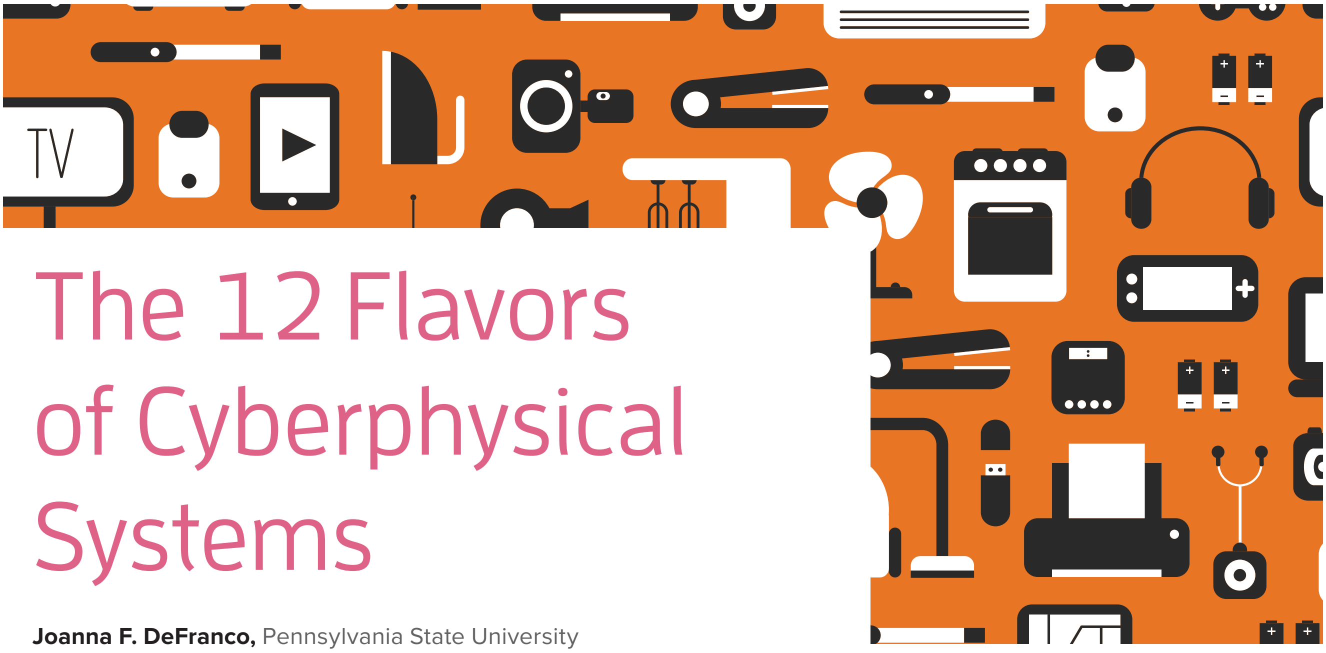


The 12 Flavors of Cyberphysical Systems

Joanna F. DeFranco, Pennsylvania State University

Dimitrios Serpanos, University of Patras

There is wide variation in the definitions of cyberphysical systems and the Internet of Things. Different organizations have attempted to provide clarity, as consensus and consistency will help advance both technologies.

In the October issue of *Computer*, the "12 Flavors of IoT" were presented in this column.[1] A part two and follow-up column on cyberphysical systems (CPSs) is appropriate given their relationship to the Internet of Things (IoT).

It is not surprising that, when a new technical concept is introduced, its definition evolves until it reaches a stable state—this can take years. The definition variations could simply be due to the technology's application use expanding and/or its architecture being refined, and so on. The problem is that, given the nature of the Internet, the varying definitions are persistent and cause confusion. This situation has occurred with the definitions of both *IoT* and *CPS*. In addition, the relationship between the IoT and CPS technologies adds to the complexity of creating clear definitions. Thus, work groups, consortiums, government entities, and various stakeholders have attempted to provide clarity with their own definitions.

The term *CPS* was coined by Dr. Helen Gill, a scientist at the National Science Foundation (NSF). CPSs were at the forefront of discussions beginning in 2006.[8] In 2008, Dr. Gill defined *CPS* at a workshop titled "New Research Directions for High Confidence Transportation CPS: Automotive, Aviation, and Rail" and at a conference held at Carnegie Mellon University.[9,10]

Since 2008, the CPS domains have expanded to systems such as

- communication (for example, cellular, sensor networks, and wireless)
- consumer (such as audio and video systems as well as interactive games)
- energy (including energy production, distribution, and optimization)
- infrastructure (for example, disaster recovery; health monitoring; and water safety, distribution, and optimization)

Digital Object Identifier 10.1109/MC.2021.3112319
Date of current version: 17 November 2021

EDITOR JOANNA F. DEFRANCO
Pennsylvania State University; jfd104@psu.edu

- manufacturing (such as robotic machinery, embedded vision, and computer-controlled actuation)
- military (encompassing unmanned vehicles and weapon systems, among others)
- physical security (including card access control, video analytics, and so on)
- robotics (such as motion control, among others)
- smart buildings (for example, building system management)
- transportation (including automotive, avionics, aerospace, railroads, traffic management, and so forth).

