NIST Special Publication 1900-202

Cyber-Physical Systems and Internet of Things

Christopher Greer
Martin Burns
David Wollman
Edward Griffor

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-202

CYBER-PHYSICAL SYSTEMS

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1900-202

Cyber-Physical Systems and Internet of Things

Christopher Greer
Martin Burns
David Wollman
Edward Griffor
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-202

March 2019

CYBER-PHYSICAL SYSTEMS

U.S. Department of Commerce
Wilbur L. Ross Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology (NIST) Special Publication 1900-202

61 pages (March 2019)

Publications in the SP 1900 subseries present information of interest to the cyber-physical systems (CPS) community, where CPS are defined as smart systems that include engineered interacting networks of physical and computational components. The series was established in 2016 by the Smart Grid and Cyber-Physical Systems Program Office of the NIST Engineering Laboratory to provide a separate identity for CPS and Internet of Things publications, including those concerned with the foundations of CPS, CPS testbed science, and CPS applications, e.g., smart grid, smart cities and intelligent transportation. The series reports on research, guidelines, and outreach efforts in CPS, and its collaborative activities with industry, government, and academic organizations.

Certain commercial entities, equipment, or materials may be identified in this document to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the by NIST, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose. All registered trademarks or trademarks belong to their respective organizations.

National Institute of Standards and Technology Special Publication 1900-202
Natl. Inst. Stand. Technol. Spec. Publ. 1900-202, 61 pages (March 2019)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-202

Revision Tracking

Version	Date	Editor	Changes
1.0	March 2019	Christopher Greer	First Release

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The phrases "cyber-physical systems," or "CPS," and "Internet of Things," or "IoT," have distinct origins but overlapping definitions, with both referring to trends in integrating digital capabilities, including network connectivity and computational capability, with physical devices and systems. Examples range from intelligent vehicles to advanced manufacturing systems, in sectors as diverse as energy, agriculture, smart cities, and beyond.

There has historically been uncertainty about the relationship between CPS and IoT, which has hindered close interaction and communication across the respective communities. This document describes the origins of these terms, analyzes the range of definitions over time, and describes a unified perspective that clarifies that relationship and reduces uncertainty to promote a common basis for working together — exchanging best practices and ideas, pursuing shared goals, avoiding duplication of effort, reducing the proliferation of conflicting standards, and catalyzing discovery and innovation.

Analysis of CPS publication trends over the past decade reveals a pattern of steady expansion. Review of 31 published CPS definitions reveals common terminology from computer science and systems engineering. The definitions are largely consistent over time and highlight a set of 6 common CPS characteristics: hybrid physical and logical systems, hybrid analytical and measurement methods, control, component classes, time, and trustworthiness.

Analysis of IoT publication trends reveals 3 temporal phases: low numbers and growth rates in 2005-2009, an increase in 2010-2013, and rapid growth after 2014. Review of 30 IoT definitions reveals terminology from the networking/information technology communities. Analysis of these definitions over time reveals an evolution from trackable and data objects to hybrid systems in which these objects are components in interactive and smart systems. Recent IoT definitions are largely interchangeable with those for CPS.

In 11 publications comparing and contrasting CPS and IoT, distinctions between them were found to hinge on 4 issues: control, platform, internet, and human interactions. Further analysis indicates these issues are insufficient for drawing a reliable distinction between CPS and IoT. The lack of consistent distinguishing metrics and the convergence of definitions indicate an emerging consensus around the equivalence of CPS and IoT concepts. This convergence creates opportunities for progress through integrating the research, innovation, and standards efforts of the respective communities.

Two models provide the bases for a unified CPS/IoT perspective. A unified components model provides 4 categories for CPS and IoT components: logical, physical, transducing, and human. A unified interactions model provides a formal basis for describing CPS and IoT performance. The unified perspective reflects the convergence of CPS and IoT definitions and can be expressed as follows: Internet of Things and cyber-physical systems comprise interacting logical, physical, transducer, and human components engineered for function through integrated logic and physics. Three criteria based on a characteristic set of components, capabilities, and functions are proposed for interchangeably labeling a system ‘CPS’ or ‘IoT’.

Implications of a unified CPS and IoT perspective include the opportunity for CPS and IoT research communities to work together to develop unified, new, hybrid discrete and continuous methods for CPS and IoT design, operation, and assurance; and highlight the importance of tight logical-physical linkage (e.g. robust sensing and actuation, secure systems, sound digital models, etc.) as the basis for the transformational nature of CPS and IoT concepts. The depth of these implications is illustrated in examples of design assurance and cyber-physical security for complex CPS/IoT systems. Collectively, the conclusions in this document can inform research; commercial; standards; and legal, policy, and regulatory efforts designed to realize the value to society of advanced cyber-physical systems and Internet of Things technologies.

1 Introduction

This document focuses on the meanings of the phrases "cyber-physical systems" (CPS) and "Internet of Things" (IoT), and on the relationship between them. The purpose is to promote a unified measurement science and standards foundation for assured design and operation of complex CPS and IoT applications.

These phrases emerged in the science and technology literature at different times and from different expert communities. Despite distinct origins, CPS and IoT refer to a related set of trends in integrating digital capabilities (i.e. network connectivity and computational capability) with physical devices and engineered systems to enhance performance and functionality. Examples of such systems[1] range from intelligent vehicles and smart grids to advanced manufacturing systems and wearable medical devices. These technology trends create opportunities for progress and economic growth in sectors ranging from energy and transportation to health care, agriculture, public safety, smart cities, and beyond.

Uncertainty about the relationship between CPS and IoT has hindered close interaction and communication across the respective communities. The analyses presented in this document are intended to clarify that relationship and reduce uncertainty to promote a common basis for working together — exchanging best practices and ideas, pursuing shared goals, avoiding duplication of effort, reducing the proliferation of conflicting standards, and catalyzing discovery and innovation.

This document is not intended as a comprehensive review of the extensive CPS and IoT literature. Informative reviews can be found in the accompanying list of references [1-16].

2 Cyber-Physical Systems History and Definitions

2.1 History and Trends

Recent published histories of CPS [cf. 4,9] generally ascribe coining of the phrase 'cyber-physical systems' in 2006 to Helen Gill of the US National Science Foundation (NSF), but also point to its emergence from earlier concepts, including mechatronics, embedded systems, pervasive computing, cybernetics, and others. Key initial events were an October 2006 NSF Workshop on Cyber-Physical Systems [17]; a November 2006 workshop on Network Embedded Control for Cyber-Physical Systems [18]; a 2007 report from the President's Council of Advisors on Science and Technology (PCAST) that highlighted CPS as a national research and development priority [19]; and a call for proposals for CPS research by NSF [20]. These events led to steady growth in research in cyber-physical systems.

Figure 1 below shows the results of a Google Scholar search for the terms 'cyber-physical systems' or 'cyberphysical systems.' Note that the results were restricted to those articles with the relevant terms in the title to capture those with a significant focus on the subject. The results show a steady growth from 35 articles in 2006 to more than 1,000 articles in 2017.

[1] 'Throughout this document, "system" has the meaning provided by the ISO/IEC/IEEE 15288 definition: "Combination of interacting elements organized to achieve one or more stated purposes."

Figure 2 shows the results of a Google Trends analysis of worldwide queries for 'cyber-physical systems.' These results also show a steady increase in interest in CPS (as reflected in web queries) over the period January 2005 through May 2018.

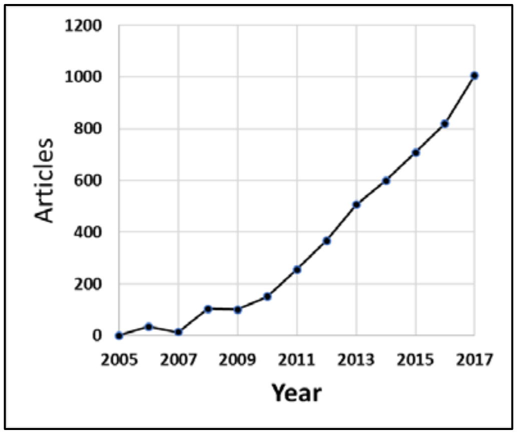

FIGURE 1. CPS ARTICLE TRENDS

Two implications of these results are as follows. First, the trend lines in both CPS research articles and search queries are consistent with a field that is in a steady expansion phase with no indications of a decline in growth. Second, the absolute value of the number of articles for CPS (e.g. 1,007 in 2017; Figure 1) is much less than that for IoT (e.g. 13,840 in 2017; Figure 4), consistent with a much broader adoption of the latter term in the research community and corresponding interest in the technical and popular press.

2.2 Examples of CPS Definitions

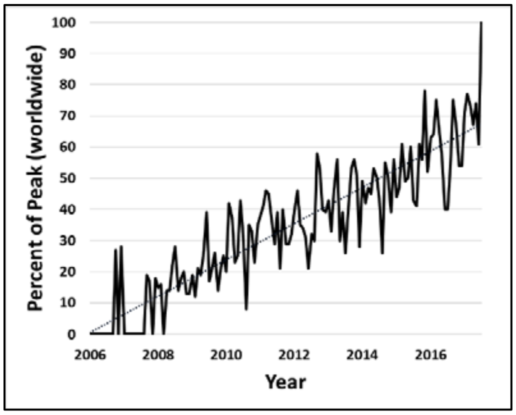

FIGURE 2. CPS QUERY TRENDS

Appendix A provides examples of CPS definitions. These examples are intended to provide a representative sampling and are not comprehensive. In total, 31 definitions are included, covering the period 2006 through 2018 to show the evolution of the definitions over time.

Figure 3 below shows a word cloud image generated from the combined text of CPS definitions in Appendix A. The image was generated with the Word Clouds application (https://wordclouds.com) using the word count listed in Table 1, which comprises words occurring 5 or more times in the definitions. Common terms (the, and, of, will, etc.) were excluded from this list.

Table 1. CPS Word Count

Count	Word	Count	Word
93	system(s)	13	communication
75	physical	12	capabilities
43	CPS(s)	10	actuator(s,ing)
34	cyber-physical	9	interact(ing)
30	world	8	computer(s)
26	integrate(ion)	7	dynamics
25	computation(s, al)	6	(inter)connected
23	cyber	6	human(s)
19	networked(s, ing)	6	monitor(ed)
18	components	5	core
17	control	5	design
17	processes	5	devices
17	sensor(s,e,ing)	5	interactions
15	engineered(ing)	5	monitoring
14	computing	5	smart
14	embedded	5	software

The CPS concept emerged from an intersection of the computer science and engineering communities in areas like embedded computing and mechatronics. The former – computer science — is reflected in the frequent use of terms like cyber, computation, networks, and software. The latter in terms like physical, integration,

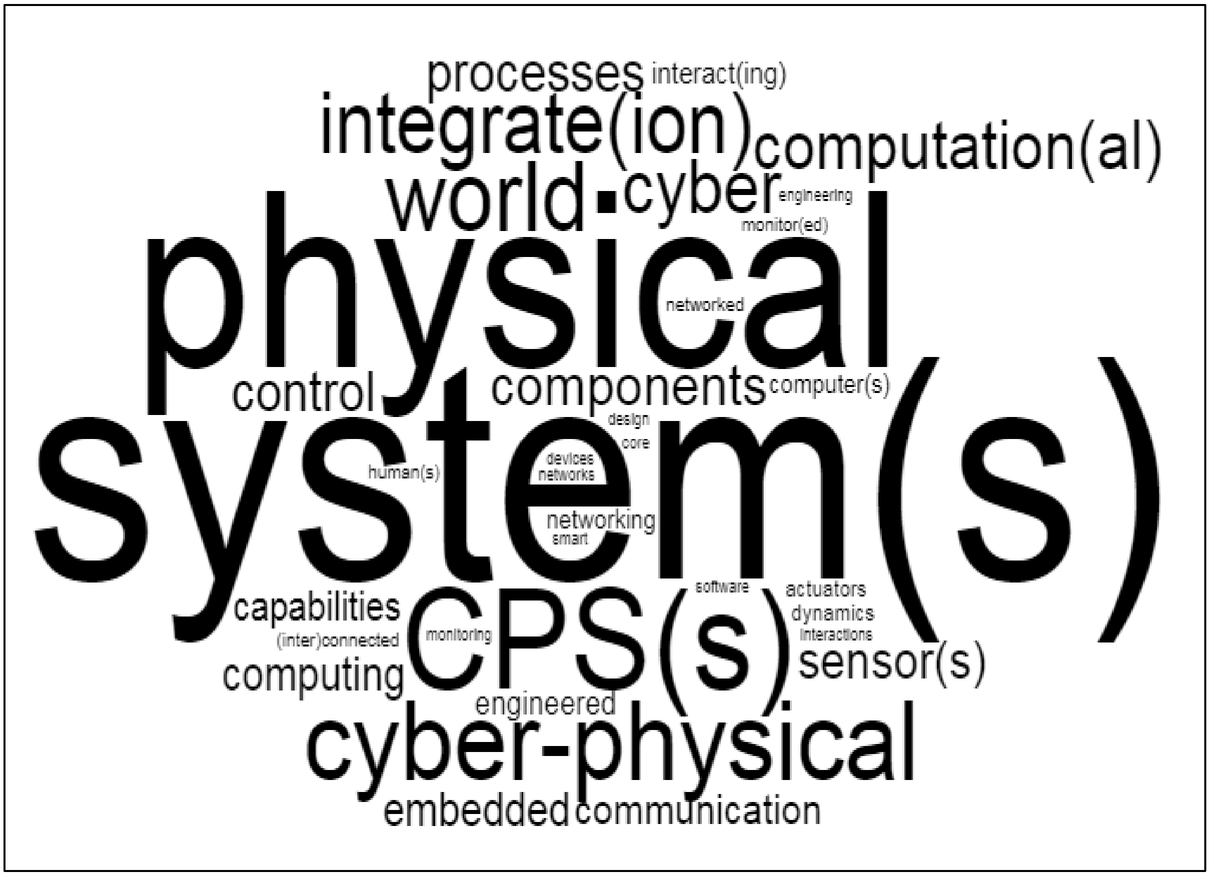

FIGURE 3. CPS WORD FREQUENCY

components, control, processes, engineering, and systems (the anchor for the CPS label). This intersection of fields has focused descriptions of research challenges and corresponding innovation opportunities around the concepts of hybrid physical and logical systems. A comparison of terms used in CPS and IoT definitions (compare Tables 1 and 2) reveals their distinct origins, with IoT arising in the networking and information technology communities.

2.3 Analysis of CPS Definitions

The CPS definitions in Appendix A are listed by year of publication or web page update to enable evaluation of trends in the evolution of definitions over time. The definitions are largely consistent over the years covered in this collection and highlight a set of six common CPS characteristics as follows.

1. **Hybrid Systems**: Systems that are hybrids of physical and logical elements are central to both early and more recent definitions.

   2006: *Cyber-Physical Systems (CPS) are integrations of computation with physical processes* [21]

   2018: *CPS addresses the close interactions and feedback loop between the cyber components, such as sensing systems, and the physical components* … [22]

2. **Hybrid Methods**: The unique challenge of developing hybrid approaches that join discrete and continuous methods for integrated physical and logical systems is highlighted in many definitions.

   The intellectual heart of CPS is in studying the joint dynamics of physical processes, software, and networks. [23]

   The dynamics among computers, networking, and physical systems interact in ways that require fundamentally new design technologies. [24]

   Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. This makes smart systems possible but also creates the need for a new 'systems science' that can lead to unprecedented capabilities. [6].

3. **Control**: Many definitions highlight as a central characteristic the control of physical processes and engineered systems by computational systems.

   Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world [25]

   Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core [1]

4. **Component Classes**: While individual definitions focus on subsets, collectively, the definitions describe a consistent set of three, overarching classes of CPS components: physical/engineered components, transducers (sensors and actuators), and information technology (IT) systems, including network/communication systems, and computation/analysis/control systems. Some definitions include humans as interacting components.

   CPS is envisioned to be a heterogeneous system of systems, which consists of computing devices and embedded systems including distributed sensors and actuators. These components are inter-connected together … [26]

   These NIT [networking and information technology] *systems, in which computing and networking are deeply integrated into other engineered systems, are connected to the physical world through sensors and actuators to perform crucial monitoring and control functions safely and dependably* [19]

   The computational and physical components of such systems are tightly interconnected and coordinated to work effectively together, sometimes with humans in the loop [7]

   Eindhoven Institute for Research on ICT (EIRCT) identified the six components which, occasionally, have been used to make up CPS: physical world, transducers, control components, data analytics elements, computation elements and communication components (cited in [10])

5. **Time**: The integration of physical-world time with event-driven computation is highlighted as a unique challenge for CPS.

