International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 11 ǁ November 2022 ǁ PP. 366-370

Embedded System for Intelligent Mobile Cyber-Physical Systems (CPS)

Uma G. Kartha
Lecturer in Electronics,
Govt. Polytechnic College, Chelad, Kothamangalam, Kerala.

Abstract:
A cyber-physical system is made up of a collection of computing devices that communicate with one another and interact with the physical world via feedback loops of sensors and actuators. A cyber-physical system (CPS) is a system that seamlessly monitors and controls physical processes by integrating physical and computer components. These systems combine sensing, actuation, computation, and communication functions to improve physical system performance, security, and reliability.
Keywords: *Embedded System, Mobile, Cyber-Physical System, Mobile IoT, Sensor Network, Physical System.*

I. Introduction:

The first is an embedded system, the second is the Internet of Things (IoT), the third is an autonomous vehicle, and the fourth is a sensor network. A mechanism is a cyber-physical system (CPS). Computer-based algorithms are intended to control or monitor that mechanism. The entire system is obviously linked to the Internet, hence the cyber part of the name. Physical and software components in cyber-physical systems operate on different spatial and temporal scales. CPS applications include self-driving cars, medical monitoring, process control systems, robotics systems, automatic pilot avionics, smart grids, traffic logistics systems, and so on. CPS (cyber-physical systems) have emerged as an exciting research paradigm. This advancement is the result of the convergence of control, communication, and computation. We can expect to find them embedded in various objects and structures in the physical environment as they become less expensive. This lays the groundwork for applications that connect the "cyberworld" of computing and communications with the physical world, with the potential for significant social and economic impact. Unlike traditional embedded systems, which focus solely on computing elements, CPS considers the physical, real-world components that interact with computing elements in cyberspace. CPS examples include a wide range of complex man-made systems, including avionics, vehicles, transportation, healthcare, smart grid systems, and others. [1-2]

However, the majority of the initial CPS research efforts have come from the real-time and embedded systems communities. For example, the ACM Special Interest Group on Embedded Systems (SIGBED) and the IEEE Technical Committee on Real-Time Systems (TCRTS) cosponsored ICCPS. As previously stated, because the distinguishing feature of CPS is the tight integration of cyber and physical components, it is obvious that networking (or mobile computing) plays a critical role in the coordination of CPS's cyber and physical elements. In fact, "Internet of Things" (IoT) architectures and protocols must necessarily promote CPS applications. The combination of IoT and CPS enables the collection, management, and processing of large datasets, as well as the support of complex processes for managing and controlling physical systems at various scales.

The provision of IoT-enabled CPS for mobile objects and devices is the focus of mobile IoT/CPS. With their increasing processing power, range of sensors, and pervasive cellular connections, mobile internet devices such as the iPhone and Android phones already provide ubiquitous platforms for developing robust, reliable, and secure mobile IoT/CPS applications. As a result, the goal of this special issue is to contribute to the direction of research on mobile IoT/CPS by addressing issues critical to mobility, ranging from advances in the underlying science to development and implementation challenges. Figure 1 depicts the primary research areas on which this special issue focuses. [3-4]

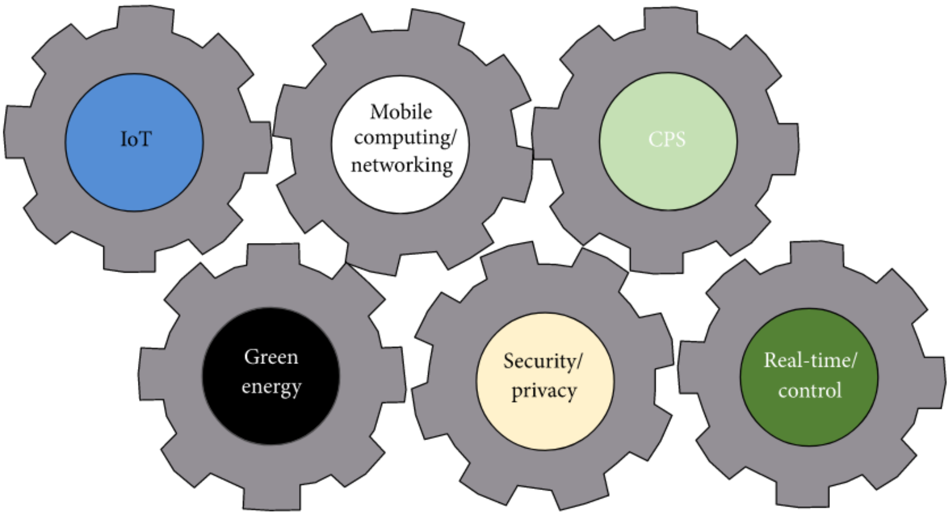

Figure 1: Major areas of research focus in this special issue.

