The Journal of Systems & Software 200 (2023) 111631

Contents lists available at ScienceDirect

The Journal of Systems & Software

journal homepage: www.elsevier.com/locate/jss

A literature review of IoT and CPS—What they are, and what they are not☆

Veronika Lesch [a,*], Marwin Züfle [a], André Bauer [a], Lukas Iffländer [a], Christian Krupitzer [b], Samuel Kounev [a]

[a] Department of Computer Science, University of Würzburg, Würzburg, Germany
[b] Department of Food Informatics, University of Hohenheim, Stuttgart, Germany

ARTICLE INFO

Article history:
Received 5 January 2022
Received in revised form 30 January 2023
Accepted 2 February 2023
Available online 15 February 2023

Keywords:
Cyber Physical System
Internet of Things
CPS
IoT
Literature review

ABSTRACT

Today, we are confronted with many concepts such as Cyber–Physical-Systems (CPS), Internet of Things (IoT), Industry 4.0, Industrial Internet, Ubiquitous Computing, Pervasive Computing and many more. Some researchers use all of these terms interchangeably, while others interpret them in ways that contradict each other. The inconsistent and interchangeable usage of these terms creates the impression that authors abuse them as buzzwords to attract attention. Hence, the question arises: Is the existence of all these terms justified? In this paper, we first look at the origin of the terms. Then, we focus on Internet of Things (IoT) and Cyber-Physical-Systems (CPS) as those terms are more often used as the others and further often seen as underlying technologies. We presentthe results of a literature review, including academic, industry and gray literature, with the objective to identify and discuss several clusters of similar statements on both terms. Building on this, we present definitions for IoT and CPS that reflect the core intuition of the terms as found in the literature review while providing a clear demarcation of the two terms. Then, we illustrate the applicability of our findings on several use cases. Finally, we discuss the relation to the other topics closely related to adaptive systems, namely Industry 4.0, Industrial Internet, Ubiquitous Computing, and Pervasive Computing.

1. Introduction

In recent years, the Internet of Things (IoT) and Cyber-Physical-Systems (CPS) have gained significant attraction and are becoming increasingly omnipresent. By the year 2030, the installed base of IoT devices will grow to 500 billion worldwide according to Cisco (Anon, 2016), while the estimated value of CPS will reach 12 USD Billion by 2028 (Data Bridge Market Research, 2020). Both IoT and CPS find applications in many different domains, such as healthcare, energy and utilities, smart cities and communities, manufacturing, and transportation and distribution. Besides IoT and CPS, many other related terms have found increasing use including but not limited to: Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing. All these terms have become increasingly important in recent years, both in industrial and academic environments.

The often interchangeably use of those terms lead to several questions: Is the usage of all these terms justified? What exactly do researchers mean when using these terms? How to distinguish these terms or can some of them be used interchangeably?

In the literature, IoT is seen as a global network of physical and virtual things that have identities, attributes, and personalities (e.g., Al-Garadi et al., 2020; Fahmideh and Zowghi, 2020; Tawalbeh et al., 2020; Anon, 2022l; Sundmaeker et al., 2010a; Uckelmann et al., 2011). These things provide intelligent interfaces accessible over standard and interoperable communication protocols. CPS are often defined as physical systems and computational entities that contain computing and communication cores (e.g., Lee, 2008b; Monostori, 2014; Pasqualetti et al., 2013; Kim and Kumar, 2012; Inderwildi et al., 2020; Waschull et al., 2020; Rathore et al., 2020). The connection of physical and virtual entities with behavioral aspects is an important property of CPS. So, CPS and IoT show much overlap: Both are defined as physical systems made of entities that communicate and have a virtual part or representation that mirrors resources and behavior. Additionally, a variety of descriptions on the terms Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing exist, many of which are very similar to the ones for CPS and IoT. These statements vary in their precision and scope: Some

☆ Editor: Uwe Zdun.