> *In the physical world, the passage of time is inexorable, and concurrency is intrinsic. Neither of these properties is present in today's computing and networking abstractions* [21]

> *These concerns are of particular importance in cyberphysical systems in which computation and communication timing and event semantics are interdependent with physical timing and event semantics* [26]

6. **Trustworthiness**: Many CPS definitions invoke requirements for safety, reliability, and security (elements of the Trustworthiness Aspect in the NIST CPS Framework [11]) where there is involvement of critical physical processes and engineered systems.

> *There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general-purpose computing* [28]

> C*yber Physical Systems (CPS) are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications*. [29]

> *A cyber-physical system (CPS) integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safety, securely, efficiently and real-time* [3]

3 Internet of Things History and Definition

3.1 History and Trends

An accounting of the history of IoT, including the technology advances that led to the concept, can be found in the following references [12-15, 30]. The origin of the specific phrase 'Internet of Things' is generally ascribed to Kevin Ashton in 1999, with a presentation to Proctor and Gamble and related work in the MIT Auto-ID Center [31, 32, 33]. Thus, the IoT concept emerged from the RFID (radio-frequency identification) community and initially focused on the ability to track location and status for any physical object or thing, particularly in supply-chain applications.

> *If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best* [31]

Figure 4 shows the results of a Google Scholar search for articles with 'Internet of Things' or 'IoT' in the title. The results show significant growth in the field from 32 instances in 2005 to nearly 14,000 worldwide in 2017. The curve is consistent with at least 3 temporal phases: low numbers and growth rates from 2005 to 2009, moderate numbers and growth rates in 2010-2013, and large numbers and rapid growth from 2014 to 2017 (the last full year for which data are available). The recent, rapid growth phase coincides with increased commercial and popular interest in IoT (see, for example, Fig. 5 below).

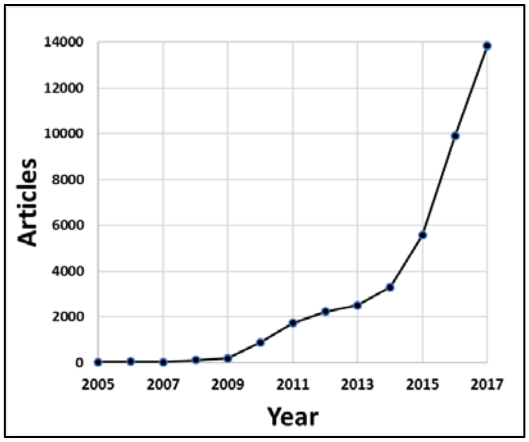

FIGURE 4. IOT ARTICLE TRENDS

Figure 5 shows the results of a Google Trends analysis of worldwide queries for 'Internet of Things' or IoT. The results show slow growth rates for the period 2005 through 20013, followed by rapid growth in 2014 through 2016. The growth rate tapers off in 2017 and the first half of 2018, possibly signaling a plateau in interest.

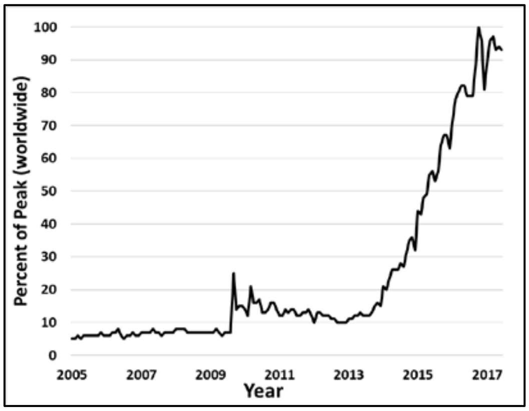

FIGURE 5. IOT QUERY TRENDS

In another measure of popular interest, reference to 'Internet of Things' was first made in the annual Gartner hype curve published in 2011, with IoT placed in the rising phase of the curve [34]. IoT reached the peak of the curve in 2014 and 2015, and then was replaced by "IoT Platform" in 2016 [35]. This sequence is also consistent with a period of popularization followed by a more recent shift in popular interest.

3.2 Examples of Definitions

Figure 6 below shows a word cloud image generated from the combined text of the 30 examples of IoT definitions listed in Appendix B that cover the years 2002 through 2018 to show the evolution of definitions over time. The image was generated with the Word Clouds application (https://wordclouds.com) using the word count listed in Table 2, which comprises words occurring 5 or more times in the definitions. Common terms (the, and, of, will, etc.) were excluded from this list.

Consistent with its emergence from the networking and information technology communities, frequently used terms include information, communication, networks,

Table 2. IoT word Count

Count	Word	Count	Word
53	thing(s)	8	smart
39	Internet	7	digital
38	IoT	7	everyday
34	physical	7	infrastructure
25	world	7	protocols
24	information	7	system(s)
22	connect(ed,ivity,ion)	6	capable
21	objects	6	human(s)
20	network(s)	6	global
19	communication	6	interconnected
17	sensor(s,e,ing)	6	process(ing)
16	virtual	6	seamlessly
14	services	6	technologies
13	data	5	anything
13	devices	5	capability
9	actuator(s,e,ion)	5	environment
9	intelligent(ce)	5	identities
8	capabilities	5	interoperable
8	computer(s,ing)	5	self-configuring
8	integrated	5	standard

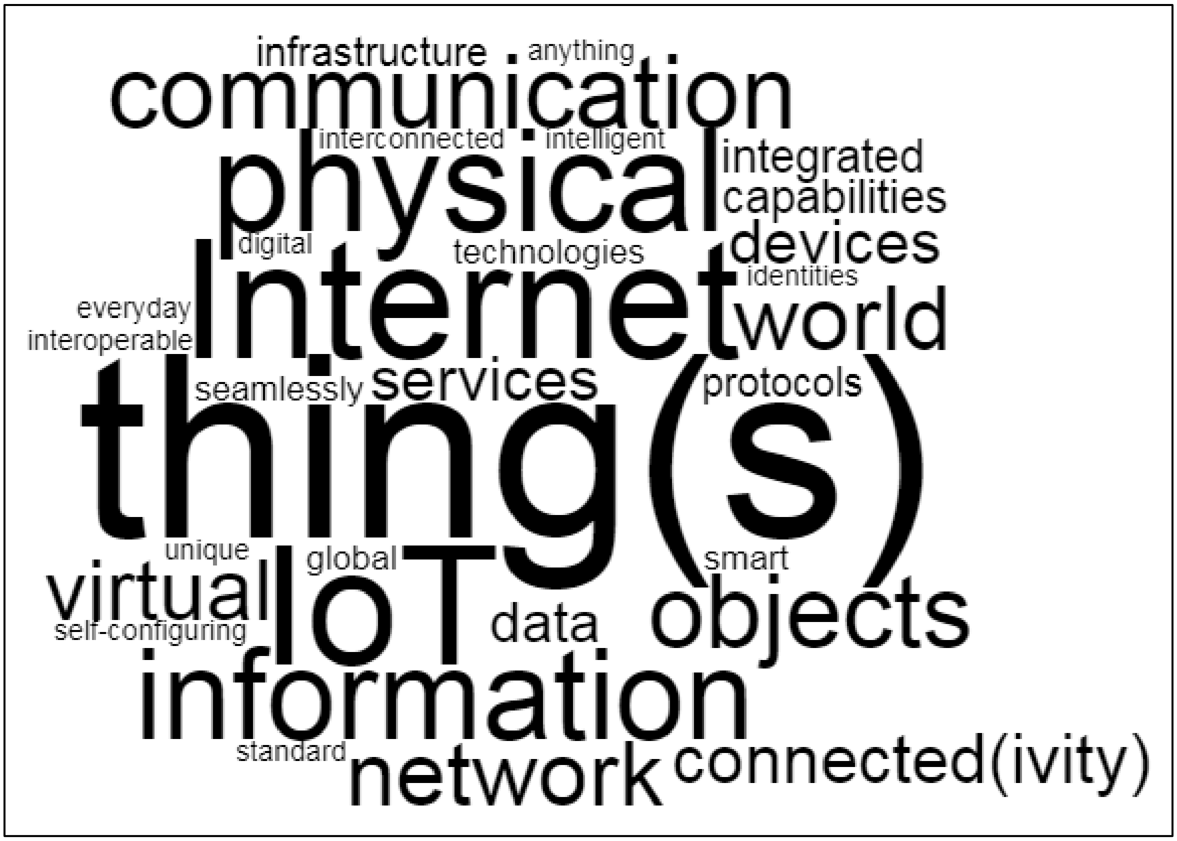

FIGURE 6. IOT WORD FREQUENCY

connectivity, and data. Highlighting the role of IoT in linking the physical and virtual worlds, 'physical' is the fourth most frequently used term, occurring in 19 of 30 definitions in Appendix B.

> *The idea of IoT is to interconnect the physical world with the digital world* [36]

This linking of physical and virtual worlds is the role of transducers – sensors that gather information about the physical world and actuators that act upon it. Notably, the term 'sensors' is used more frequently than 'actuators,' among both CPS and IoT definitions (compare tables 1 and 2), with 'sensors' appearing alone in those definitions that emphasize information flow while omitting consideration of the applications of that information. Thus, an emphasis on information gathering is not, alone, a discriminating factor between CPS and IoT.

3.3 Analysis of IoT Definitions

The examples of IoT definitions in Appendix B are listed by year of publication or web page update and cover the years 2002 through 2018. This list is intended to be a representative sampling and is not comprehensive.

3.3.1 IoT Object Categories

A set of 4 categories of objects, defined by their capabilities, have previously been described based on an analysis of the IoT literature [33] and provide a convenient means for describing the relationships among the various IoT definitions and their evolution over time. These Object Categories are:

- *Trackable Objects (TO): Mobile things that can be uniquely identified and are aware of their physical location*
- *Data Objects (DO): Things producing data either from sensors or their current properties or state*
- *Interactive Objects (IO): Things that allow an interaction with the environment where they are immersed, either by measuring environmental variables, modifying the environment or both*
- *Smart Objects (SO): Interactive things that can apply some degree of processing to data obtained or received and act accordingly* [33]

With origins in the RFID context, most initial IoT concepts focused on Trackable Objects: low-power, limited-capability 'things' (e.g. a packaged product with an RFID tag) that are uniquely identified and can interact to provide location or simple state information. Over time, the IoT concept expanded to include 'things' with sensors (Data Objects; e.g. consumer appliances with sensors) offering new data streams that could be used for measurement and analytical purposes and to create value-added features and services. A more recent expansion has been to things that actively interact with the physical world through actuators (Interactive Objects, e.g. a remotely-accessible door lock) and that have analytical capabilities for adaptive and responsive interactions (Smart Objects, e.g. an autonomous vehicle).

These IoT Object Categories – Trackable, Data, Interactive, and Smart - are useful in component-level design. For example, requiring significant computational capability may be feasible for many Smart Objects but not for most simple Trackable Objects. However, these Categories can be productively considered not just in isolation but rather in a systems context in which the functional objective (i.e. the desired goal or outcome in system design) is considered. Take, for example, the functional objectives of safety and quality in a food supply chain management system. An active RFID tag and the crate of tomatoes to which it is attached is a Trackable Object in that system. The handheld, wireless RFID reader used when the crate is transferred from one shipper to another is a Data Object for streaming information about routing and timing of intermediate steps. The composite system of sensors, actuators, networks, and analytics that evaluates delay times, excessive temperatures, jostling and other factors and activates a diverter (possibly an Interactive Object) to automatically separate out a suspect crate it has identified in an automatic sorting facility is a Smart Object (see [33]).

This example illustrates three points. First, many IoT applications are systems-of-systems in which the components may themselves be a mix of Trackable, Data, Interactive, or Smart Objects. Enumeration of design requirements and assurance assessment for each component can only be undertaken in the context of the overall functional objective, including evaluating not only the capability of each component but also requirements for interactions with other components in the system.

Second, the progression over time from an emphasis on Trackable and Data Objects to Interactive and Smart Objects represents a convergence of the IoT concept with cyber-physical systems by including interactions between logical and physical components. Indeed, many current IoT instances cited as examples of Trackable or Data Objects may best be seen as components in an Interactive or Smart IoT system when considered in their functional context. For example, a wearable fitness device (e.g. a smart watch) has the function of helping a user to improve fitness. The device has sensors for detecting the physical environment (e.g. LED-based heart rate measurement), networking for data transmission, on-board and remote analytics, and actuation (e.g. a buzzer for alerts) to modify a physical state (the wearer's activity). Note that the latter – invoking the wearer as component – is essential to measuring system performance against the objective (increased fitness). Collectively, this system could be described as either an IoT application or a CPS with considerations of component capability equally relevant in both perspectives.

Third, a single device or system may fall into multiple Object Categories, depending on the application. A smart phone may be used as a Trackable Object in one application (e,g, navigation or 'find-your-phone' applications), a Data Object in another (posting information to friends about your current location), or an Interactive or Smart Object in a third (e.g. interacting remotely as a component in your home energy management system). This example underlines the importance of considering the concept of IoT Object Category in an integrated systems and functional context and not just enumerating capabilities in isolation.

3.3.2 Evolution over Time

Examining the IoT definitions in Appendix B over time reveals additional insights into the evolution of the IoT concept.

> *Technology has been constantly evolving and so has the concept of the Internet of Things, incorporating new terminology appropriate to technological advances and different application domains* [33]

Early IoT definitions, in the period 2002-2010, focus on adding things – physical devices and objects – to the digital world by giving them a digital identity and network connectivity.

> *The Web, the collection of all devices connected to the Internet, is on the verge of experiencing a massive evolution from a Web of computers to a Web of things as new devices such as phones, beepers, sensors, wearable computers, telemetry sensors, and tracking agents connect to the Internet* [37]

> *A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, any place connectivity for anyone, we will now have connectivity for anything* [38]

This early, digital-world-centric focus expanded a bit in 2011 with increased attention to new capabilities that could be provided by connectivity.

> *The mash-up of captured data with data retrieved from other sources, e.g., with data that is contained in the Web, gives rise to new synergistic services that go beyond the services that can be provided by an isolated embedded system*. [39]

> … *physical and virtual objects with unique ID are discovered and integrated seamlessly (taking into account security and privacy issues) in the associated information network where they are able to offer and receive services which are elements of business processes* … [40]

Consistent with this expansion was the emergence in 2011 and 2012 of the Industrial Internet [41] and Industry 4.0 concepts [42], which added complex industrial and manufacturing systems to the everyday devices and objects that prevailed in earlier IoT concepts.

This trend towards more complex 'things' was reflected in an expansion of IoT definitions in 2014 and beyond from Trackable and Data Objects to include Interactive and Smart Objects.

> *The smart object is the building block of the IoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact/control the physical world, but also to be interconnected …* [43]

> *The IoT model involves sensing, thinking, and acting, usually occurring iteratively in that order* [44]

> *The three most recurring* [IoT] *concepts are sensors, intelligence, and actuators. While sensing capabilities have been considered since the first interpretations of the IoT, it is not the case with intelligence and actuators* [33]

The most recent step in the evolution of IoT definitions has been an emphasis on the integration of the physical and digital worlds. These most-recently evolved IoT definitions are largely interchangeable with those for CPS.

> *Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an aeroplane, into part of the IoT. This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without a human being involved, and merging the digital and physical worlds* [45]

4 Comparison of CPS and IoT

4.1 Distinct Origins

Appendix C provides examples from articles that compare and contrast CPS and IoT concepts, listed by year of publication or web page update. This list is intended to be a representative sampling and is not comprehensive. In total, 11 references are included, covering the period 2011 through 2018.

The CPS and IoT concepts emerged from different communities, with CPS primarily emerging from a systems engineering and control perspective.

> *A cyber-physical system is a system of collaborating computational elements controlling physical entities. It is when the mechanical and electrical systems … are networked using software components. They use shared knowledge and information from processes to independently control logistics and production systems* [30]

In contrast, the IoT concept emerged primarily from a networking and information technology perspective, which envisioned integrating the digital realm into the physical world.

> *The term "Internet-of-Things" is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities* [46]

4.2 Description of Previously-Proposed CPS/IoT Overlap Models

Despite their distinct origins, most of the analyses in Appendix C recognize an overlap between the CPS and IoT concepts. Descriptions of this overlap fall into at least four general categories as illustrated in the Venn diagrams of Figures 7A through 7D and described in the paragraphs below (see also [10]).

These categories are: (A) Partial Overlap; (B) Equivalence; (C) CPS as a Subset of IoT; and (D) IoT as a Subset of CPS. Each of these categories is described below.

4.2.1 Category A, Partial Overlap

This category (Figure 7A) was characterized by assertions among proponents that there are CPS that are not IoT and vice-versa and, thus, the two concepts are distinct with limited overlap. Two types of assertions were made within this category. The first described the overlap between CPS and IoT as limited to a common outcome pursued with different goals. Cited among the unique aspects were networking and connectivity for IoT and feedback and control for CPS.