An embedded system is a computer system that is embedded within a physical device or product to perform a specific function. It is intended to carry out specific tasks and functions and is frequently part of a larger system. Embedded systems are typically built around a microcontroller or microprocessor, but may also include sensors, actuators, and input/output interfaces. [5-6]

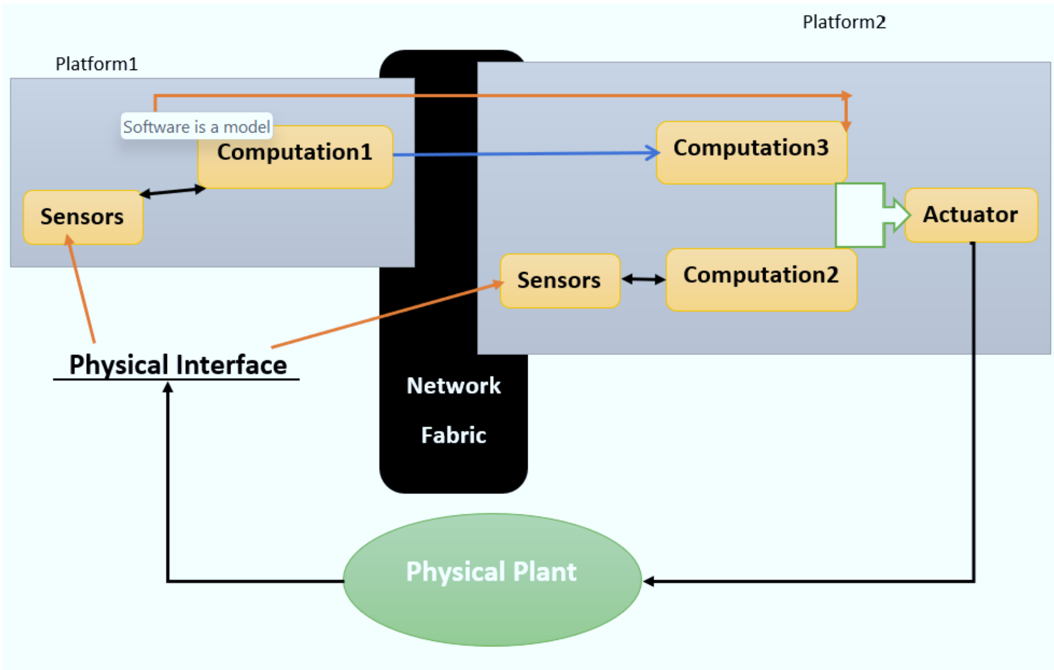

Figure 2: Cyber-Physical System

Objectives:

- Embedded system is integrated into Cyber-Physical System
- Analysis Cyber-Physical System Components
- To define Model of a smart cyber-physical manufacturing system.

II. Research Methodology:

This study focuses on cyber physical systems, with a particular emphasis on real-time issues. Computation and communication are integrated with physical processes in cyber physical systems. Embedded computers continuously monitor and control physical processes. As these embedded computers become more networked, it is expected that a revolutionary transformation will occur. Embedded computers will evolve from small self-contained systems to cyber-physical systems by sensing, monitoring, and controlling our physical environment, just as personal computers evolved from word processors to global communications devices for information gathering and sharing. Journals, articles, books, and websites were used to complete this research.

III. Result and Discussion:

Figure 3 depicts the proposed framework's three main components. The first component is the physical system, which is primarily a sensor network or a multi-sensory device that reads data from the environment via physical sensors and converts sensory information into digital signals that a computer can process. The physical system can be any type of sensor network that generates valuable data and requires CPS action and/or outputs. The second component is the Cyber System, which is where the majority of the processing takes place. The Cyber System is a modular software on a cloud server that controls sensory and UI inputs, handles data flow, and prepares outputs. The Cyber System is also in charge of defining a set of rules for communicating with the data storage server via a Database Management System (DBMS). The communication protocol is the third and final component of this CPS framework. The communication protocol specifies the rules for sending and receiving instructions and data between cyber and physical systems. The proposed framework enables the connection of multiple physical systems to a single cyber system. As a result, the communication protocol makes physical system configurations easier as well as continuous, uninterrupted data transmission for real-time applications possible. The main CPS components are described in greater detail below. [7-8]