* Corresponding author.
E-mail addresses: veronika.lesch@uni-wuerzburg.de (V. Lesch), marwin.zuefle@uni-wuerzburg.de (M. Züfle), andre.bauer@uni-wuerzburg.de (A. Bauer), lukas.ifflaender@uni-wuerzburg.de (L. Iffländer), christian.krupitzer@uni-hohenheim.de (C. Krupitzer), samuel.kounev@uni-wuerzburg.de (S. Kounev).

https://doi.org/10.1016/j.jss.2023.111631
0164-1212/

statements are rather general, while others define terms very strictly.

However, a clear delineation of the respective concepts from one another cannot be found in the literature. Therefore, the following research questions arise:

(i) How are these different terms defined in the various fields, and are there overlaps or even contrasts between them?
(ii) What is the common interpretation of the terms and can this be used to propose refined definitions?
(iv) How are the terms to be distinguished from each other?

In this paper, we address these questions through a literature review, including academic, industry and gray literature. We start by discussing the origins of the different terms and their evolution. We analyze and compare statements on each term that can be found in the literature, while focusing on IoT and CPS as they are most actively used by the research community (based on the search results we had in an initial screening). We formulate refined definitions for IoT and CPS that precisely capture their essential aspects and intended meaning. Finally, the two refined definitions for IoT and CPS are used as reference points to delineate the remaining concepts.

Our goal is to help improve communication among researchers and practitioners, reducing confusion and misunderstandings due to the lack of understanding of the underlying concepts, aims and capabilities of the different terms as well as their historical evolution. Conceptual understanding of the state-of-the-art coupled with clear and consistent terminology provide a basis for supporting interoperability between emerging technologies, novel concepts and frameworks as well as for future research driving the further advancement of the field.

The remainder of this paper is organized as follows: First, Section 2 gives a discussion of the background of all terms. After that, Section 3 describes the methodology of the literature review, gives an overview of the collected statements, and presents statistics of the used data set. Then, Section 4 gives an overview and categorizes the statements on IoT, followed by Section 5, which summarizes and clusters the statements on CPS. Section 6 analyzes the statements, presents a refined definition for IoT and CPS, and illustrates them using different use cases. Section 7.4 proposes a delineation of the terms using the refined definitions of IoT and CPS as reference points. Finally, Section 9 summarizes the findings and concludes the paper.

2. Background

This section provides a brief summary of the background of the concepts discussed in this paper.

IoT. The term *Internet of Things* was first used by Kevin Ashton in 1999 (Ashton, 2009). In a presentation at Procter & Gamble, Ashton used the term to describe the idea of integrating RFID into the Procter & Gamble supply chain. He pointed out that humans controlled the collection of information by these systems at that time. According to Ashton, this was a problem since humans have limited time, accuracy, and attention, and therefore, they cannot capture data very well. As systems depend on data captured by humans, Ashton states that "computers know more about ideas than things" (Ashton, 2009). To overcome this lack of accuracy, computers need to gather information by themselves without relying on humans. Also, in an article in the Forbes magazine from 2002, Ashton is cited with: "We need an Internet for things, a standardized way for computers to understand the real world" (Schoenberger, 2002). Ashton claims that if computers knew everything important about things without the intervention of humans, it would be possible to track those things in order to reduce waste, loss, and cost, considerably. In this context, he also mentions repairing on time in the sense of predictive maintenance (Ashton, 2009). Later on, Kevin Ashton co-founded the Auto-ID Labs, which made the term *Internet of Things* more popular (Mattern and Floerkemeier, 2010b).

CPS. The term *Cyber–Physical System* was coined by Helen Gill in 2006 at the US National Science Foundation. Gill defines the term as a "new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities" (Baheti and Gill, 2011). Thus, CPS deals with the intersection of the physical and the cyber world. In the context of CPS, 'cyber' does not originate from the term *cyberspace* but more from the term *cybernetics* (Lee and Seshia, 2017), which was coined by Norbert Wiener in 1948 in the domain of control theory. According to Wiener, cybernetics can be seen as a combination of control and communication and is highly based on closed feedback loops, hence, the control logic depends on the real measurement values and the physical process is managed by the control loop. Similar to this definition, feedback loops are typically an important part of CPS where computations and physical processes affect each other (Lee and Seshia, 2017).