> *Although both IoT and CPS are aimed at increasing the connection between the cyber space and the physical world by using the information sensing and interactive technology, they have obvious differences: the IoT emphasizes the networking, and is aimed at interconnecting all the things in the physical world, thus it is an open network platform and infrastructure; the CPS emphasizes the information exchange and feedback, where the system should give feedback and control the physical world in addition to sensing the physical world, forming a closed-loop system* [47]

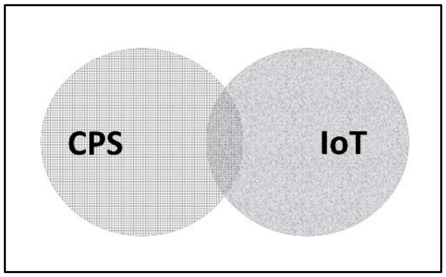

FIGURE 7A. PARTIAL OVERLAP

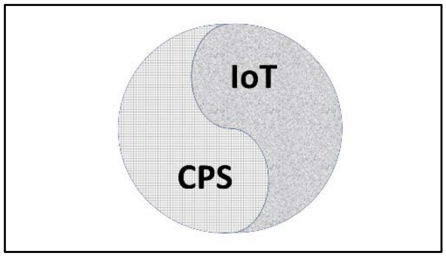

FIGURE 7B. EQUIVALENCE

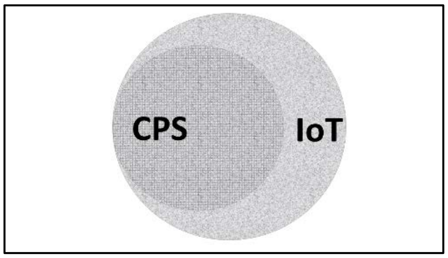

FIGURE 7C: CPS AS A SUBSET

A second assertion within this category was that the role of humans is different. While CPS and IoT collections in Appendix A and B include the term ‘human’ with similar frequencies, the context is different: CPS definitions emphasize system interactions with humans, including ‘human-in-the-loop,’ while IoT definitions emphasize system-to-system interactions and automation, while minimizing human intervention.

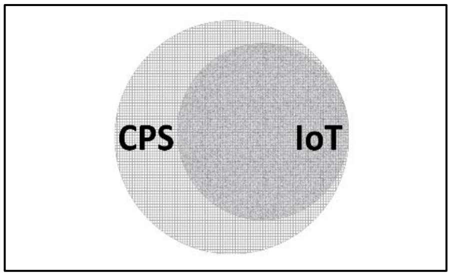

FIGURE 7D: IOT AS A SUBSET

> [CPS] *systems also target the control of combined organizational and physical processes, and therefore specifically address tight human-machine interaction, mostly not addressed in Internet of Things* [48]

> *CPS encompasses both open-loop and closed-loop control systems, while IoT usually focuses on open-loop systems. For instance, both dynamic pricing for indirect/human-in-the- loop load control and closed-loop microgrid control belong to the topics of CPS* [49]

4.2.2 Category B, Equivalence

In this category (Figure 7B), the CPS and IoT concepts were described by proponents as interchangeable with no clear distinctions between the two.

> *In most academic and project activities, the difference between "Internet of Things" and "CyberPhysical Systems (CPS)" is not made clear and it is difficult to find a source that draws a clear-cut distinction between the two terms. Most persons consider the two definitions as different explanations for the same idea and use the words interchangeably* [30]

> *IoT greatly overlaps with CPS, because IoT addresses observing the things in the physical world, exploiting communication capabilities, and capturing data needed to manage the things that aren't efficiently managed today. Even though IoT originally targeted identification and monitoring technologies, today IoT also applies to the control of the physical systems by the integration of RFID systems and Sensor Networks, namely RFID sensor networks* [9]

4.2.3 Category C, CPS as a Subset of IoT

Two distinctions were asserted by proponents of this category to support the notion of CPS as a subset of IoT (Figure 7C). The first described CPS as a platform or building block for IoT.

> *Through cyber-physical systems, the physical world is linked with the virtual world to form an Internet of Things, Data and Services* [50]

A second assertion was that there are IoT instances that are not CPS because they are focused on simple Trackable and/or Data Objects with limited consideration of system-level control.

> [M]*ore encompassing definitions* [of IoT] *include also applications outside the domain of CPS and CPSoS* [cyber-physical systems of systems]*, such as IoT-connected home entertainment systems or geolocation-enabled tracking infrastructures for consumer items* [51]

4.2.4 Category D, IoT as a Subset of CPS

Three distinctions were asserted among proponents of this category to support the notion of IoT as a subset of CPS (Figure 7D). The first focused on a greater emphasis on control for CPS.

> *CPS adds more emphasis to control technologies in what is known colloquially by the term, the 'Internet of Things' ... CPSs feature a tight combination of, and coordination between, the system's computational and physical elements, and integration of computer- and information-centric physical and engineered systems. An important class of CPS is called IoT, and this term is favoured by grant agencies in Europe and Asia* [52]

The second distinction within this category is the assertion that IoT can be a platform for or a simpler form of CPS. The examples below illustrate the breadth of perspectives within this broad category.

> *Internet of Things generally focusses on the sensing of the physical world and the (internet) connectivity, emphasizing individual things providing data over the net to steer (usually organizational) processes. While sensing physical data and communicating it – not necessarily via internet – is generally also required for cyber-physical systems, these systems also target*

> *the control of combined organizational and physical processes, and therefore specifically address tight human-machine interaction, mostly not addressed in Internet of Things* [49]

> *Primarily, IoT is concerned with unique identification, connecting with the Internet and accessibility of "things." Yet, identified objects in an IoT system can still be networked together so as to control a certain scenario in a coordinated way, in which case an IoT system can be considered to grow to the level of a CPS. Generally, we can say that CPS is mainly concerned about the collaborative activity of sensors or actuators to achieve a certain goal and to do this CPS uses an IoT system to achieve the collaborative work of the distributed systems*. [31]

> *Cyber-Physical Systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components … The Internet of Things (IoT) refers to the billions (and growing) of networked physical objects, devices, and systems … The resulting new generations of CPS and their emerging platforms such as the IoT and Industrial Internet (II) have major implications for the future of smart and connected environments* [53]

> *Cyber Physical Systems are Smart Systems that comprises of* [sic] *the merging and integration of Industry Control Systems, Critical Infrastructures, Internet of Things (IoT) and Embedded Systems* [49]

The third distinction within this category was the assertion that systems that are highly-networked internally, but lack broad network connectivity beyond system boundaries, are examples of CPS that are not IoT. An autonomous vehicle with extensive onboard networks operating in an environment with limited or no external connectivity (e.g. driving in a remote location) may be an example.

> *Furthermore, interconnection and addresses are not required in CPS, and IoT is a subset of CPS* [52]

4.3 Analysis of Overlap Models

A comparison of the assertions for each of Categories A-D above indicates that the distinctions being drawn hinge on differing views with respect to four basic issues:

1. **Control**: Emphasis on or de-emphasis of systems-level control, particularly for IoT examples centered on Trackable and Data Object components;
2. **Platform**: Whether IoT should be considered a platform for CPS or vice-versa;
3. **Internet**: Requirements for internet connectivity and the role of Internet Protocol (IP)-based networking; and
4. **Human**: Characterization of the nature and relevance of machine-human interactions.

This section provides an analysis of the differing views on each issue and evidence for an emerging consensus around the convergence of CPS and IoT concepts.

4.3.1 Control

Various definitions in the appendices focus on the assertion that CPS have a greater emphasis on control than IoT. Examples of applications such as smart appliances and tagged objects for location tracking are cited as examples of reduced emphasis in IoT on control of physical states through actuation and greater emphasis on information flows from sensors.

To evaluate this assertion, consider the example of a smart refrigerator, which has sensors and actuators for status awareness and functional control, internet access through a home network, an operating system that supports software applications, and a large touch-screen interface for users. Whether this refrigerator is considered an IoT, CPS, both, or neither depends not just on its capabilities, but how it is used. Consider the following descriptions of uses for this smart refrigerator.

1. If the use is limited to providing network access as an information resource – 'browsing' the web, for example – the device is functioning in the mode of a conventional IT system, analogous to a laptop or tablet. This use case fits neither the IoT or CPS definitions well.
2. If the use is limited to gathering and storing sensor data, locally or remotely, without consideration for any attendant application, it's operating in the mode of a conventional sensor network and fits neither IoT or CPS definitions well. However, this example is overly-constrained as it is neither realistic or useful to invoke stored data never used by any application, or to arbitrarily exclude the application(s) of the data from consideration.
3. If the use includes providing sensor data directly to an application running on the refrigerator operating system – controlling temperature, for example – this is consistent with a conventional embedded system and not a good fit to either IoT or CPS.
4. If the use involves providing sensor data to a remote application via networks – for a service-provider's maintenance system, for example – this would be consistent with some early IoT definitions focused on Trackable or Data Objects, but not with CPS or more recent IoT definitions so long as any outputs or actions by the application are excluded from consideration. As above, this example is overly-constrained as it is neither realistic or useful to invoke an application with no outputs or actions, or to arbitrarily exclude any outputs or actions from consideration.
5. If the use involves sending sensor data to a remote maintenance analytics application resulting in a technician service call for maintenance of refrigerator systems (the overall purpose of this particular system), it fits both IoT and CPS definitions.

This analysis of smart refrigerator uses (and the descriptions in previous sections of RFID-tagged objects in tracking applications and wearable personal fitness devices) illustrate how distinctions between IoT and CPS that are based either on control considerations or constrained to Trackable or Data Object components are often limited to arbitrarily-constrained use cases. When the full system (and not just a subset of components) and its function or purpose are considered, there is typically no meaningful distinction between an IoT and a CPS label. Further, the designation of a system as CPS or IoT is not solely determined by a list of its capabilities, but by how the system is used.

Indeed, omitting considerations of function can lead to significant design errors. For example, failure to implement stringent security requirements could result from failure to recognize that data streamed from a digital camera are intended for private use by parents for remotely monitoring a baby in its crib. Failure to implement stringent network latency provisions could arise from failure to recognize the data are used by a time-sensitive collision-avoidance system in an autonomous vehicle. Designers of a system gathering health data that could be useful to pharmaceutical companies should consider whether the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule apply. These examples illustrate why effective IoT design requires consideration of the functions and applications of the system.

4.3.2 Platform

In the information and communications technology (ICT) context, a platform comprises a set of technology components providing select functions and services for use in supporting a range of applications. An example might be a smartphone operating system that is the foundation for applications with functions ranging from messaging to geolocation, financial transactions, or entertainment. The operating system alone doesn't provide these end functions; they arise from the composition of platform and application. Sound design for compositionality requires that a platform creator consider the range of applications that the platform will support. Similarly, an application developer must assess the range of services provided by a given platform to ensure that these are suitable to the end function. For example, for a financial transaction function involving sharing of sensitive information, effective platform- and application-level cybersecurity are both required. If either is missing, the transaction is vulnerable to intruders. Similarly, a platform without guaranteed latency provisions would create safety risks for a time-critical function such as automated vehicle collision avoidance. These examples illustrate why considering a platform or application in isolation can lead to design limitations or omissions that create safety, security, reliability, and other risks in CPS/IoT systems that can lead to damage or injury in the real world. In this light, IoT or CPS should not be considered only at the platform level and, instead, always in the context of the end functions of the system as a whole. When considered in the overall functional context, considerations for platforms and platform-based design are equivalent for CPS and IoT and are not distinguishing factors.

4.3.3 Internet

The published literature includes a mixture of views on whether IoT may be constrained to systems with internet connectivity or IP-based networking.

> *The use of the word "Internet" in the catchy term "Internet of Things" which stands for the vision outlined above can be seen as either simply a metaphor – in the same way that people use the Web today........or it can be interpreted in a stricter technical sense, postulating that an IP protocol stack will be used by smart things (or at least by the "proxies", their representatives on the network)* [54]

Less than half of the IoT definitions in Appendix B explicitly reference 'internet' (outside of the "Internet of Things" label) or IP networks. The majority use only more general terms such as 'network', 'connected', or 'communication technologies'.

> *[T]he IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT) … The IoT network infrastructure may be realized via existing networks, such as conventional TCP/IP-based networks, and/or evolving networks, such as next generation networks (NGN)* [55]

> *(IoT) is defined by ITU and IERC as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where*

> *physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network* [56]
>
> *IoT is a network that can interconnect ordinary physical objects with identified addresses, based on the traditional information carriers including Internet and telecommunication networks. Therefore, Internet is not mandatory in IoT* [52].

Additionally, there is much discussion in the academic literature and technical press about next-generation protocols, such as Named Data Networking (NDN; see [57]), and the role of alternative protocols, such as USSD (Unstructured Supplementary Service Data) [58] for IoT instances. Thus, there does not seem to be a consensus within the community that IoT is limited to internet-connected systems. There are also various counterexamples. For example, smart grid and smart manufacturing, often cited as a prominent IoT examples, include systems implemented by utilities and manufacturers over private, not public, networks, which may or may not be based on an IP stack. Additionally, most embedded sensor networks have non-TCP/IP protocols yet are typically routed to the Internet via gateways. Such connected devices are frequently cited as IoT instances. These counterexamples also illustrate the degree to which the extent of networking (global versus regional or local, for instance) is not consistently used to rule in or rule out a system as an IoT instance.

Finally, the CPS definitions in Appendix A neither preclude nor constrain CPS with respect to internet or IP networks. Both CPS and IoT definitions assume end-to-end connectivity across various wireless, back-haul, core networks, etc., implicating a diversity of standards and protocols.

Collectively, inconsistent association of IoT with internet, inclusion of internet among CPS options, and the diversity of protocols implemented in both CPS and IoT make this characteristic – internet connectivity – unreliable as a distinguishing feature for IoT versus CPS.

4.3.4 Human

A third issue proposed in distinguishing IoT and CPS emerges from a comparison of definitions that describe the role of human users and operators. While the CPS and IoT collections in the appendices include the term 'human' with similar frequencies, the context is different. CPS definitions emphasize system interactions with humans, including 'human-in-the-loop,' while IoT definitions emphasize system-to-system interactions while minimizing human intervention.

> Appendix A, CPS: *The term cyber-physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities*, [59]; *Cyber Physical Systems (CPS) are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users)* [29]
>
> Appendix B, IoT: *The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention*, [60]; *This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without a human being involved, and merging the digital and physical worlds*, [45]

The distinction being drawn might be compared to the different descriptions a poker player and opponent might provide for a hand of playing cards. While the player would describe his/her cards as having different numbers and symbols, so each card is unique; the opponent would describe the player's cards as all identical with the same pattern or image. Each perspective is correct but non-exclusive, and together are insufficient evidence for two classes of cards. Both automated processes and interactions with humans can simultaneously be true of an IoT or CPS system. In particular, none of the CPS definitions excludes automated system processes. Indeed, autonomy is among the important goals in CPS research (e.g. autonomous vehicles, robotics, etc.). Similarly, none of the IoT definitions envision a physical world without human users. Instead, benefits to and useful interactions with human users are highlighted as key functional goals. In analyzing the IoT concept, van Lier observes that:

> *In many situations it will be unclear or imperceptible whether communication and interaction actually takes place between two or more persons, two or more machines, or a random combination of both* [61]

Thus, the roles of humans and automation do not seem to be valid factors for drawing a distinction between IoT and CPS.

Overall, this analysis indicates that the most commonly cited issues for differentiating between CPS and IoT are insufficient for drawing a reliable distinction. Taken together, this lack of clear and consistent distinguishing metrics and the convergence of definitions over time provide evidence for an emerging consensus around the convergence of current CPS and IoT concepts.

5 Significance of Convergence

This section describes opportunities for progress that arise with the emerging convergence of CPS and IoT concepts. In this section and throughout the document, 'CPS/IoT' is used to refer to systems-of-systems that fit within the converging CPS and IoT definitions. These systems-of-systems are composed of engineered, physical systems integrated with networking, data, and computational systems linked via transducers and interacting with humans who may function as designers, operators, components, etc.

The opportunities for progress fall into three classes. The first is associated with the continuing investment that is being made in CPS research focused on the science and engineering challenges of hybrid systems.

> *Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these critical systems … in a range of application domains including agriculture, aeronautics, building design, civil infrastructure, energy, environmental quality, healthcare and personalized medicine, manufacturing, and transportation* [62]

A clear understanding of the convergence of the CPS and IoT concepts can help the IoT stakeholder community understand how the results of CPS research can best be applied to their efforts. This includes over-the-horizon views of next-generation technologies for future IoT applications.

Second, applications based on IoT concepts are being aggressively expanded across all sectors.

> *Because the benefits really are enormous and the technical advances in smart devices are now rapidly improving, expect the IoT revolution to hit hard in all areas of daily life before 2025 similar to the great impacts occurring now in business-to-business applications* [63]

An understanding of the breadth and complexity of IoT applications; including challenges around scalability, interoperability, and expanded risks to security, safety, resilience, reliability, and privacy; can help the CPS community, armed with an understanding of the relationship between CPS and IoT, to ensure that their basic and applied research efforts are informed by (and address) real-world needs, constraints, and opportunities in the commercial IoT sector.