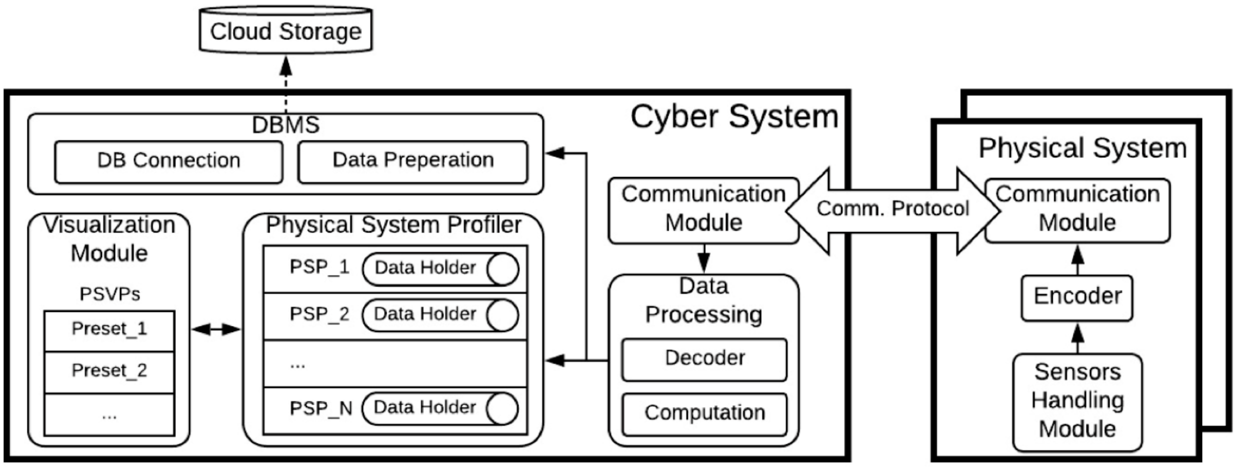

Figure 3: The main components of the proposed Cyber-Physical Systems (CPS) framework include one or more physical systems, a cyber system, and a well-defined communication protocol. PSVPs: pre-coded physical system visualisation presets; DMBS: Database Management System; DB: Database.

Figure 4 depicts the smart cyber-physical manufacturing system (Smart-CPMS) model of a manufacturing system. Individualised products are one of the major manufacturing trends. More customised products, shorter product life cycles, highest quality, and lower prices are demanded. In order to meet these requirements, manufacturing systems must be equipped with advanced features that allow them to adapt to manufacturing changes. The Smart-CPMS is capable of responding quickly and correctly to changes in the manufacturing environment without the need for external intervention. [9-10]