The goal of this article is to facilitate a path toward a consistent understanding of CPSs, as was done with the "12 Flavors of IoT" column in October 2021.[1] Definitions of CPSs written by the most prominent CPS stakeholders, beginning with Dr. Gill's 2008 definition to the present, are analyzed and compared to the agreed upon CPS characteristics. This article also discusses the key differences and relationship between CPSs and the IoT.

CPS CHARACTERISTICS

Platforms4CPS and the National Institute of Technology (NIST) gathered different experts to specifically discuss and determine CPS characteristics. The results from these two major collaboration efforts were used to analyze the prevalent CPS definitions.

Platforms4CPS (platforms4cps.eu) is a European consortium of experts from academia and industry with the mission of creating a "vision, strategy, and technology building blocks" to support the developers of CPS applications. One of the outcomes of this consortium is a document describing the foundations of CPS engineering that includes six CPS characteristics.[7]

The Smart Grid and Cyber-Physical Systems Program Office at NIST also defined six CPS characteristics in SP 1900-202.[5] Table 1 shows both sets as well as a mapping of the Platforms4CPS characteristics to the NIST ones. As a result, two of the Platforms4CPS components were mapped to the NIST hybrid system attribute. Also, the trustworthiness characteristic was not addressed by Platforms4CPS. Therefore, the six NIST CPS characteristics are used to analyze the 12 CPS definitions in the next section.

CPS DEFINITIONS

Table 2 shows the 12 CPS definitions from key CPS stakeholders. The CPS characteristics from Table 1 were mapped to each definition in Table 2. For example, one of the first CPS definitions is from the NSF. It shows that the first definition in 2008 maps to all NIST components except for trustworthiness. Overall, most definitions recognize the hybrid systems and hybrid methods. However, most are missing some verbiage to address control (nine out of 12), component classes (eight out of 12), time (eight out of 12), and trustworthiness (10 out of 12).

TABLE 1. The CPS characteristics.

	NIST (SP 1900-202)[5]	Platforms4CPS[7]
1	*Hybrid systems*: The architecture of CPSs consists of both physical and logical elements, for example, a system that can address the close interactions and feedback loop between sensing systems and physical components	*Physical action or processes*: For example, motion/control functionalities *Energy*: For example, storage, distribution, harvesting, and efficiency
2	*Hybrid methods*: Software to join the integrated physical and logical systems, comprising the networking, information processing, sensing, and actuation that allow the physical device to operate in a changing environment	*Processing*: For example, information
3	*Control*: Using computational systems to control physical processes and engineered systems, such as to monitor, coordinate, and control physical operations using computing and communication	*Communication*: For example, between things and machines, including wired/wireless and local/global
4	*Component classes*: For example, physical/engineered components, sensors, actuators, IT systems, and so on	*Sensing*: Of the physical world
5	*Time*: Integrating the physical-world time with event-driven computation	*Coordination and collaboration*: For example, for physical actions occurring outside the system
6	*Trustworthiness*: Safety, reliability, and security	—

TABLE 2. The CPS definitions mapped to defined CPS characteristics.