Third, alignment of standards and best practices around a shared understanding of the relationship between CPS and IoT can improve the efficiency and effectiveness of standards efforts and, most importantly, significantly enhance the opportunities for innovation, economic growth, and progress that result from these efforts.

> *The heterogeneity of IoT platforms is the consequence of multiple different standards and approaches. This leads to problems of comprehension, which can occur during the design up to the selection of an appropriate solution* [36]

An example of the benefits of standards alignment lies in the opportunities for innovation posed by CPS/IoT systems designed for composability and compositionality through standards for modularity and interoperability. Here, composability is defined as the ability to build new things from existing components [64] and compositionality as the principle that the properties of a system are a function of the properties of its components and the interactions between those components, a key aspect of components-based engineering [65].

> *Our central finding is that the hype may actually understate the full potential of the Internet of Things—but that capturing the maximum benefits will require an understanding of where real value can be created and successfully addressing a set of systems issues, including interoperability … We estimate a potential economic impact—including consumer surplus—of as much as $11.1 trillion per year in 2025 for IoT applications in nine settings … Interoperability between IoT systems is critically important to capturing maximum value; on average, interoperability is required for 40 percent of potential value across IoT applications and by nearly 60 percent in some settings* [66]

Composability enables new applications to be built by combining existing sensors, networks, analytics, and other infrastructure for added value and return on previous investment. Compositionality provides a means for ensuring that complex systems assembled from new or existing components, or as modifications to existing systems, are trustworthy: safe, secure, resilient, reliable, and privacy-protecting.

Enablers for both composability and compositionality are interoperability (the ability of two or more systems or components to exchange information and use that information [67]) and modularity (a module is a unit whose structural elements are tightly connected among themselves and relatively weakly connected to elements in other units [68]). At the heart of modularity and interoperability are open, consensus-based standards for communications protocols, reference architectures, data models, and more.

A unified CPS/IoT systems perspective could facilitate coordination across the respective standards efforts to broaden provisions for interoperability and modularity with the goal of enabling creative composition of applications and services by industry.

6 Unified Perspective

Connecting the physical and logical worlds is a central characteristic attributed to both CPS and IoT in recent definitions. This characteristic provides the basis for unified components and interactions models applicable to both CPS and IoT.

6.1 Components Model: Linked Logical and Physical Elements

Figure 8A provides, at a high level, a unified perspective based on the central characteristic of linked physical and logical worlds. The essential features of this figure are as follows.

The upper half of the figure represents the logical realm of information and communications technology (ICT), where processes are described in terms of formal logic and systems are developed with the tools and methods of computer and information sciences and engineering. Both the flow of information through IT systems and operations on that information are represented by the semi-circular arrow in the upper half.

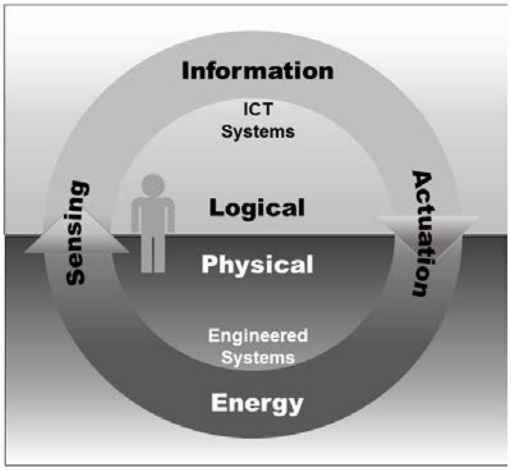

FIGURE 8A. COMPONENTS MODEL

The lower half of the figure represents the physical realm of engineered systems, where processes are subject to the provisions of physics and implementations to those of systems engineering and other engineering disciplines. The flow of energy and energy transformations in physical systems is represented by the semi-circular arrow in the lower half.

Bridging the logical and physical realms in Figure 8A are transducers – sensors that gather data about the physical state of the system that can be used to inform the logical state; and actuators that produce energy inputs that can be used to act on the physical state. The central role of transducers in CPS/IoT systems is to tightly link physical and logical components.

Figure 8A also includes a human-figure icon spanning the logical and physical realm. This icon is intended to represent individual people; collections of individuals, such as a social organization or corporation; or a functional or operational class of people, such as drivers or passengers, etc. The icon also represents the spectrum of roles for people in CPS/IoT systems, including, user, owner, operator, beneficiary, and component. The icon spans the logical and physical realms reflecting human logical/emotional and physical states that are linked through sensing and actuation and that affect the interactions of people with the other components of the system. Note that CPS/IoT systems that include an interacting human component are labeled in some of the literature as 'Human-CPS' or 'H-CPS'.

This model provides a unified means for classifying the components of a CPS/IoT system into four categories: logical, physical, transducing, and human (comprising individuals and organizations).

6.2 Interactions Model: Linked State Transitions

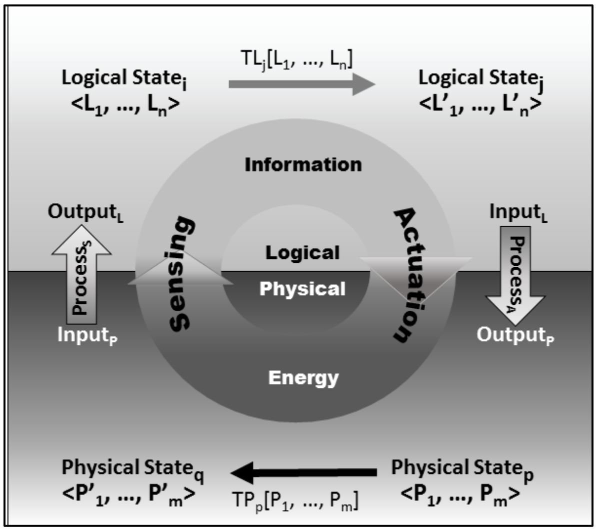

FIGURE 8B. INTERACTIONS MODEL

Figure 8B summarizes the state transitions and their linkage in a CPS/IoT system. The top of the figure shows that a given system has an initial logical state, which is a vector of logical state parameters $<L_1 \ldots L_n>$. That logical state is acted upon by transformations (TL) involving exchanges of information, and operations on that information by algorithms, equations, and other logical processes, resulting in a new logical state.

The bottom of the figure shows that a given CPS/IoT system also has an initial physical state, which is a vector of physical state parameters $<P_1 \ldots P_m>$. That physical state is operated on by transformations (TP) involving exchanges and transformations of energy, resulting in a new physical state. Energy in this model includes all enthalpic and entropic sources and all forms, potential and kinetic, including mechanical, electrical, chemical, thermal, etc.

The sides of the figure show linkage of logical and physical states through transducers. Sensors (left side) respond to a change in the physical state (Input$_P$, e.g. an analog signal level) by producing a new digital representation of that state (Output$_L$, e.g. new values for parameters such as temperature, etc.) for logical system use. The processing (Process$_S$) required to produce Output$_L$ involves the application of a sensor model that includes signal conditioning, analog-to-digital conversion, calibration, quantization, and metadata association. Processing may occur on-board for a smart transducer or remotely in a transducer system. Actuators provide the inverse function, responding to a change in the logical state (Input$_L$, e.g. new state parameters representing 'on' or 'off,' etc.) by producing a new physical representation (Output$_P$, e.g. a new analog signal level to a relay) for physical system use. Although functionally inverse, sensors and actuators differ in two important ways with respect to uncertainty. First, Input$_P$ is subject to physical uncertainty whereas Input$_L$ is subject to computational uncertainty. Second, the sensor model and actuator model for processing each introduce their own forms of uncertainty, which are not equivalent. Managing these differing sources of uncertainty and their interactions for design assurance, including for safety-critical applications, remains an important area of research.

In summary, the essence of this interactions model is that any meaningful[2] change in the logical state of a CPS/IoT system results in a change in the physical state, and vice versa. This model provides a formal basis for describing the behavior of CPS/IoT systems.

[2] 'Meaningful' refers here to a change relevant to the functional objective(s) of the system. For example, in logical systems variation in the value of a parameter may be meaningful but variation in its memory location might not.

6.3 Components Categories

The hybrid physical and logical character of CPS/IoT systems provides a unifying means for categorizing the various components of CPS/IoT systems (see for example [30], [33]) as those that are physical, those that are logical, and those that are transducers between the two. A fourth category is provided for humans, reflecting their combined roles.

6.3.1 Physical Components

Components in the physical realm are frequently given the generic label “things,” (as in Internet of *Things*) and referenced by the term “physical” in cyber-*physical* systems).

> *Within the context of the ‘Internet of Things’, a ‘thing’ is defined as a real/physical or digital/virtual entity that exists and moves in time and space and that can be identified*. [60]

A key phrase in this statement is “exists and moves in time and space and that can be identified.” Thus, in typical CPS/IoT usage, “thing” refers to an engineered system – specifically to the collection of physical and mechanical components serving structural, functional (i.e. energy transformations), or other engineering requirements – and associated digital/logical systems that can be uniquely identified. However, consideration of elements in the physical realm sometimes extends beyond the immediate system of interest to include elements of the physical environment with which the system interacts.

> *A “physical entity” may be defined as a discrete, identifiable part of the physical environment which is of interest to the user for the attainment of his/her goal. Physical entities can be almost any object or environment, from humans or animals to cars, from store or logistic chain items to computers, from electronic appliances to closed or open environments* [30]

Thus, the ‘things’ in a CPS/IoT system can comprise both active (motors, switches, hydraulics, etc.) and passive (shell, frame, structural elements, etc.) components of an engineered system as well as the objects in and characteristics of the physical environment with which it functionally interacts (obstacles, temperature, frictional surface, people, etc.).

6.3.2 Logical components

Components in the logical realm are frequently given the generic label “information and communication technologies (ICT).”

> *Information and Communication Technology. This includes information technology and is any equipment or interconnected system, or subsystem of equipment, which is used in the creation, conversion, duplication, automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, reception, or broadcast of data or information. ICT includes, but is not limited to: electronic content, including email, electronic documents and Internet and Intranet web sites; telecommunications products, including video communication terminals; computers and ancillary equipment, including external hard drives; software, including operating systems and applications; information kiosks and transaction machines; videos; IT services; and multifunction office machines that copy, scan and fax documents* [70]

> *Information and communication technologies (ICT) are defined as digital and analogue technologies that facilitate the capturing, processing, storage and exchange of information via electronic communication* [71]

The term "Information" in ICT typically refers to at least three elements of the data pyramid: data, information, and knowledge. Whether artificial intelligence (AI) extends systems into the realm of "wisdom" at the top of the pyramid is the subject of much debate (cf. [72])

> *Data are symbols that represent the properties of objects and events … Information is contained in descriptions, answers to questions that begin with such words as who, what, when, where, and how many. Knowledge is conveyed by instructions, answers to how-to questions. Understanding is conveyed by explanations, answers to why questions … The difference between efficiency and effectiveness—that which differentiates wisdom from understanding, knowledge, information, and data—is reflected in the difference between development and growth* [73]

Some ICT definitions also include the human aspects of the system.

> *An information (ICT) system is an organised collection of hardware, software, equipment, policies, procedures and people that store, process, control, and provide access to information*. [74]

> *Information and communication technology, or ICT, is defined as the combination of informatics technology with other, related technologies, specifically communication technology. UNESCO defines informatics as the science dealing with the design, realization, evaluation, use, and maintenance of information processing systems, including hardware, software, organizational and human aspects, and the industrial, commercial, governmental and political implications of these* [75]

Thus, the logical components of an Internet of Things/cyber-physical system, implicit in the terms "Internet" and "cyber," respectively, comprise:

- Software layers from firmware, handlers, and drivers to operating systems, middleware, and applications;
- Hardware components from boards, power supplies, and cables to peripherals, fiber, and cooling systems;
- Network and communications fabric, comprising the systems, services and processes described in the 7-layer ISO Open Systems Interconnection (OSI) stack, from physical and data link layers to presentation and application [76], and including wireless messaging and telecommunications protocols, etc.; and
- Information at the levels of data, information, and knowledge.

6.3.3 Transducing Components

The components of CPS/IoT systems that bridge the physical and logical realms are transducers; specifically, sensors and actuators.

6.3.3.1 Transducers

The American National Standards Institute (ANSI) standard MC6.1 defines a transducer as "a device which provides a usable output in response to a specific measurand". An output is defined as an "electrical quantity," and a measurand is ''a physical quantity, property, or condition which is measured."

> *Converts energy input in one form to output in another, with those forms including mechanical, thermal, electrical, magnetic, radiant, and chemical energy* [77]

> *Input transducers are termed sensors, or detectors for radiation, and output transducers are termed actuators or effectors* [78]

6.3.3.2 Sensors

> ***Sensor element**: The fundamental transduction mechanism (e.g., a material) that converts one form of energy into another. Some sensors may incorporate more than one sensor element (e.g., a compound sensor). **Sensor**: A sensor element including its physical packaging and external connections (e.g., electrical or optical). **Sensor system**: A sensor and its assorted signal processing hardware (analog or digital) with the processing either in or on the same package or discrete from the sensor itself. Smart sensors: **Smart sensor:** A sensor designed to present a simple face to the host structure via a digital interface, such that the complexity is borne by the sensor and not by the central signal processing system* [77]

> *Devices which perform an "Input" function are commonly called Sensors because they "sense" a physical change in some characteristic that changes in response to some excitation, for example heat or force, and covert that into an electrical signal* [79]

6.3.3.3 Actuators

> *Devices which perform an "Output" function are generally called Actuators and are used to control some external device, for example movement or sound* [79]

> *Actuator: a mechanical device for moving or controlling something* [80]

Thus, the transducing components of a CPS/IoT system are sensors, which gather information about the physical state of the system for use in logical processes, and actuators, which act in response to logical system outputs, applying energy to alter the physical state of the system.

6.3.4 Human

Note that 'human' is cited in the descriptions of both physical and logical components. This emerges from the combined physical and logical interactions of humans with their environment and is reflected in the positioning of the human icon in Figure 8A (see above) as spanning the two realms. These interactions include designing, operating, assuring, interacting with, guiding, and using CPS/IoT systems. These interactions reflect the varying roles humans may have in CPS/IoT systems, ranging from user to component, environmental factor, etc. (for example, for a Level 3 automated vehicle a passenger is a user, a safety driver is a component, and a pedestrian is an environmental factor). The interactions of humans with CPS/IoT systems may be limited to the logical realm, to the physical realm, or extend to (and link) both. Because of this diversity of interactional modes, humans are treated as a distinct component in the CPS/IoT Components Model.

6.4 Component Capabilities

This section describes general capabilities attributed to the physical, logical, and transducing components of CPS/IoT systems. This list of capabilities provides a basis for organizing CPS/IoT component analyses.

Capabilities attributed to CPS/IoT system logical and physical components are of three categories: transmit, transform, and store. For physical components, it is energy that is transmitted, transformed, or stored; and for logical components, it is information (or data in its most basic form). While storage is an instance of transformation, it is listed separately here as it is treated as a distinct function in many CPS/IoT system component analyses.

The transmission, transformation, and storage of energy in physical components is described by the laws of physics. Examples of physical components in each category include circuits for energy transmission, reactors for energy transformation, and batteries for storage. Thus, the world of CPS/IoT physical components, or things, is populated by engineered, physical systems such as motors, transmissions, and pumps. Events in this world are continuous and subject to physics-based time, and typically described by sets of ordinary differential equations.

The transmission, transformation, and storage of information in logical components is described by the rules of logic. Examples of logical components in each category include networks for transmission, algorithms for transformation, and flash drives for storage. Thus, the world of CPS/IoT logical components is populated by cyber or information and communications technology (ICT) systems such as linked networks, cloud platforms, and data centers. This is a world of discrete events and logical time that is typically described by sets of algorithms.

For transducing components, capabilities attributed to smart transducers are described in the IEEE 1451 family of standards (and in application-based standards) [81], and are of three categories: input, processing and output. Input is derived from the state of the physical or logical systems for sensors or actuators, respectively. Processing includes signal conditioning, analog/digital conversion, metadata (including timing/synchronization), and data processing. For sensors, output is the communication of parameter values and associated metadata to logical systems. For actuators, output takes the form of signaling a change in state settings for engineered systems with energy transmission/transformation control functions (e.g. switches, relays, solenoids etc.).

As described above, humans are placed in a separate category to reflect their varying capabilities (logical, physical, or transducing), differing system roles (user, component, etc.), and varying functions (operator, environmental factor, fail-safe, etc.).