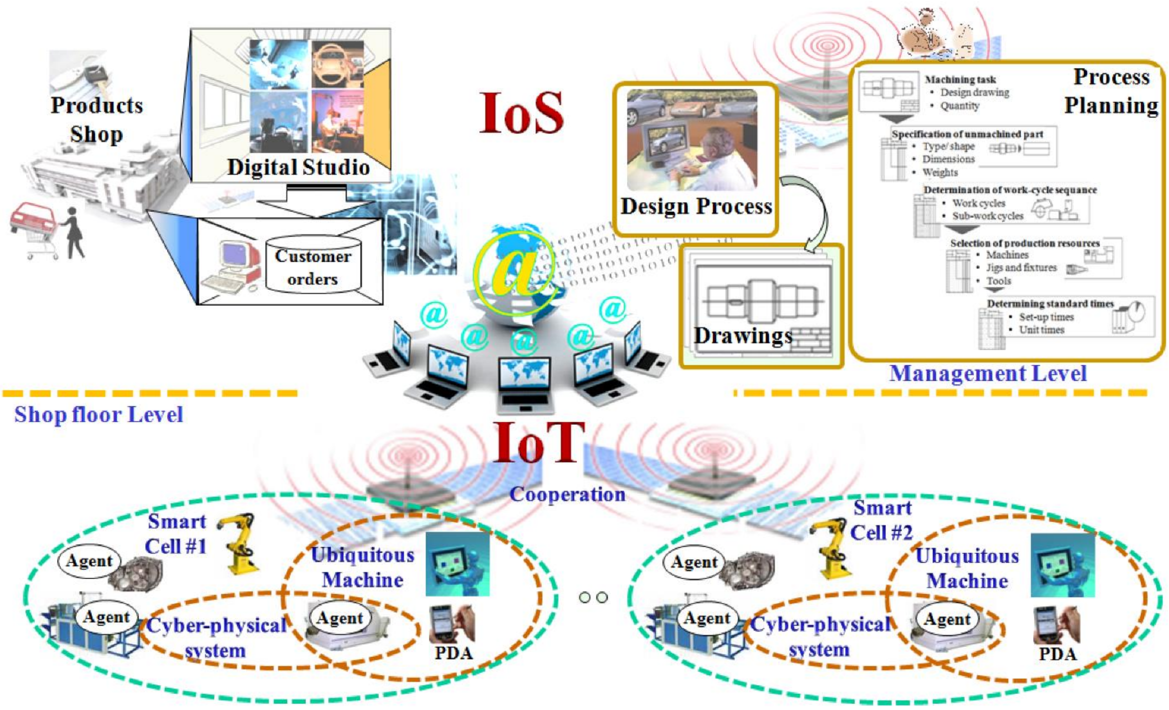

Figure 4: Model of a smart cyber-physical manufacturing system.

Customers order their products in the digital studio using the head mounted display with automatic guides for selecting product characteristics. The product information is then sent to the design process and process planning department, which generates the scheduling for the product's manufacturing on the shop floor. Evolutionary algorithms inspired by biology, such as genetic algorithms, ant colony optimisation, and so on, are used in this phase to generate optimal process planning. Numerous studies have used methods such as holonic execution manufacturing systems and agent-based dynamic scheduling to address optimisation problems at the management level. The internet of service (IoS) is effectively used in Smart-CPMS for task sharing ranging from design to process planning generation. [11-12]

IV. Conclusion:

CPSs combine computational and physical processes. The economic potential of CPSs is far greater than has been realised, and significant investments are being made around the world to develop the technology. CPS technological advancements will enable capability, adaptability, scalability, resiliency, safety, security, and usability far exceeding that of today's simple embedded systems. Mobile system design and deployment should consider network structures and protocols, access points, communication and presentation standards, privacy, security, and encryption, among other things. Operating systems embedded in these end devices are also taken into account for data encoding and presentation. Mobile systems must take into account the fact that sensitive data can be accessed and possibly modified from anywhere in the world.

References:

[1]. Cognivue, G2-APEX IP - High Performance Image Cognition Processor Core. Available from: <http://www.cognivue.com/G2APEXIP.php>.[2015].

[2]. Henshaw, M. J. C. (2016). "Systems of systems, cyber-physical systems, the Internet-of-things… What next?" Insight, vol.19, no. 3, October 2016, pp. 51–54.

[3]. Jordans, R., Corvino, R., Jóźwiak, L. and Corporaal, H. (2013). Exploring Processor Parallelism: Estimation Methods and Optimization Strategies. DDECS 2013 - 16th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems, IEEE Computer Society Press, pp. 18-23, (Best Paper Award).

[4]. Wan, K. et al. (2011). "Investigation on composition mechanisms for cyber physical systems," International Journal of Design, Analysis nd Tools for Circuits and Systems, vol. 2, no. 1, August 2011, pp. 30-40

[5]. L. Jóźwiak, N. Nedjah, M. Figueroa Modern Development Methods and Tools For Embedded Reconfigurable Systems - A survey Integration - The VLSI Journal, 43 (1) (2010), pp. 1-33

[6]. Ashibani, Y. and Mahmoud, Q. H. (2015) "Cyber physical systems security: analysis, challenges and solutions," Computer & Security, vol. 68, 2017, pp. 81-97.

[7]. Pirbhulal, S.; Zhang, H.; E Alahi, M.; Ghayvat, H.; Mukhopadhyay, S.; Zhang, Y.-T.; Wu, W. A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network. Sensors **2016**, 17, 69.

[8]. Derhamy, H.; Eliasson, J.; Delsing, J.; Priller, P. A survey of commercial frameworks for the Internet of Things. In Proceedings of the IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–8.

[9]. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf. Secur. Appl. **2018**, 38, 8–27.
[10]. Leitao, P. A bio-inspired solution for manufacturing control systems. In International Conference on Information Technology for Balanced Automation Systems; Azevedo, A., Ed.; Springer: Boston, MA, USA, 2008; pp. 303–314.
[11]. Al-Jaroodi, J. et al. (2016). “Software engineering issues for cyber physical systems,” Proceedings of IEEE International Conference on Smart Computing, May 2016.
[12]. Stojmenovic, I. and Zhang, F. (2015). “Inaugural issue of ‘cyber physical systems,’” Cyber-Physical Systems, vol. 1, no. 1, 2015, pp.1-4.