Entity	Definition	CPS component mapping
NSF (2008)[10]	"Cyber-physical systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale. Computing is 'deeply embedded' into every physical component, possibly even into materials. The computational core is an embedded system, usually demands real-time response, and is most often distributed. The behavior of a cyber-physical system is a fully-integrated hybridization of computational (logical) and physical action."	Maps to 1, 2, 4, and 5 Missing 6: trustworthiness
NIST (website)[11]	"Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic."	Maps to 1 and 2 Missing 3, 4, 5, and 6: control, component classes, time, and trustworthiness
CPS PWG NIST SP 1500-201 (2017)[3]	"Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment including human interaction."	Maps to 1, 2, 4, and 5 Missing 3 and 6: control and trustworthiness
IEEE Standard 2413 (2019)[2]	"A cyber-physical system is a system in which the physical world, such as production sites, and the digitalized cyber world are harmoniously combined."	Maps to 1 Missing 2, 3, 4, 5, and 6: hybrid methods, control, component cases, time, and trustworthiness
An academic work group website on CPSs[12]	"Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa."	Maps to 2 and 3 Missing 1, 4, 5, and 6: hybrid systems, component classes, time, and trustworthiness
IEEE Technical Committee on CPS (website)[13]	"CPS addresses the close interaction and deep integration between the cyber components such as sensing systems and the physical components such as varying environment and energy systems."	Maps to 1, 2, 4 Missing 3, 5, and 6: control, time, and trustworthiness.
ACM[14]	"Cyber-physical systems are systems with a coupling of the cyber aspects of computing and communications with the physical aspects of dynamics and engineering that must abide by the laws of physics."	Maps to 1 and 2 Missing 3, 4, 5, and 6: control, component classes, time, and trustworthiness
Cyber-Physical Systems Virtual Organization (website)[15]	CPSs "are engineering systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components."	Maps to 1 and 2 Missing 3, 4, 5, and 6: control, component classes, time, and trustworthiness
NASA (website)[16]	"Cyber-Physical (CPS) denotes the emerging class of physical systems that exhibit complex patterns of behavior due to highly capable embedded software components. Also known as hybrid systems (a hybrid of hardware and software), or mechatronic systems (mechanical + electronic), these include devices with content, or knowledge, that gives them unprecedented capabilities in interoperability and interaction, resilience, adaptivity, and emergent behavior."	Maps to 1 and 2 Missing 3, 4, 5, and 6: control, component classes, time, and trustworthiness
U.S. Department of Transportation (2014)[17]	(From a presentation): A CPS is connected system with a path to vehicle automation using an infrastructure and new data for asset monitoring, predictive modeling, and control. Impacts safety, mobility, and the environment.	Maps to 1, 2, 3, and 6 Missing 4 and 5: component classes and time
U.S. Department of Homeland Security (website)[18]	"Smart networked systems with embedded sensors, processors and actuators that sense and interact with the physical world and support real-time, guaranteed performance in safety-critical applications."	Maps to 1, 2, 4, 5, and 6 Missing 3: control
Cyber-Physical Systems Program Solicitation NSF (2021)[19]	"Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components."	Maps to 1 Missing 2, 3, 4, 5, and 6: hybrid methods, control, component cases, time, and trustworthiness

TABLE 3. The CPS and IoT component consensus issues.

Components	CPS	IoT
Control	Some definitions have a greater emphasis on the control of physical processes.	Some definitions have a greater emphasis on information flows from sensors.
Platform	Platform choice is a systemic decision and depends on system functionality.	The IoT can be a platform for or a simpler form of a CPS to achieve collaboration in a distributed system.
Internet	Inconsistency occurs if the Internet is among CPS design options.	There can be inconsistent association of the IoT with the Internet.
Human	Some emphasize human interaction.	Some minimize human interaction.

CPSs VERSUS THE IOT

There is no doubt that the CPS and IoT technologies are related; however, there is limited consensus on the exact similarities, differences, and relationship between them. Many researchers have attempted to explain distinct variations; however, the challenge is, again, a lack of consistency in their respective definitions. In the work by Greer,[5] an analysis of the literature discussing CPSs versus the IoT showed four schools of thought: equivalency, partial overlap, CPSs are a subset of the IoT, and the IoT is a subset of CPSs. Note that IEEE Standard 2413 states, "An IoT system is a cyberphysical system, which interacts with the physical world through sensors and actuators."[2] Does this imply equivalency?

Greer[5] also described four specific components that add to the inconsistency between how much the CPS and IoT technologies overlap: control, platform, Internet, and human. The respective definitions of these four components for both CPSs and the IoT, shown in Table 3, create a problem in drawing a distinct conclusion about the CPS/IoT relationship/differences.

Another way to analyze and determine the exact distinctions between these two technologies is to review and compare the functionality of CPSs and the IoT within system architecture layers. Fatima et al.[6] reviewed functionalities in the analytic, intelligence, control, and configuration layers of each system architecture. For example, in the analytic layer, performance prediction (for example, tracking and responding to system changes) is a significant system requirement of a CPS but not common in an IoT system. Thus, theoretically, adding performance prediction to an IoT device would convert it to a CPS.

We are still left with four questions: Is the IoT a subset of CPSs? Are CPSs a subset of the IoT? Are CPSs and the IoT equivalent technologies? Do the CPS and IoT technologies only partially overlap? We can't answer these questions until there are clear and consistent definitions of CPS and IoT. The hope is that the two "12 Flavors" columns together will provoke clear definitions for both technology communities, as consistency in these definitions will help to incite new innovations, applications, and collaborations.