6.5 CPS/IoT Criteria

A key question is when a system can be labeled CPS, IoT, or both. The analyses described above suggest there are three criteria for addressing this question:

1) Does the system have one or more elements in each of the component categories: logical, physical, transducing, and human? (Note that the relevant capabilities of the human component vary with differing roles such as user, component, environmental factor, etc.)
2) Are these elements integrated to provide for transmission, transformation, and storage of energy for physical elements and information for logical elements; as well as input, processing, and output functions for transducing elements?
3) Does the system have one or more CPS/IoT functions where such a function is defined as involving the linkage of logical and physical system states?

If the answers to all three are 'yes' — in other words if the system has the components, capabilities, and functions of a CPS/IoT system — then it can be appropriately labeled 'CPS,' 'IoT,' and both.

A system missing one of the component categories, lacking transducing elements for example, is not a CPS or IoT instance. Thus, a shipping crate with an RFID tag is not in itself an IoT instance but becomes an IoT component when it interacts with a sensor to transmit information to a tracking system for processing in an active supply chain management system.

A system missing one of the component capabilities, lacking the transformation capability of a logical system for example, is not a CPS or IoT instance. Thus, a sensor network with a database storage system is not in itself a CPS or IoT instance but becomes a CPS/IoT component when coupled with processing capability for analysis and output.

A system being used solely for a non-CPS/IoT function is not a CPS or IoT instance. In the example of Section 4.3 above, a smart refrigerator with the full range of CPS/IoT components and capabilities that is only ever used strictly for keeping consumables cold and surfing the web is a refrigerator with an internet interface. While it has latent components and capabilities, it becomes a CPS/IoT system or component when the capabilities of the logical, physical, transducer and human components are integrated to enhance function (e.g., controlling appliance function in response to utility price signals to reduce energy costs).

Collectively, these criteria can be expressed as follows: Internet of Things and cyber-physical systems comprise interacting logical, physical, transducing, and human components engineered for function through integrated logic and physics.

7 Implications for Research, Development, and Standards

Two important implications arise from this unified CPS/IoT systems perspective. First, unified, new, hybrid discrete and continuous methods are needed to provide a sound science and engineering foundation for robust design, operation, and assurance of CPS, IoT, and CPS/IoT systems.

> *To understand the behavior of hybrid systems, to simulate, and to control these systems, theoretical advances, analyses, and numerical tools are needed* [69]
>
> *[I]t will not be sufficient to improve design processes, raise the level of abstraction, or verify (formally or otherwise) designs that are built on today's abstractions. To realize the full potential of CPS, we will have to rebuild computing and networking abstractions. These abstractions will have to embrace physical dynamics and computation in a unified way* [28]

Second, the concept of tight logical-physical linkage is at the heart of the transformational nature of CPS and IoT. The ability to use powerful computational systems to manage events in the physical world is dependent on the nature and quality of this linkage. The lack of robust sensing or actuating, insecure channels, poor digital models, coarse engineered-system responsiveness, and other limitations in functions for logical-physical linkage significantly constrain CPS and IoT capabilities.

Focusing research, development and standards efforts on addressing these implications – enabling tight physical and logical state linkage and developing hybrid methods – could catalyze progress and promote innovation. Additionally, with these new hybrid methods, there is benefit in identifying and leveraging symmetries between physical- and logical-state-focused mathematical formalisms, to gain insights from each perspective.

Progress in addressing these implications is important for all applications of these systems, ranging from legal, regulatory, and policy provisions to engineering, lifecycle management, and human perception. Two examples – design assurance and cyber-physical security – are provided below to illustrate the depth and breadth of these implications.

7.1 Design Assurance

Enabling effective design assurance for hybrid CPS/IoT systems will require evolving existing approaches embodied in standards such as the ISO 9000 family for quality assurance, ISO 15288 for systems engineering lifecycle management, and others. The Trustworthiness Aspect of NIST's CPS Framework [11] illustrates this point. This Aspect recognizes the interactions and interdependencies between ICT design provisions for cybersecurity and digital privacy with engineering requirements for safety, security, resilience, and reliability. Challenges that emerge from these interdependencies include the following [82]:

- *How can we mathematically prove timeliness, correctness, and other essential properties for systems that may be adaptive and even self-healing?*
- *How do we represent, reason about, and ensure the correctness of an inherently discrete system (the computer) that interacts with an inherently continuous system (the real world)?*
- *How can we expand the notion of trustworthiness to include system support aspects such as ensuring that a software defect doesn't drain the batteries of a critical component?*
- *How can we establish, reason about, and ensure trust between CPS components that are designed, installed, maintained, and operated by different organizations, and which may never have really been intended to work together?*
- *How can we make sure that when we use a new replacement part for an older component, the entire system won't come crashing down around us due to a subtle incompatibility?* [82]

New approaches to reasoning about CPS/IoT systems are being developed to manage these interdependencies for design assurance and other applications [83].

Another challenge for effective CPS/IoT design assurance lies in managing uncertainty for hybrid physical and logical systems.

> *Due to the interdisciplinary nature of CPS, we felt that it was difficult to precisely understand uncertainties. This is mainly because uncertainties not only exist in software, but also in hardware, communications, humans, and the interactions among them. Comprehending an*

> *uncertainty requires a wide range of knowledge across different disciplines. Particularly we observed that, based on our experience of collecting requirements from the industrial partners, a large number of uncertainties exist due to the mismatch between software and physical worlds.* [84]

While methods for expressing measurement uncertainty in physical systems are well documented [85], methods for measuring computational uncertainty [86] and for reliably combining the different methodologies into an integrated physical and logical uncertainty budget are subjects for ongoing research.

7.2 Cyber-Physical Security

Cybersecurity in CPS/IoT systems differs from that in conventional ICT-only systems in at least three categories: complex cybersecurity deployment landscapes, cyber-attacks on physical systems, and physical attacks on and physics-based mitigation for cyber systems.

First, the number and diversity of "things" being deployed in CPS/IoT systems present significant challenges [87]. Adding networked connectivity to everyday objects increases the number of points of attack that must be protected. Variation in computational capacity, system memory, networking bandwidth, physical access, upgradeability, and other factors among heterogeneous, connected CPS/IoT elements means any single cybersecurity approach may have limited application. Instead, tailored approaches with attention to security compositionality are required.

Second, the integration of logical and physical components means that an attack on IT systems can be used to gain control over critical physical systems for medical, critical infrastructure, life-safety, and other functions with the potential for causing damage, injury, or death [88]. For engineering design and assurance considerations, this also means that provisions for digital cybersecurity and privacy cannot be considered independent of provisions for system physical security, safety, resilience, and reliability. Instead, concerns related to all of these engineering goals must be considered as interdependent, with provisions for trade-offs and interactions evaluated in any comprehensive CPS/IoT design and assurance process [11].

Third, and most importantly, the physical components of networked CPS/IoT systems provide both new threat vectors and novel threat mitigation means. Examples of the former – threat vectors – include the use of background noise or ultrasound to attack audio interfaces of smart systems [89] or hidden features for backdoor attacks on image recognition [90].

Examples of the latter — novel mitigation means — include using information about the physical properties of a CPS/IoT system to provide insights into whether the logical state has been compromised by fault or attack. One example is the addition to a conventional cyber-intrusion detection approach of monitoring of logical system commands for instructions that would place the physical system in an unsafe state. Detecting such commands provides the basis for an alert of a fault in or attack on sensing or control systems. Such an approach has been labeled specification-based intrusion detection and relies on knowledge of the physics and engineering properties of the system in question.

> *When considering the ramifications of the potential for widespread damage to infrastructure and property, it becomes clear that both new and legacy* [CPS/IoT] *systems must be secured in a more robust and clearly understood manner. To address this problem, our solution closely*

> *integrates the cybersecurity components with control commands, physical constraints, and safety constraints of physical devices to mitigate a substantial class of vulnerabilities in cyber-physical systems … By leveraging an understanding of the physical limitations of cyber-physical systems under control as well as the protocols used to monitor and send commands to such devices, specification-based intrusion detection can be used to monitor a cyber-physical system to verify that it operates according to the specifications of the networked physical system being controlled* [91]

A similar approach has been described for monitoring of code bound for a programmable logic controller (PLC) for evidence of malware that would put the system in an unsafe state.

> *Our proposed solution crosses the boundary between infrastructural security and safety research. In particular, our solution makes sure that the PLC code won't violate the underlying physical plant's safety requirements; thus, it could also act as a cyber-physical security intrusion detection engine through identification of malicious PLC code injection attempts* [92]

A related class of physics-based mitigation is the use of multiple, distributed sensor inputs to identify state estimation discrepancies as indicators of faulty or malicious data inputs.

> *By combining the knowledge of secure measurements and power system specific measurement models, an unconventional measurement residual can be obtained to achieve data attack isolation in addition to the standard BDD (bad data detection methods)* [93]

> *Smart grid systems have a unique advantage in the detection of falsified state attacks because process control decisions have an observable effect on a shared physical infrastructure. The physical infrastructure acts as a high-integrity message channel that broadcasts changes in individual process states. This work proposes a new distributed security mechanism called physical attestation that combines physical feedback with methods from computer security to detect state fabrications in the smart grid* [94]

Additional examples especially relevant to CPS/IoT systems include cybersecurity approaches that can accommodate the continuing evolution of operating systems, threat environments, and IT capabilities for long-lifecycle CPS/IoT systems with components expected to be deployed for decades; cybersecurity in systems that must operate in physical rather than logical time; resilience including fail-safe/fail-operational provisions, and authentication solutions that operate at the speed and scale required for massive numbers of interacting CPS/IoT systems.

Collectively, these examples illustrate the opportunities for using physics-based and engineering-grounded methods for improved cybersecurity in CPS/IoT systems; an approach that might be labeled "better cybersecurity through physics."

8 Conclusions

In summary, the analyses described in this document lead to six major conclusions.

(1) The definitions of CPS and IoT are converging over time to include a common emphasis on hybrid systems of interacting digital, analog, physical, and human components in systems engineered for function through integrated physics and logic.

(2) Recognizing this convergence can bring currently isolated fields and sectors together for progress around shared research, application, and innovation goals and opportunities.

(3) Effectively designing, building, and assuring CPS/IoT systems requires consideration of the system's functional context, including how the system is used and for what purpose or outcome.

(4) A unified perspective on CPS/IoT systems allows a common classification structure for components, illuminating a path forward for enabling open composablity and reliable compositionality for innovation in the creation of novel systems and systems-of-systems applications.

(5) This unified perspective also allows for prioritizing research, development, and deployment goals, including enabling tight physical and logical state linkages and developing hybrid discrete and continuous methods for conceptualization, realization, and assurance of CPS/IoT systems.

(6) The hybrid nature of CPS/IoT systems has important implications for engineering, including design assurance, cyber-physical security, lifecycle management, timing and synchronization, and more.

Collectively, these conclusions can inform research; commercial; standards; and legal, policy, and regulatory efforts designed to realize the value to society of advanced CPS/IoT technologies.

9 References

1. Rajkumar R, Lee I, Sha L, Stankovic J (2010) Cyber-Physical Systems: The Next Computing Revolution. *Proceedings of the 47th Design Automation Conference* (IEE, Anaheim, CA), pp 731–736. https://ieeexplore.ieee.org/document/5523280
2. Kim KD, Kumar PR (2012) Cyber–Physical Systems: A Perspective at the Centennial. *Proceedings of the IEEE* 100 (Special Centennial Issue): 1287. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6176187.
3. Sanislav T, Miclea L (2012) Cyber-Physical Systems -Concept, Challenges and Research Areas. *Journal* of *Control Engineering* and *Applied Informatics* 14 (2): 28–33. http://www.ceai.srait.ro/index.php?journal=ceai&page=article&op=view&path%5B%5D=1292
4. Horvath I, Gerritsen B (2012) Cyber-Physical Systems: Concepts, Technologies and Implementation Principles. *Proceedings of the Tools and Methods of Competitive Engineering* (Delft Faculty of Industrial Design Engineering, Delft University of Technology, Karlsruhe, Germany), pp. 7–11. https://www.researchgate.net/publication/229441298_CYBER-PHYSICAL_SYSTEMS_CONCEPTS_TECHNOLOGIES_AND_IMPLEMENTATION_PRINCIPLE
5. Steering Committee for Foundations for Innovation in Cyber-Physical Systems (2013) Strategic R&D Opportunities for 21st Century Cyber-Physical Systems: Connecting computer and information systems with the physical world. (National Institute of Standards and Technology, Gaithersburg, MD). http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf
6. National Institute of Standards and Technology (2013) Foundations for Innovation in Cyber-Physical Systems Workshop Summary Report. (Prepared by Energetics Incorporated Columbia, Maryland). https://www.nist.gov/sites/default/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf
7. Executive Roundtable on Cyber-Physical Systems (2013) Strategic Vision and Business Drivers for 21st Century Cyber-Physical Systems. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/sites/default/files/documents/el/Exec-Roundtable-SumReport-Final-1-30-13.pdf
8. Wan J, Chen M, Xia F, Di L, Zhou K (2013) From Machine-to-Machine Communications towards Cyber-Physical Systems. *Computer Science and Information Systems* 10 (3): 1105–1128. http://www.comsis.org/archive.php?show=ppr426-1203
9. Gunes JV, Peter S, Givargis T, Vahid F (2014) A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. *Transactions on Internet and Information Systems* 8 (12): 4242–4268. http://www.itiis.org/digital-library/manuscript/894
10. Bordel B, Alcarria R, Robles T, Martin D (2017) Cyber-Physical Systems: Extending Pervasive Sensing from Control Theory to the Internet of Things. *Pervasive and Mobile Computing* 40: 156–184. https://www.sciencedirect.com/science/article/pii/S1574119217303127?via%3Dihub
11. Griffor E, Greer C, Wollman D, Burns M (2017) Framework for Cyber-Physical Systems Volume 1, Overview. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201
12. Atzori L, Lera A, Morabito G (2010) The Internet of Things: A Survey. *Computer Networks* 54 (15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
13. Koreshoff T, Robertson T, Leong T (2013) Internet of Things: A Review of Literature and Products. *OzCHI '13 Proceedings of the 25th Australian Computer-Human Interaction*

Conference: Augmentation, Application, Innovation, Collaboration, (ACM, Adelaide, Australia) pp 335-344 http://doi.org/10.1145/2541016.2541048

14. Li S, Xu L, Zhao S (2015) The Internet of Things: A Survey. *Information Systems Frontiers* 17: 243. https://doi.org/10.1007/s10796-014-9492-7
15. Whitmore A, Agarwal A, Xu L (2015) The Internet of Things - A survey of Topics and Trends. *Information Systems Frontiers* 17 (2): 261-274. https://link.springer.com/article/10.1007/s10796-014-9489-2
16. Woodside, A, Sood, S (2017) Vignettes in the two-step arrival of the internet of things and its reshaping of marketing management's service-dominant logic, *Journal of Marketing Management* 33:1-2, 98-110, DOI: 10.1080/0267257X.2016.1246748
17. CPS Virtual Organization (2018) *NSF Workshop on Cyber-Physical Systems, October 16-17, 2006, Austin, Texas*, Available at https://cps-vo.org/node/179
18. Krogh, B, Ilic M, Sastry S (2007) National Workshop on Beyond SCADA: Networked Embedded Control for Cyber-Physical Systems (NE4CPS): Research Strategies and Roadmap. Available at https://cps-vo.org/NEC4CPS-report
19. President's Council of Advisors on Science and Technology (2007) *Leadership Under Challenge: Information Technology R&D in a Competitive World* (Executive Office of The President, Washington, DC). https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-07-nitrd-review.pdf
20. National Science Foundation (2007) *Computer Systems Research, NSF Program Solicitation 07-504* https://www.nsf.gov/pubs/2007/nsf07504/nsf07504.htm
21. Lee E (2006) Cyber-Physical Systems - Are Computing Foundations Adequate? Position Paper. *NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, (Austin TX). https://ptolemy.berkeley.edu/publications/papers/06/CPSPositionPaper/Lee_CPS_PositionPaper.pdf
22. IEEE Technical Committee on Cyber-Physical Systems (2018) *Cyber Physical Systems Technical Committee*. Available at https://www.ieeesystemscouncil.org/pages/cyber-physical-systems-technical-committee.
23. Lee E (2010) CPS Foundations. *DAC '10 Proceedings of the 47th Design Automation Conference*, (ACM, Anaheim, California), pp 737-742. https://dl.acm.org/citation.cfm?doid=1837274.1837462
24. Shi J, Wan J, Yan H, Suo H (2011) Survey of Cyber-Physical Systems. *2011 International Conference on Wireless Communications and Signal Processing,* (IEEE, Nanjing, China), https://ieeexplore.ieee.org/document/6096958
25. Cardenas A, Amin S, Sastry S (2008) Secure Control: Towards Survivable Cyber-Physical Systems. *The 28th International Conference on Distributed Computing Systems Workshops,* (IEEE, Beijing, China). https://ieeexplore.ieee.org/document/4577833
26. Tan Y, Vuran M, Goddard S (2009) Spatio-Temporal Event Model for Cyber-Physical Systems. *29th IEEE International Conference on Distributed Computing Systems Workshops*, (IEEE Montreal, QC, Canada). https://ieeexplore.ieee.org/document/5158832
27. Tidwell T, Gill C (2018) Abstract Interpretation of Time for Preemptive Scheduling of Cyber-Physical Systems. *Semantic Scholar.*

https://pdfs.semanticscholar.org/a44c/72cb679b6b9074a1b081d3ff3a203d1058f1.pdf (accessed August 2018)

28. Lee E (2008) Cyber Physical Systems: Design Challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, 1, p. 363-369. http://doi.ieeecomputersociety.org/10.1109/ISORC.2008.25

29. *Networking and Information Technology Research and Development,* Cyber-Physical System Interagency Working Group (2015) CPS Vision Statement, working document, p. 2. https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf (accessed August 2018)

30. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the Internet of Things (IoT). IEEE. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

31. Ashton K (2009) That 'Internet of Things' Thing. *RFID Journal.* https://www.rfidjournal.com/articles/view?4986

32. Sarma S, Brock D, Ashton (2000) White Paper: The Networked Physical World: Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification. MIT Auto-ID Center (Cambridge, MA). http://cocoa.ethz.ch/downloads/2014/06/None_MIT-AUTOID-WH-001.pdf (accessed August 2018)

33. Ibarra-Esquer J, González-Navarro F, Flores-Rios B, Burtseva L, Astorga-Vargas M (2017) Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. *Sensors*. Sun Y, Cai Z, Jara A, eds. 17(6): 1379. https://www.mdpi.com/1424-8220/17/6/1379 or http://www.doi.org/10.3390/s17061379

34. Gartner (2011) Press Release*:* Gartner's 2011 Hype Cycle Special Report Evaluates the Maturity of 1,900 Technologies. Available at https://www.gartner.com/newsroom/id/1763814.

