber-Physical Systems in Manufacturing.* Springer 2018.

ABOUT THE AUTHORS

Matthew N.O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Philip O. Adebo is an instructor at Texas Southern University. He completed his PhD in Electrical and Computer Engineering, Prairie View A&M University with emphasis on power systems. His research interests include power systems, renewable energy, microgrids, smart-grid systems, restructuring power system and optimization of power systems.

Abayomi Ajayi-Majebi is a professor in the Department of Manufacturing Engineering at Central State University in Wilberforce, Ohio. In 2015 he was honored by the White House as a Champion of Change for his significant contributions to the engineering education of minority students. He is a senior member of both the Society of Manufacturing Engineers and the American Society for Quality.

Sarhan M. Musa is a professor in the Department of Electrical Engineering at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His research interests include computer networks and computational electromagnetics.

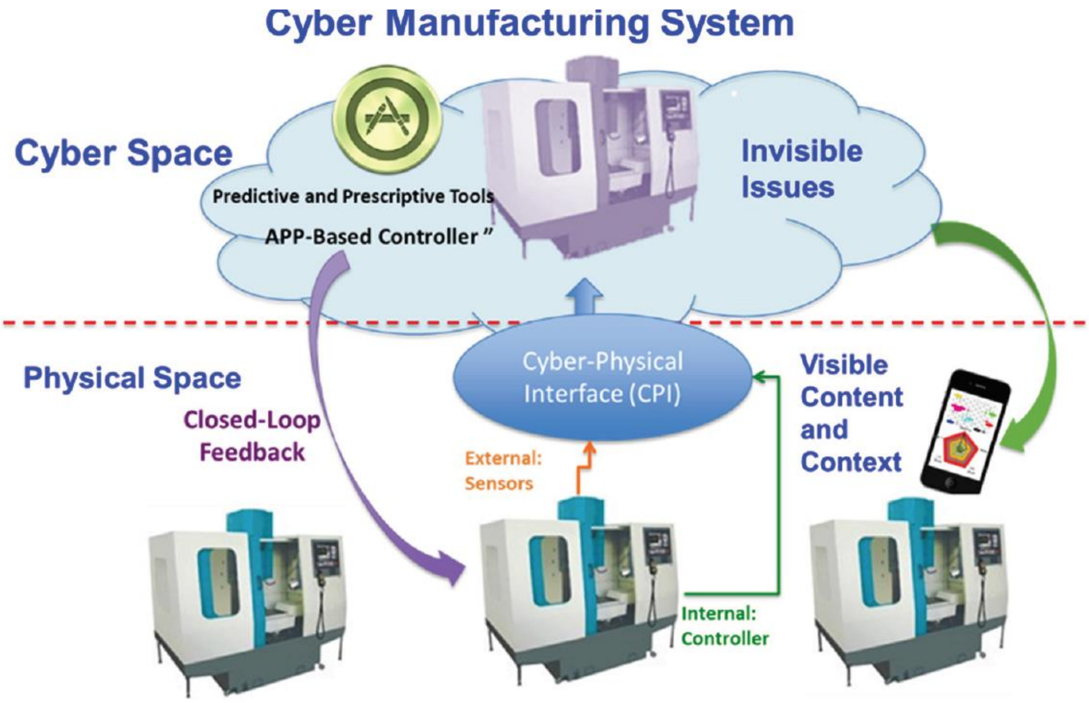

Figure 1. Cyber manufacturing system [3].

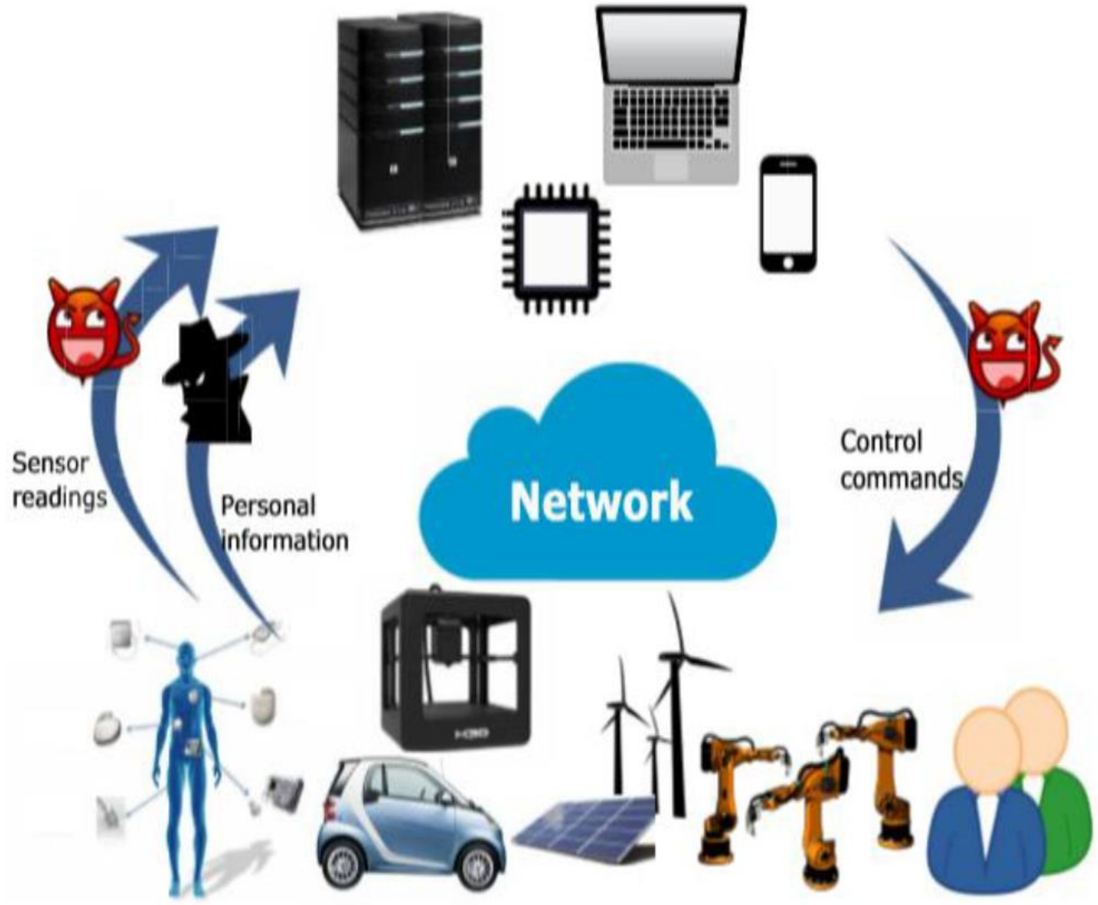

Figure 2 General representation of CPS [4].