REFERENCES

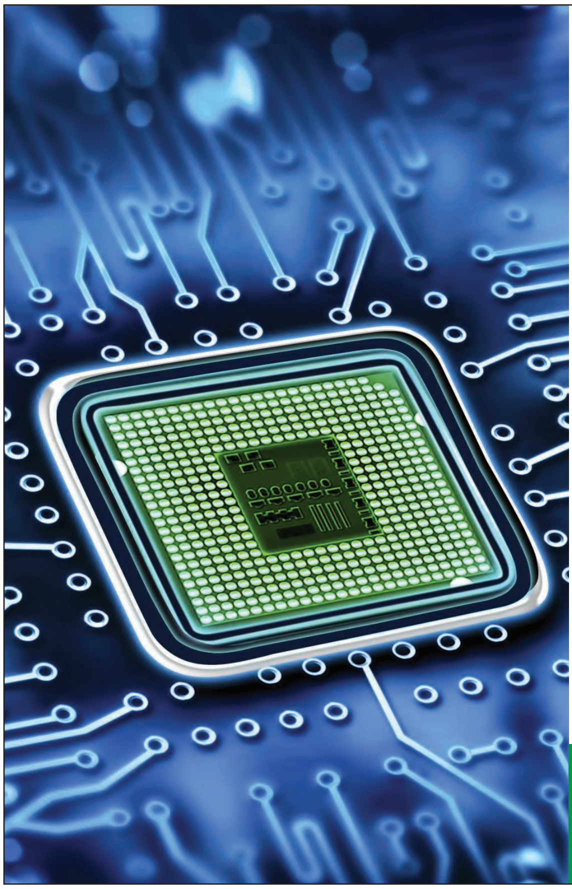
1. J. DeFranco, "12 flavors of IoT," *Computer*, vol. 54, no. 10, pp. 133-137, Oct. 2021.
2. *IEEE Standard for an Architectural Framework for the Internet of Things*, IEEE Standards Association, Piscataway, NJ, IEEE 2413, 2019.
3. Cyber-Physical Systems Public Working Group, "Framework for cyber-physical systems: Volume 1, overview," NIST, Gaithersburg, MD, NIST SP 1500-201, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
4. D. Serpanos, "The cyber-physical systems revolution," *Computer*, vol. 51, no. 3, pp. 70–73, 2018. doi: 10.1109/MC.2018.1731058.
5. C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and internet of things" NIST, Gaithersburg, MD, NIST SP 1900-202, 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf
6. I. Fatima, A. Anjum, S. Malik, and N. Ahmad, "Cyber physical systems and IoT: Architectural practices, interoperability, and transformation," *IT Prof.*, vol. 22, no. 3, pp. 46–54, May 2019. doi: 10.1109/MITP.2019.2912604.
7. "D4.3 Collaboration on the Foundations of CPS Engineering," Platforms4CPS, 2018. [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bf0e32f9&appId=PPGMS
8. NSF Workshop on Cyber-Physical Systems, Cyber-Physical Systems Virtual Organization, 2006. [Online]. Available: https://cps-vo.org/node/179
9. "From vision to reality: Cyber-physical systems," NITRD, 2008. https://tinyurl.com/khf8p2
10. "A continuing vision: Cyber-physical systems," NITRD, 2008. https://tinyurl.com/frwkkedv
11. "Cyber-physical systems," NIST, Gaithersburg, MD. Accessed: Sept. 8, 2021. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems
12. "Cyber-physical systems," Berkeley CPS Publications. Accessed: Sept. 8, 2021. [Online]. Available: https://ptolemy.berkeley.edu/projects/cps/
13. IEEE Technical Committee on Cyber-Physical Systems (CPS), IEEE

Systems Council, 2017. Accessed: Sept. 8, 2021. [Online]. Available: www.ieee-cps.org

14. ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). Accessed: Sept. 8, 2021. [Online]. Available: http://iccps.acm.org/
15. “Internet of Things & cyber-physical systems,” CPS-VO. Accessed: Sept. 8, 2021. [Online]. Available: https://cps-vo.org/group/iot
16. “Cyber-physical systems modeling and analysis (CPSMA) initiative,” NASA, Washington, DC. Accessed Sept. 8, 2021. [Online]. Available: https://www.nasa.gov/centers/ames/cct/office/studies/cyber-physical_systems.html
17. NSF Workshop on Cyber-Physical Systems, NSF Transportation CPS, 2014. [Online]. Available: https://highways.dot.gov/sites/fhwa.dot.gov/files/docs/research/publications/multimedia/6606/cps.pdf
18. “Cyber physical systems security,” Homeland Security. Accessed: Sept. 8, 2021. [Online]. Available: https://www.dhs.gov/science-and-technology/cpssec
19. “Cyber physical systems (CPS),” National Science Foundation, Alexandria, VA, 2021. [Online]. Available: https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm

JOANNA F. DEFRANCO is an associate professor of software engineering at The Pennsylvania State University, Malvern, Pennsylvania, 19355, USA. Contact her at jfd104@psu.edu.

DIMITRIOS SERPANOS is president of the Computer Technology Institute and a professor at the University of Patras, Patras, 26504, Greece. He is the editor of the “Cyber-Physical Systems” column of *Computer*. Contact him at serpanos@computer.org.



Digital Object Identifier 10.1109/MC.2021.3122783