35. Gartner (2016) Press Release: Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage. Available at https://www.gartner.com/newsroom/id/3412017.

36. Guth J, Breitenbucher U, Flkenthal M, Leymann F, Reinfurt L (2016) Comparison of IoT Platform Architectures: A Field Study Based on a Reference Architecture. *Cloudification of the Internet of Things (CIoT)*, (IEEE, Paris, France), pp 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7872918&isnumber=7872907

37. Traversat B, Abdelaziz M, Doolin D, Duigou M, Hugly J, Pouyoul E (2003) Project JXTA-C: Enabling a Web of Things. *36th Annual Hawaii International Conference on System Sciences*, (IEEE, Big Island, HI). https://doi.org/10.1109/HICSS.2003.1174816

38. International Telecommunications Union (2005) Internet Reports 2005: The Internet of Things. (International Telecommunications Union, Geneva, Switzerland).
http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf (accessed August 2018)

39. Kopetz H (2011) Internet of Things. *Real-Time Systems Series*, (Springer, Boston, MA), 307-323. https://doi.org/10.1007/978-1-4419-8237-7_13

40. Kiritsis D (2010) Closed-loop PLM for Intelligent Products in the Era of the Internet of Things. *Computer-Aided Design*, 43 (5): 479-501. https://doi.org/10.1016/j.cad.2010.03.002

41. Evans P, Annunziata M (2012) Industrial Internet: Pushing the Boundaries of Minds and Machines. (General Electric). https://www.ge.com/docs/chapters/Industrial_Internet.pdf

42. Jasperneite J (2012) Was hinter Begriffen wie Industrie 4.0 steckt. *Computer-Automation.de.* Available at https://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/0/.
43. Borgia E (2014) The Internet of Things Vision: Key features, Applications and Open Issues, *Computer Communications*, 54 (1): 1-31. https://doi.org/10.1016/j.comcom.2014.09.008
44. Hurlburt G(2018) The Internet of Things ... All Things. *XRDS: Crossroads, The ACM Magazine for Students*, 22 (2): 22-26. https://dl.acm.org/citation.cfm?id=2845143 (accessed August 2018)
45. Ranger S (2018) What is the IoT? Everything You Need to Know about the Internet of Things Right Now. *ZDNet*. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (accessed August 2018).
46. Miorandi D, Sicari S, Pellegrini F, Chlamta I (2012) Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks* 10 (7): 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016
47. Ma H (2011) Internet of tThings: Objectives and Scientific Challenges. *Journal of Computer Science and Technology* 26 (6): 919–924. https://doi.org/10.1007/s11390-011-1189-5
48. Schatz B, Torngren M, Bensalem S, Cengarle M, Pfeifer H, McDermid J, Passerone R, Sangiovanni-Vincentelli A (2014) CyPhERS – Cyber-Physical European Roadmap & Strategy: Research Agenda and Recommendations for Action. (CyPhERS project, co-funded through the European Union's Framework Programme). http://cyphers.eu/sites/default/files/d6.1+2-report.pdf. (accessed August 2018)
49. Yeboah-ofori A, Abdulai J, Katsriku F (2018) Cybercrime and Risks for Cyber Physical Systems: A Review. *Preprints 2018.* https://doi.org/10.20944/preprints201804.0066.v1
50. Acatech (2011)Position Paper: Cyber-Physical Systems Driving Force for Innovation in Mobility, Health, Energy and Production. (National Academy of Science and Engineering, Munich, Germany) https://www.acatech.de/wp-content/uploads/2018/03/acatech_POSITION_CPS_Englisch_WEB-1.pdf (accessed August 2018)
51. PICASSO Opportunity Report (2017) Towards Enhanced EU-US ICT Pre-Competitive Collaboration (European Union's Horizon 2020 Research and Innovation Programme funded PICASSO). http://www.picasso-project.eu/wp-content/uploads/2017/03/PICASSO-Opportunity-Report_March-2017_revMar19.pdf (accessed August 2018)
52. Stojmenovic I, Zhang F (2015) Forward: Inaugural issue of '*cyber-physical systems*'. *Cyber-Physical Systems* 1 (1): 1-4. http://dx.doi.org/10.1080/23335777.2015.970764
53. Cyber-Physical Systems - Virtual Organizations (2018) *Internet of Things & Cyber-Physical Systems.* Available at https://cps-vo.org/group/iot .
54. Mattern F, Floerkemeier C (2010) From the Internet of Computers to the Internet of Things. *Active Data Management to Event-Based Systems and More* 6462: 242-259. https://link.springer.com/chapter/10.1007/978-3-642-17226-7_15#citeas
55. Recommendations ITU-T Y.2060 (2012) Overview of the Internet of Things. *Unleashing the Potential of the Internet of Things 2016* (International Telecommunication Union) p. 8 https://www.itu.int/en/publications/Documents/tsb/2016-InternetOfThings/mobile/index.html#p=22
56. Friess P, Ibanez F (2014) Putting the Internet of Things Forward to the Next Level. *Internet of Things – From Research Innovation to Market Deployment 2018,* eds Vermesan O, Friess P,

(Aalborg, Denmark, River Publishers) pp 3-6. https://docplayer.net/386191-Internet-of-things-from-research-and-innovation-to-market-deployment.html

57. Shang W, Bannis A, Liang T, Wang Z, Yu Y, Afanasyev A, Thompson J, Burke J, Zhang B, Zhang L (2016) Named Data Networking of Things. *2016 IEEE First International Conference on Internet-of-Things Design and Implementation,* (IEEE, Berlin, Germany). https://doi.org/10.1109/IoTDI.2015.44
58. Hatch Smart Manufacturing (2018) Overview of USSD (Unstructured Supplementary Service Data) for IOT. Available at http://www.hatchmfg.com/overview-of-ussd-for-iot/
59. Baheti R, Gill, H (2011) Cyber-physical Systems. *The Impact of Control Technology 2011*, eds Samad T, Annaswamy (IEEE Control Systems Society). http://www.ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf
60. Rose K, Eldridge S, Chapin L (2015) The Internet of Things: An Overview. (The Internet Society, Reston, VA) https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (accessed August 2018)
61. van Lier B (2011) Connections, Information and Reality: Thinking about the Internet of Things. *The 15th World Multi-Conference on Systemics, Cybernetics and Informatics*, (World Multi-Conference on Systemics, Cybernetics and Informatics Orlando, FL) . https://pdfs.semanticscholar.org/2a5e/841d7d27c7ac72767538b7c0e96b7bba32b7.pdf?_ga=2.244722117.112273469.1541264016-1477856370.1541113161&_gac=1.183708116.1541113237.CjwKCAjwyOreBRAYEiwAR2mSkowwTnqiSZXNJjGKH5lnaa-ZbMeETa0YTqfhDW4BfQDc-Pw3fpNuLBoCk3IQAvD_BwE
62. National Science Foundation (2018) *Cyber-Physical Systems (CPS)*. Available at https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286
63. Woodside A, Sood S (2016) Vignettes in the Two-Step Arrival of the Internet of Things and Its Reshaping of Marketing Management's Service-Dominant Logic. *Journal of Marketing Management*, 33 (1-2): 98-110.
64. Pratt D, Ragusa L, von der Lippe (1999) Composability as an Architecture Driver. *Proceedings of the 1999 Interservice/Industry Training, Simulation and Education Conference*, (National Training Systems Association, Orlando FL). http://www.dtic.mil/dtic/tr/fulltext/u2/a373368.pdf (abstract on p. 96)
65. de Roever W**,** Langmaack H, Pnueli A, Eds. (1998) *Compositionality: The Significant Difference*. Papers from the *International Symposium on Compositionality COMPOS'97* (Springer-Verlag Berlin Heidelberg). https://www.springer.com/us/book/9783540654933
66. Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) The Internet of Things: Mapping the Value Beyond the Hype (McKinsey & Company) https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx
67. IEEE (1991) 610-1990 - IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries (Withdrawn Inactive Date: 20-4-2001) Available at https://ieeexplore.ieee.org/document/182763
68. McClelland D, Rumelhart J (1986) *Parallel Distributed Processing* (The MIT Press, A Bradford Book, Cambridge, MA), twelfth printing, 1999.

https://academiaanalitica.files.wordpress.com/2016/11/david-e-rumelhart-james-l-mcclelland-pdp-research-group-parallel-distributed-processing_-explorations-in-the-microstructure-of-cognition_-foundations-vol-11986.pdf

69. Tomlin C, Mitchell I, Bayen A, Oishi M (2003) Computational Techniques for the Verification of Hybrid Systems. Proceedings of the IEEE 91 (7): 986-1001. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1215682
70. U.S. Access Board (2010) Draft Information and Communication Technology (ICT) Standards and Guidelines (U.S. Access Board, Washington, DC). https://www.access-board.gov/attachments/article/560/draft-rule2010.pdf
71. Gagnon M, Légaré F, Labrecque M, Fremont P, Pluye P, Gagnon J, Car J, Pagliari C, Desmartis M, Turcot L, Gravel K (2009) Interventions for promoting information and communication technologies adoption in healthcare professionals. *Cochrane database of systematic reviews*. https://www.ncbi.nlm.nih.gov/pubmed/19160265
72. Hoppe A, Seising R, Nürnberger A, Wenzel C (2011) Wisdom - the blurry top of human cognition in the DIKW-model? *7th conference of the European Society for Fuzzy Logic and Technology,* (The Atlantis Press, Aix-les-Bains, France). https://www.atlantis-press.com/php/download_paper.php?id=2276
73. Ackoff, R (1989). From data to wisdom. *Journal of Applied Systems Analysis* 16: 3–9. http://faculty.ung.edu/kmelton/documents/datawisdom.pdf
74. Queensland Government Chief Information Office (2018) *ICT system (Definition*). Available at https://www.qgcio.qld.gov.au/publications/qgcio-glossary/ict-system-definition
75. United Nations Educational, Scientific and Cultural Organization (2002) Information and Communication Technology in Education: A Curriculum for Schools and Programme of Teacher Development. (UNESCO, Paris, France). http://unesdoc.unesco.org/images/0012/001295/129538e.pdf
76. ISO (2018) *35.100 - Open systems interconnection (OSI)* . Available at https://www.iso.org/ics/35.100/x/.
77. National Research Council (1995) Expanding the Vision of Sensor Materials. (National Academy Press, Washington, D.C.). https://www.nap.edu/read/4782/chapter/1
78. *Pallás-Areny R, Webster J (*2001) *Sensors and Signal Conditioning* (John Wiley & Sons, New York, NY) 2nd Edition. http://192.168.1.1:8181/http://ebooks.bharathuniv.ac.in/gdlc2/gdlc2/SecondYear/SecondSem/EIE/Sensors%20and%20Signal%20Conditioning/e%20books/Sensor%20And%20Signal%20Conditioning%20-%202ed%20-%20Ramon%20Pall%C3%83%C2%A0s-Areny.pdf
79. Electronics Tutorial (2018) *Sensors and Transducers*. Available at https://www.electronics-tutorials.ws/io/io_1.html
80. Merriam-Webster (2018) *actuator*. Available at https://www.merriam-webster.com/dictionary/actuator
81. Song EY, FitzPatrick GJ, Lee KB (2017) Smart Sensors and Standard-Based Interoperability in Smart Grids. IEEE Sensors Journal 17(23): 7723-7730. https://ieeexplore.ieee.org/abstract/document/7986956
82. Romanovsky A, Ishikawa F, Eds., (2017) *Trustworthy Cyber-Physical Systems Engineering* (CRC Press Taylor & Francis Group, Boca Raton, FL). https://universalflowuniversity.com/Books/Computer%20Programming/Security%20and%20Cyber%20Warfare/Trustworthy%20Cyber-Physical%20Systems%20Engineering.pdf

83. Balduccini M, Griffor E, Huth M, Vishik C, Burns M, Wollman D (2018) Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems. *IET PETRAS 2018 Conference*, (IET, London, UK). https://arxiv.org/pdf/1803.07438.pdf
84. Zhang M, Selic B, Ali S, Yue T, Okariz O, Norgren R (2016) Understanding Uncertainty in Cyber-Physical Systems: A Conceptual Model. *Modelling Foundations and Applications* eds Wąsowski A, Lönn H. ECMFA: European Conference on Modelling Foundations and Applications. (Springer International Publishing, Vienna, Austria), pp 247-264. https://link.springer.com/chapter/10.1007%2F978-3-319-42061-5_16#citeas
85. ISO (2018) *ISO/IEC Guide 98-3:2008 (JCGM/WG1/100) Uncertainty of measurement -- Part 3: Guide to the expression of Uncertainty in Measurement (GUM:1995).* Available at https://www.iso.org/standard/50461.html
86. Dienstfrey A, Boisvert R, Eds., (2011) Uncertainty Quantification in Scientific Computing. *10th IFIP WG 2.5 Working Conference* (Springer, Boulder, CO). https://www.springer.com/us/book/9783642326769
87. Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, O'Rourke D, Piccarreta B, Scarfone K (2018) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), *Draft NISTIR 8228.* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf
88. Humayed A, Lin J, Li F, Luo B (2017) Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things (IoT) Journal* 4 (6): 1802-1831. https://ieeexplore.ieee.org/document/7924372
89. Alznatot M, Balaji B, Srivastava M, (2018) Did You Hear That? Adversarial Examples Against Automatic Speech Recognition. *31st Conference on Neural Information Processing Systems,* (NIPS, Long Beach, CA). https://arxiv.org/pdf/1801.00554.pdf
90. Gu T, Doan-Gavitt B, Garg S (2017) BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. https://arxiv.org/pdf/1708.06733.pdf
91. McParland C, Peisert S, Scaglione A (2014) Monitoring Security of Networked Control Systems: It's the Physics. *IEEE Security & Privacy*, 12 (6): 32-9. https://escholarship.org/uc/item/8f8738wd
92. Zounoz S, Rrushi J, McLaughlin S (2014) Detecting Industrial Control Malware Using Automated PLC Code Analytics. *IEEE Security & Privacy* 12 (6): 40-47. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7006408
93. Sou K, Sandberg H, Johansson K (2014) Data Attack Isolation in Power Networks Using Secure Voltage Magnitude Measurements. *IEEE Transactions on Smart Grid* 5 (1): 14-28. https://ieeexplore.ieee.org/abstract/document/6693798
94. Roth T, McMillin B (2018) Physical Attestation in the Smart Grid for Distributed State Verification. *IEEE Transactions on Dependable and Secure Computing*, 15 (2): 275-288. https://ieeexplore.ieee.org/document/7485817

10 Appendix A – Examples of CPS Definitions

2006: Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. In the physical world, the passage of time is inexorable and concurrency is intrinsic. Neither of these properties is present in today's computing and networking abstractions. Edward A. Lee, Cyber-Physical Systems - Are Computing Foundations Adequate? Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap. Austin TX, 2006 https://ptolemy.berkeley.edu/publications/papers/06/CPSPositionPaper/Lee_CPS_PositionPaper.pdf (accessed August 2018)

2007: NIT systems connected with the physical world – also called embedded, engineered, or cyber-physical systems – are essential to the effective operation of U.S. defense and intelligence systems and critical infrastructures (e.g., air-traffic-control, power-grid, and water-supply systems). Cyber-physical systems are also at the core of human-scale structures such as vehicles and clinical and home health-care devices as well as large-scale civilian applications such as environmental monitoring, industrial process control, and ground transportation management. These NIT systems, in which computing and networking are deeply integrated into other engineered systems, are connected to the physical world through sensors and actuators to perform crucial monitoring and control functions safely and dependably. President's Council of Advisors on Science and Technology, Leadership Under Challenge: Information Technology R&D in a Competitive World; 2007 https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-07-nitrd-review.pdf (accessed August 2018)

2008: Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed by a set of networked agents, including: sensors, actuators, control processing units, and communication devices. Alvaro A. Cardenas, Saurabh Amin, Shankar Sastry; The 28th International Conference on Distributed Computing Systems Workshops, IEEE Xplore, DOI: 10.1109/ICDCS.Workshops.2008.40

2008: These concerns are of particular importance in cyberphysical systems in which computation and communication timing and event semantics are interdependent with physical timing and event semantics. Terry Tidwell and Christopher Gill, Abstract Interpretation of Time for Preemptive Scheduling of Cyber-Physical Systems, Semantic Scholar, https://pdfs.semanticscholar.org/a44c/72cb679b6b9074a1b081d3ff3a203d1058f1.pdf (accessed August 2018).

2008: Cyber-Physical Systems (CPS) are large-scale interconnected systems of heterogeneous components that are envisioned to provide integration of computation with physical processes [1] Yunbo Wang, Mehmet C. Vuran, Steve Goddard Cyber-physical Systems in Industrial Process Control, ACM SIGBED Review - Special issue on the RTSS forum on deeply embedded real-time computing Homepage archive, Volume 5 Issue 1, January 2008, Article No. 12

2008: 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. From Vision to Reality: Cyber-Physical Systems Helen Gill, Ph.D. CISE/CNS National Science Foundation Co-Chair, NITRD High Confidence Software and Systems Coordinating Group HCSS National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive, Aviation, and Rail November 18-20, 2008, URL: https://www2.ee.washington.edu/research/nsl/aar-cps/Gill_HCSS_Transportation_Cyber-Physical_Systems_2008.pdf (accessed August, 2018)

2008: The integration of physical systems and processes with networked computing has led to the emergence of a new generation of engineered systems: Cyber-Physical Systems (CPS). Such systems use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. Cyber-Physical Systems. CPS Steering Group of the Networking and Information Technology Research and Development Program (NITRD), 2008, http://iccps.acm.org/2011/_doc/CPS-Executive-Summary.pdf (accessed August, 2018)

2008: Cyber-Physical Systems (CPS) are integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa … There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general-purpose computing. Moreover, physical components are qualitatively different from object-oriented software components. Edward A Lee, 2008, 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC)DOI 10.1109/ISORC.2008.25

2008: Cyber-Physical Systems are a next-generation network-connected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws. Here, cyber systems are collections of control logic and sensor units, while physical systems are collections of actuator units. Ying Tan, Steve Goddard, and Lance C. Pérez. 2008. A prototype architecture for cyber-physical systems. SIGBED Rev. 5, 1, Article 26, DOI=http://dx.doi.org/10.1145/1366283.1366309 (accessed August 2018)

2009: Cyber-Physical Systems (CPSs) are integrations of computation, communication, and control with the physical world. More specifically, a CPS is envisioned to be a heterogeneous system of systems, which consists of computing devices and embedded systems including distributed sensors and actuators. These components are inter-connected together in a large-scale and execute autonomous tasks to link the cyber world and the physical world. Tan, M. C. Vuran and S. Goddard, "Spatio-Temporal Event Model for Cyber-Physical Systems," *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal, QC, 2009, pp. 44-50. doi: 10.1109/ICDCSW.2009.82 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5158832&isnumber=5158801

2009: The emerging cyber-physical systems (CPSs) are envisioned to integrate computation, communication and control with the physical world. Therefore, CPS requires close-interactions between the cyber and physical worlds both in time and space. These interactions are usually governed by events, which occur in the physical world and should autonomously be reflected in the cyber-world, and actions, which are taken by the CPS as a result of detection of events and certain decision mechanisms. Ying Tan; Mehmet C. Vuran ; Steve Goddard, 2009, 29th IEEE International Conference on Distributed Computing Systems Workshops, IEEE Xplore DOI: 10.1109/ICDCSW.2009.82

2010: Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. R. Rajkumar, I. Lee, L. Sha and J. Stankovic, "Cyber-physical systems: The next computing revolution," *Design Automation Conference*, Anaheim, CA, 2010, pp. 731-736. doi: 10.1145/1837274.1837461
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5523280&isnumber=5522347
(accessed August 2018)

2010: CPS is about the intersection, not the union, of the physical and the cyber. In the physical world, a central property of a system is its dynamics, the evolution of its state over time. In the cyber world, dynamics is reduced to sequences of state changes without temporal semantics. The intellectual heart of CPS is in studying the joint dynamics of physical processes, software, and networks. Edward A. Lee, CPS Foundations. DAC '10 Proceedings of the 47th Design Automation Conference Pages 737-742, ACM, 2010, doi: 10.1145/1837274.1837462 https://dl.acm.org/citation.cfm?doid=1837274.1837462

2010: Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, Cyber-physical systems: The next computing revolution,2010, in Proc. 47th Design Autom. Conf., pp. 731–736.
https://www.cs.virginia.edu/~stankovic/psfiles/Rajkumar-DAC2010-Final.pdf (accessed August 2018).

2010: Cyber-physical system (CPS) is a promising new class of systems that deeply embed cyber capabilities in the physical world, either on humans, infrastructure or platforms, to transform interactions with the physical world. Advances in the cyber world such as communications, networking, sensing, computing, storage, and control, as well as in the physical world such as materials, hardware, and renewable "green" fuels, are all rapidly converging to realize this class of highly collaborative computational systems that are reliant on sensors and actuators to monitor and effect change.Tomorrow's CPS is expected to enrich cyber-physical interactions by intimately coupling assets and dynamics of the physical and engineered systems with the computing and communications of cyber systems, at grand scales and depths from nanosystems to geographically dispersed systems-of-systems. Radha Poovendran, Cyber–Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View]" in Proceedings of the IEEE, vol. 98, no. 8, pp. 1363-1366, http://doi.org/10.1109/JPROC.2010.2050377

2011: Cyber-Physical Systems (CPSs) integrate the dynamics of the physical processes with those of the software and communication, providing abstractions and modeling, design, and analysis techniques for the integrated whole. The dynamics among computers, networking, and physical systems interact in ways that require fundamentally new design technologies. Jianhua Shi Jiafu Wan Hehua Yan, Hui Suo Survey of Cyber-Physical Systems. In Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November 9-11, 2011
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.4496&rep=rep1&type=pdf

2011: The term cyber-physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control is a key enabler for future technology developments. IEEE Control Systems

Society Pages 1-6 The Impact of Control Technology: Cyber-physical Systems, Baheti, R., Gill, H. 2011 http://www.ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf

2012: CPS is an integration of computation with physical processes, is about the intersection, not the union of the physical and the cyber. Also, a complex CPSs definition was given by Shankar Sastry from University of California, Berkeley in 2008: "A cyber-physical system (CPS) integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safety, securely, efficiently and real-time". CPSs are not: the traditional embedded systems or the realtime systems, the today's sensor networks and only desktop applications, but they have certain characteristics that define them, as mentioned in Huang (2008) and presented below: (1) Cyber capabilities in every physical component; (2) Networked at multiple and extreme scale; (3) Dynamically reconfiguring/reorganizing; (4) High degrees of automation, the control loops must close; (5) Operation must be dependable and certified in some cases; (6) Cyber and physical components are integrated for learning and adaptation, higher performance, self-organization, autoassembly. Teodora Sanislav, Liviu Miclea CEAI, 2012, Vol.14, No.2, pp. 28-33 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.8858&rep=rep1&type=pdf

2013: Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. This makes smart systems possible but also creates the need for a new ‘systems science’ that can lead to unprecedented capabilities. Tightly coupled cyber and physical systems that exhibit this level of integrated intelligence are sometimes referred to as cyber-physical systems (CPS). All CPS have computational processes that interact with physical components. Strategic R&D Opportunities for 21st Century Cyber-Physical Systems: Connecting computer and information systems with the physical world, Jan. 2013. http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf

2013: Cyber-physical systems (CPS) can be described as smart systems that encompass computational (i.e., hardware and software) and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world. These systems involve a high degree of complexity at numerous spatial and temporal scales and highly networked communications integrating computational and physical components. Foundations for Innovation in Cyber-Physical Systems Workshop Summary Report, Foundations for Innovation in Cyber-Physical Systems Workshop Summary Report, https://www.nist.gov/sites/default/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf

2013: Systems that integrate the cyber world with the physical world are often referred to as cyberphysical systems (CPS). The computational and physical components of such systems are tightly interconnected and coordinated to work effectively together, sometimes with humans in the loop. NIST, Strategic vision and business drivers for 21st century cyber-physical systems, Report from the Executive Roundtable on Cyber-physical Systems (2013), https://www.nist.gov/sites/default/files/documents/el/Exec-Roundtable-SumReport-Final-1-30-13.pdf

2014: The role played by devices is no longer limited to connect users to the Internet, but it has been expanding becoming an opportunity to interlink the physical world with the cyber world [1], leading to the emergence of Cyber-Physical Systems (CPS). The notion of CPS refers to a next generation of embedded ICT systems where computation and networking are integrated with physical processes and they control and manage their dynamics and make them more efficient, reliable, adaptable and secure. Information about physical processes, for example gathered through sensors, are transferred, processed, and used in the digital world, but they may also affect physical processes through feedback loops, for example by using actuators. The peculiarity of CPS is that the ICT system is designed together with the physical components to maximize the overall efficiency, thus being in contrast with classic embedded systems where the goal is to include electronics/computing/communication/abstraction in an already operating physical world. Eleonora Borgia, The Internet of Things vision: Key features, applications and open issues, Computer Communications, Volume 54, Pages 1-31, https://doi.org/10.1016/j.comcom.2014.09.008

2015: Cyber Physical Systems (CPS) are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behavior of the "cyber" and "physical" elements of the system is critical - computing, control, sensing and networking can be deeply integrated into every component, and the actions of components and systems must be safe and interoperable. NITRD CPS Interagency W. Group (IWG). CPS Vision Statement. 2015. Working Document. https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf (accessed August 2018).

2015: Main features of Cyber-Physical Systems are therefore the automated integration of physical and digital components, the enclosing monitoring of the physical reality through sensors, and the possibility to act upon this reality through actuators. Furthermore, the embedded processing of information and data, as well as capabilities of autonomous decision making and control, are essential functions. Finally, Cyber-Physical Systems should contain the technical capabilities to communicate and coordinate with each other, as well as with associated information systems and with human authorities, and to respond dynamically and intelligently to changes within the physical world thereby improving their abilities, experience and knowledge (networks). Christoph Klotzer and Alexander Pflaum, Cyber-Physical Systems (CPS) in Supply Chain Management – A definitional approach; Article 13 in NOFOMA 2015 Post Conference Proceedings, http://hdl.handle.net/11250/2359479, or https://brage.bibsys.no/xmlui/handle/11250/2359479

2016: Cyber-physical systems (CPS) are "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components." CPS can be small and closed, such as an artificial pancreas, or very large, complex, and interconnected, such as a regional energy grid. CPS engineering focuses on managing inter- dependencies and impact of physical aspects on cyber aspects, and vice versa … CPS bridges engineering and physical world applications and the computer engineering hardware and computer science cyber worlds. Basic principles of the physical world include physics, mathematical modeling, analysis, and algorithm and systems design and deal with their associated uncertainty and risk. Principles of the computer engineering and computer science (cyber) worlds deal with embedded computation and communications hardware systems, software programming, and networking, National Academies of Sciences, Engineering, and Medicine. 2016. A 21st Century Cyber-Physical Systems Education. Washington, DC: The National Academies Press. https://doi.org/10.17226/23686

2016: CPS are spatially-distributed, time-sensitive, and multi-scale, networked embedded systems, connecting the physical world to the cyber world through sensors and actuators. Lukas Esterle, Radu

Grosu; Elektrotechnik und Informationstechnik, Volume 133, Issue 7, pp 299–303, https://doi.org/10.1007/s00502-016-0426-6 .

2016: A CPS can be thought of as the utilization of the logical and discrete properties of the computers to control and oversee the continuous and dynamic properties of physical systems. Robust Cyber–Physical Systems: Concept, models, and implementation, Fei Hua, Yu Lua, Athanasios V. Vasilakos, Qi Haoc,, Rui Ma, Yogendra Patil, Ting Zhang, Jiang Lua, Xin Li, Neal N. Xiong, Future Generation Computer Systems, Volume 56, March 2016, Pages 449-475, https://doi.org/10.1016/j.future.2015.06.006

2017: Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. Edward R. Griffor, Christopher Greer, David A. Wollman, Martin J. Burns; Framework for Cyber-Physical Systems: Volume 1, Overview; NIST SP1500-201, https://doi.org/10.6028/NIST.SP.1500-201

2018, Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. NSF Cyber-Physical Systems Program announcement 18-538, 2018, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286 (accessed August 2018)

2018: CPS addresses the close interactions and feedback loop between the cyber components such as sensing systems and the physical components such as varying environment and energy systems. The exemplary CPS research areas include the theory and practice of data sensing and manipulation, the engineering foundation of the cyber-physical interactions, the design and verification of embedded computing systems, and the application of CPS methodologies in various areas such as smart energy systems, smart home/building/community/city, connected and autonomous vehicle system, medical prosthetics, wearable device, internet of things, etc. IEEE Technical Committee on Cyber-Physical Systems (CPS), http://www.ieeesystemscouncil.org/pages/cyber-physical-systems-technical-committee (accessed August 2018).

2018: Cyber-Physical Systems (CPS) has emerged as a unifying name for systems where the cyber parts, i.e., the computing and communication parts, and the physical parts are tightly integrated, both at the design time and during operation. Such systems use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. These cyber-physical systems range from miniscule (pace makers) to large-scale (a national power-grid).ACM Transactions on Cyber-Physical Systems, https://tcps.acm.org/ (accessed August 2018).

11 Appendix B – Examples of IoT Definitions

2002: It is the ultimate in inventory management: No hand-counting necessary--just let the chips speak up to vouch that every unit ordered has indeed arrived, on time and intact. In ten years, nearly every consumer item will probably bear a tiny chip that continually broadcasts its existence to radio-frequency readers at loading docks, store shelves, entrances, security stations and parking lots--just about everywhere. C.R. Schoenberger, The Internet of Things, Forbes, Mar. 18,2002, https://www.forbes.com/global/2002/0318/092.html#3a6d34043c3e (accessed August 2018).

2003: The Web, the collection of all devices connected to the Internet, is on the verge of experiencing a massive evolution from a Web of computers to a Web of things as new devices such as phones, beepers, sensors, wearable computers, telemetry sensors, and tracking agents connect to the Internet. B. Traversat, M. Abdelaziz, D. Doolin, M. Duigou, J.-C. Hugly, E. Pouyoul, Project JXTA-C: enabling a Web of things, in: 36th Annual Hawaii International Conference on System Sciences, https://doi.org/10.1109/HICSS.2003.1174816

2005: A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, any place connectivity for anyone, we will now have connectivity for anything. ITU Internet Reports 2005: The Internet of Things. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf (accessed August 2018).

2009: This leads us to our definition of the Internet of Things: "A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues." Haller S., Karnouskos S., Schroth C. (2009) The Internet of Things in an Enterprise Context. In: Domingue J., Fensel D., Traverso P. (eds) Future Internet – FIS 2008. FIS 2008. Lecture Notes in Computer Science, vol 5468. Springer, https://doi.org/10.1007/978-3-642-00985-3_2

2009: If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. Kevin Ashton, RFID Journal, June 2009 http://www.rfidjournal.com/articles/pdf?4986 (accessed August 2018).

2010: The *Internet of Things* (*IoT*) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of *things* or *objects* – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, smart phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals. The Internet of Things: A survey. Luigi Atzori, Antonio Lera, Giacomo Morabito, Computer Networks Volume 54, Issue 15, 28 October 2010, Pages 2787-2805 2010 https://doi.org/10.1016/j.comnet.2010.05.010

2010: The basic idea is that IoT will connect objects around us to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, smart phones make it possible to materialize IoT which interact and co-operate with each other to make the service better and accessible anytime, from anywhere. The "Internet of Things (IoT)" refers to the networked interconnection of everyday objects. An "IoT" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" … In the IoT, "thing" is object of the physical world (physical thing) or of the information world (virtual thing), which is capable of being identified and integrated into the communication networks. The "thing" should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. IETF, The Internet of Things - Concept and Problem Statement, https://tools.ietf.org/html/draft-lee-iot-problem-statement-05#ref-5 (accessed August 2018).

2010: The Internet of Things represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. From the Internet of Computers to the Internet of Things, Friedemann Mattern and Christian Floerkemeier, Translated from Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum 33(2):107–121, http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

2011: The Internet of Things is a concept in which the virtual world of information technology integrates seamlessly with the real world of things. Uckelmann D., Harrison M., Michahelles F. (2011) An Architectural Approach Towards the Future Internet of Things. In: Uckelmann D., Harrison M., Michahelles F. (eds) Architecting the Internet of Things. Springer, DOI https://doi.org/10.1007/978-3-642-19157-2_1

2011: The so called “Intelligent Products” and “Smart Products”–these two terms can be used interchangeably–are meant to be used in the context of the new era of the Internet of Things (IoT) which may be defined as a global network infrastructure where physical and virtual objects with unique ID are discovered and integrated seamlessly (taking into account security and privacy issues) in the associated information network where they are able to offer and receive services which are elements of business processes defined in the environment they become active. Dimitris Kiritsis, Closed-loop PLM for intelligent products in the era of the Internet of things, Computer-Aided Design, Volume 43, Issue 5, Pages 479-501, Computer-Aided Design, https://doi.org/10.1016/j.cad.2010.03.002

2011: The connection of physical things to the Internet makes it possible to access remote sensor data and to control the physical world from a distance. The mash-up of captured data with data retrieved from other sources, e.g., with data that is contained in the Web, gives rise to new synergistic services that go beyond the services that can be provided by an isolated embedded system. The Internet of Things is based on this vision. Kopetz H. (2011) Internet of Things. In: Real-Time Systems. Real-Time Systems Series. Springer, https://doi.org/10.1007/978-1-4419-8237-7_13

2012: ITU-T Y.2060, From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT) … the IoT adds the dimension "Any THING communication" to the information and communication technologies (ICTs) which already provide "any TIME" and "any PLACE" communication. Regarding the IoT, things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic. Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment. Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software. ITU, Series Y, https://www.itu.int/rec/T-REC-Y.2060-201206-I/en (accessed August 2018)

2012: Internet-of-Things (IoT) represents a "global network and service infrastructure of variable density and connectivity with self-configuring capabilities based on standard and interoperable protocols and formats [which] consists of heterogeneous things that have identities, physical and virtual attributes, and are seamlessly and securely integrated into the Internet". Thus, IoT follows the "anything connected" vision by ITU and assumes that any physical or virtual thing which could benefit from a connection to the Internet will eventually be connected. Oleksiy Mazhelis, Eetu Luoma, Henna Warma, Defining an Internet-of-Things Ecosystem, In: Andreev S., Balandin S., Koucheryavy Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networking. Lecture Notes in Computer Science, vol 7469. https://doi.org/10.1007/978-3-642-32686-8_1

2013: The Internet of Things (IoT) refers to a broad vision whereby 'things' such as everyday objects, places and environments are interconnected with one another via the Internet. Treffyn Lynch Koreshoff, Toni Robertson, Tuck Wah Leong, Internet of Things: a review of literature and products, OzCHI '13 Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration Pages 335-344, Adelaide, Australia, November 25 - 29, 2013, ACM, http://doi.org/10.1145/2541016.2541048

2014: The Internet of Things (IoT) is defined by ITU and IERC as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network. Peter Friess and Francisco Ibanez, Putting the Internet of Things Forward to the Next Level, in Internet of Things – From Research Innovation to Market Deployment, Ovidiu Vermesan and Peter Friess, editors, River Publishers, ISBN: 978-87-93102-94-1.

2014: The Internet of Things (IoT) is a new paradigm that combines aspects and technologies coming from different approaches. Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbiotic interaction. The smart object is the building block of the IoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact/control the physical world, but also to be interconnected, to each other, through Internet to exchange data and information. Eleonora Borgia, The Internet of Things vision: Key features, applications and open issues, Computer Communications, Volume 54, Pages 1-31, https://doi.org/10.1016/j.comcom.2014.09.008

2015: IoT Definition: "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react." ISO/IEC JTC1 SWG 5 AHG1, Internet of Things (IoT) Preliminary Report, https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf (accessed August 2018).

2015: [For low-complexity systems] “An IoT is a network that connects uniquely identifiable “Things” to the Internet. The “Things” have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the “Thing” can be collected and the state of the ‘Thing’ can be changed from anywhere, anytime, by anything.” [For high-complexity systems or large environment scenarios] “Internet of Things envisions a self-configuring, adaptive, complex network that interconnects ’things’ to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.” Roberto Minerva, Abyi Biru, Domenico, Rotondi, IEEE, Towards a definition of the Internet of Things (IoT). https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

2015: The Internet of Things is a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective. Ultimately, IoT devices will be ubiquitous, context-aware and will enable ambient intelligence. Andrew Whitmore, Anurag Agarwal, Li Da Xu, 2015, The Internet of Things,- A survey of topics and trends, Inf System Front (2015) 17:261-274, https://doi.org/10.1007/s10796-014-9489-2

2015: IoT is generally defined as a dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols; physical and virtual ‘things’ in an IoT have identities and attributes and are capable of using intelligent interfaces and being integrated as an information network, Li, S., Xu, L.D. & Zhao, S., The Internet of Things: A Survey, Inf Syst Front (2015) 17: 243. https://doi.org/10.1007/s10796-014-9492-7

2015: The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition. Karen Rose, Scott Eldridge, Lyman Chapin, The Internet of Things: An Overview, The Internet Society, https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (accessed August 2018).

2015: The term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called "smart objects", are not directly operated by humans but exist as components in buildings or vehicles, or are spread out in the environment. Internet Architecture Board (IAB), Architectural Considerations in Smart Object Networking, Request for Comments: 7452, https://tools.ietf.org/html/rfc7452 (accessed August 2018).

2015: The IoT model involves sensing, thinking, and acting, usually occurring iteratively in that order. The IoT already contains a myriad of sensors, and more are being added every day. Sensor data requires some form of processing, which constitutes the thinking phase of the model. The processed data, then, initiates some type of action. G. Hurlburt, XRDS: Crossroads, The ACM Magazine for Students - The Internet of Things, Volume 22 Issue 2, Pages 22-26, https://dl.acm.org/citation.cfm?id=2845143 (accessed August 2018).

2016: [T]he Internet of Things (IoT) approach has gained momentum in connecting everyday objects to the Internet and facilitating machine-to-human and machine-to-machine communication with the physical world. IoT offers the capability to connect and integrate both digital and physical entities, enabling a whole new class of applications and services. Yongrui Qin, Quan Z. Sheng, Nickolas J.G. Falkner, Schahram Dustdar, Hua Wang, Athanasios V. Vasilakos, When things matter: A survey on data-centric internet of things, Journal of Network and Computer Applications 64 (2016) 137–153; https://doi.org/10.1016/j.jnca.2015.12.016

2016: The idea of IoT is to interconnect the physical world with the digital world. Therefore, sensors measure parameters of the physical world as well as changes of it. Consequently, this information is translated into data processible by computers. Furthermore, the aim of IoT is to act on the physical world through actuators. Jasmin Guth, Uwe Breitenbucher, Michael Flkenthal, Frank Leymann, Lukas Reinfurt, Comparison of IoT platform architectures: A field study based on a reference architecture, 2016 Cloudification of the Internet of Things (CIoT), Paris, pp. 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7872918&isnumber=7872907

2017: Both the idea and technology for connecting sensors and actuators to a network to remotely monitor and control physical systems have been known for many years and developed accordingly. However, a little more than a decade ago the concept of the Internet of Things (IoT) was coined and used to integrate such approaches into a common framework. Technology has been constantly evolving and so has the concept of the Internet of Things, incorporating new terminology appropriate to technological advances and different application domains. Ibarra-Esquer JE, González-Navarro FF, Flores-Rios BL, Burtseva L, Astorga-Vargas MA. Tracking the Evolution of the Internet of Things Concept Across Different Application Domains. Sun Y, Cai Z, Jara A, eds. Sensors (Basel, Switzerland). 2017;17(6):1379. http://www.doi.org/10.3390/s17061379 .

2017: Over the last years, different definitions of the Internet of Things (IoT) have been created that describe the IoT as both a technological system and a concept. For example, in (www.cpsos.eu), the IoT is defined as “a new era of ubiquitous connectivity and intelligence, where a set of components, products, services and platforms connects, virtualizes, and integrates everything in a communication network for digital processing.” while the IERC definition (See http://www.internet-of-things-research.eu/about_iot.htm) states that the IoT is “a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. PICASSO Opportunity Report, Towards Enhanced EU-US ICT Pre-competitive Collaboration, http://www.picasso-project.eu/wp-content/uploads/2017/03/PICASSO-Opportunity-Report_March-2017_revMar19.pdf (accessed August 2018).

2018: The Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices. The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. IETF, Internet of Things Topics of Interest Page, https://www.ietf.org/topics/iot/ accessed August 2018.

2018: The Internet of Things, or IoT, refers to billions of physical devices around the world that are now connected to the internet, collecting and sharing data. Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an aeroplane, into part of the IoT. This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without a human being involved, and merging the digital and physical worlds. Steve Ranger, What is the IoT? Everything you need to know about the Internet of Things right now, ZDNet,Jan. 19, 2018, https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (accessed August 2018).

2018: The Internet of Things (IoT) can be defined as a world of interconnected things that are capable of sensing, actuating, and communicating among themselves and with the environment (i.e., smart things or smart objects). In addition, IoT provides the ability to share information and autonomously respond to real/physical world events by triggering processes and creating services with or without direct human intervention. Qusay Hassan, Introduction to the Internet of Things, in Internet of Things A to Z: Technologies and Applications, Wiley, http://www.doi.org/10.1002/9781119456735

12 Appendix C – Relationship between IoT and CPS

2011: Through cyber-physical systems, the physical world is linked with the virtual world to form an Internet of Things, Data and Services. Cyber-Physical Systems Driving force for Innovation in Mobility, Health, Energy and Production. Acatech Position Paper, December 2011 https://www.acatech.de/wp-content/uploads/2018/03/acatech_POSITION_CPS_Englisch_WEB-1.pdf (accessed August 2018)

2011: Although both IoT and CPS are aimed at increasing the connection between the cyber space and the physical world by using the information sensing and interactive technology, they have obvious differences: the IoT emphasizes the networking, and is aimed at interconnecting all the things in the physical world, thus it is an open network platform and infrastructure; the CPS emphasizes the information exchange and feedback, where the system should give feedback and control the physical world in addition to sensing the physical world, forming a closed-loop system. Ma HD. Internet of things: Objectives and scientific challenges. J. Comp. Sci. Tech. 26(6): 919–924 Nov. 2011. DOI https://doi.org/10.1007/s11390-011-1189-5

2012: The term “Internet-of-Things” is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities. Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamta, nternet of things: Vision, applications and research challenges, Ad Hoc Networks, Volume 10, Issue 7, Pages 1497-1516, https://doi.org/10.1016/j.adhoc.2012.02.016

2013: In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, Volume 29, Issue 7, Pages 1645-1660, https://doi.org/10.1016/j.future.2013.01.010

2014: Internet of Things generally focusses on the sensing of the physical world and the (internet) connectivity, emphasizing individual things providing data over the net to steer (usually organizational) processes. While sensing physical data and communicating it – not necessary via internet – is generally also required for cyber-physical systems, these systems also target the control of combined organizational and physical processes, and therefore specifically address tight human-machine interaction, mostly not addressed in Internet of Things. CyPhERS – Cyber-Physical European Roadmap & Strategy, Schatz, B., M. Torngren, S. Bensalem, M. V. Cengarle, H. Pfeifer, J. McDermid, R. Passerone, and A. Sangiovanni-Vincentelli. 2014, CyPhERS Research Agenda and Recommendations for Action, http://cyphers.eu/sites/default/files/d6.1+2-report.pdf. (accessed August 2018)

2015: CPS adds more emphasis to control technologies in what is known colloquially by the term, the 'Internet of Things' ... CPSs feature a tight combination of, and coordination between, the system's computational and physical elements, and integration of computer- and information-centric physical and engineered systems. An important class of CPS is called IoT, and this term is favoured by grant agencies in Europe and Asia. IoT is a network that can interconnect ordinary physical objects with identified addresses, based on the traditional information carriers including Internet and telecommunication networks. Therefore, Internet is not mandatory in IoT. Furthermore, interconnection and addresses are not required in CPS, and IoT is a subset of CPS. Arguably, control technologies in non-networked embedded systems applications are examples of CPSs that are not IoT. Ivan Stojmenovic & Fumin Zhang (2015) Inaugural issue of 'cyber-physical systems', Cyber-Physical Systems, 1:1, 1-4, http://dx.doi.org/10.1080/23335777.2015.970764

2015: In most academic and project activities, the difference between "Internet of Things" and "CyberPhysical Systems (CPS)" is not made clear and it is difficult to find a source that draws a clear-cut distinction between the two terms. Most persons consider the two definitions as different explanations for the same idea and use the words interchangeably.

> A cyber-physical system is a system of collaborating computational elements controlling physical entities. It is when the mechanical and electrical systems (e.g., sensors and communication tools) embedded in products and materials are networked using software components. They use shared knowledge and information from processes to independently control logistics and production systems. Accordingly, CPS tends to go beyond a mere unique identification and control of individual things to the level of networking between identified objects and sharing information about a specific condition so as to accomplish a certain goal with better efficiency.
>
> In contrast, an IoT system starts from the level where a single "thing" is identified using a unique global identifier and can be accessed from anywhere, anytime. The level of information obtained by accessing the "thing" can be as low as a static data that is stored on the RFID tags. Primarily, IoT is concerned with unique identification, connecting with the Internet and accessibility of "things." Yet, identified objects in an IoT system can still be networked together so as to control a certain scenario in a coordinated way, in which case an IoT system can be considered to grow to the level of a CPS.
>
> Generally, we can say that CPS is mainly concerned about the collaborative activity of sensors or actuators to achieve a certain goal and to do this CPS uses an IoT system to achieve the collaborative work of the distributed systems.
>
> Towards a definition of the Internet of Things (IoT), IEEE https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf

2017: Cyber-Physical Systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components … The Internet of Things (IoT) refers to the billions (and growing) of networked physical objects, devices, and systems that utilize embedded technology, including the multitude of diverse real-world CPSs, wireless sensors, and agents spanning many application domains that operate, interact, and communicate with the external environment via the internet … The resulting new generations of CPS and their emerging platforms such as the IoT and Industrial Internet (II) have major implications for the future of smart and connected environments, includ9ijng smart cities, thus raising the stakes for how architectures, control, dependability, networking, privacy, safety, and security of these systems are addressed across multiple domains. Cyber Physical Systems Virtual Organization, https://cps-vo.org/group/iot, (accessed August 2018).

2017: According to the PICASSO definition, the IoT is seen as an enabling technology for CPS or CPSoS [CPS Systems of Systems], while other, more encompassing definitions include also applications outside the domain of CPS and CPSoS, such as IoT-connected home entertainment systems or geolocation-enabled tracking infrastructures for consumer items. PICASSO Opportunity Report, Towards Enhanced EU-US ICT Pre-competitive Collaboration, http://www.picasso-project.eu/wp-content/uploads/2017/03/PICASSO-Opportunity-Report_March-2017_revMar19.pdf (accessed August 2018)

2018: CPS vs. Internet of Things (IoT), IoT does overlap with CPS, but it does not cover all of the foundations needed for CPS, and it does not address the feedback loops between cyber and physical worlds in general. CPS also tends to have much broader scope than IoT:

- CPS encompasses both isolated and networked systems, while IoT usually focuses on the latter. For instance, CPS encompasses both isolated pace makers and those pace makers that may be connected to other health monitors and actuators.
- CPS encompasses both time-insensitive and time-sensitive systems, while IoT usually does not focus on time-sensitive systems. For instance, both longer-timescale vehicle traffic flow optimization and real-time control of connected and automated vehicles belong to topics of CPS.
- CPS encompasses both open-loop and closed-loop control systems, while IoT usually focuses on open-loop systems. For instance, both dynamic pricing for indirect/human-in-the- loop load control and closed-loop microgrid control belong to the topics of CPS.

Wayne State University, College of Engineering, Cyber-Physical Systems Program. https://engineering.wayne.edu/cyber/about.php

2018: Cyber Physical Systems are Smart Systems that comprises of the merging and integration of Industry Control Systems, Critical Infrastructures, Internet of Things (IoT) and Embedded Systems. Yeboah-ofori, A.; Abdulai, J.; Katsriku, F. Cybercrime and Risks for Cyber Physical Systems: A Review. Preprints 2018, https://doi.org/10.20944/preprints201804.0066.v1