Industry 4.0. The term *Industry 4.0* was first introduced by Henning Kagermann (President of acatech, the German Academy of Science and Engineering), Wolf-Dieter Lukas (Head of the Department for Key Technologies at the German Federal Ministry of Education and Research) and Wolfgang Wahlster (Head of the German Research Centre for Artificial Intelligence) at the 2011 Hannover Fair (Kagermann et al., 2011). Industry 4.0 stands for the fourth industrial revolution and is a result of the high-tech strategy of the German government (BMBF-Internetredaktion, 2016). The first industrial revolution was the introduction of mechanization through water and steam power. The second industrial revolution brought mass production, assembly lines and electricity. The introduction of computers and automation, especially programmable logic controllers, formed the third industrial revolution (Anon, 2012c).

The goal of the fourth industrial revolution is to build a bridge between the cyber space and the physical world through the digitization of production facilities and industrial products. This bridge leads to a fine-grained synchronization between the physical world and a digital model of it. Intelligent supervision and autonomous decision processes enable to control enterprises and the entire supply chain in real-time, in addition to the increased automation known from the third industrial revolution. This paradigm shift requires the products to take over a new, active role: Instead of a central logic, the unmachined part itself defines its processing steps.

Industrial Internet. The emergence of Distributed Control Systems (DCS) was an important step towards the *Industrial Internet*, also known as Industrial Internet of Things, enabling flexible process control of an entire plant. With the rise of the Ethernet standard in 1980, first experiments with networked smart devices followed soon. The Carnegie Mellon University presented a modified Coke machine in 1982 as the first Internet-connected appliance (Palermo, 2014). It was able to report its inventory and the temperature of the loaded drinks. Next, in 1994, Reza Raji described a large industrial application as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories" (Raji, 1994). The current interpretation of the term Industrial Internet appeared 2002 with the rise of cloud technologies. The usage

spread in 2006 with the development of the OPC Unified Architecture (OPC UA) protocol and its corresponding information model. Analysts expect that the adoption of Industrial Internet generates $15 trillion of global GDP by 2030 (Prith Banerjee, Accenture Technology Labs, 2014; Zurier, 2016).

Ubiquitous Computing. Mark Weiser from the Xerox Palo Alto Research Center introduced the term *Ubiquitous Computing* in 1991 (Weiser, 1991). According to Weiser, computers at that time were too complex and required the entire attention of their users. However, he claimed that computers should only be a means to an end. More precisely, Weiser envisioned computers that are ubiquitous but invisible. Thus, the computer should move into the background and the focus should be on the thing itself. In his article from 1991, Weiser wrote: "By pushing computers into the background, embodied virtuality will make individuals more aware of the people on the other ends of their computer links" (Weiser, 1991).

Pervasive Computing. Weiser also used the term *pervasive* in his descriptions: "Again, I saw this not as a personal computer, but as a pervasive part of everyday life, with many active at all times" (Weiser, 1993). However, the term *Pervasive Computing* was first introduced by Novell's Chairman Robert J. Frankenberg around 1994 (Ronzani, 2009). He used this term in the sense of connecting people with other people and information (Ronzani, 2009). The term was only used in the research community at that time. In 1998, IBM reintroduced the term Pervasive Computing for describing the necessity that people require a connection to the Internet at any time. Ronzani (2009). This led to a rapidly increasing interest around the turn of the millennium and finally, "pervasive computing was declared a buzzword during the peak of the dot.com bubble" (Ronzani, 2009).

So, Pervasive Computing can be seen as an industry term in contrast to the more academic term Ubiquitous Computing with a slightly different meaning (Mattern, 2007). This also applies to pervasive and ubiquitous information processing in the context of e-commerce scenarios and web-based business processes (Mattern, 2007). However, the interest in the term Pervasive Computing decreased considerably since 2001. Like Weiser, who used the term pervasive in one of his articles on Ubiquitous Computing, Uwe Hansmann of IBM also used the term ubiquitous in one of his works on Pervasive Computing (Hansmann et al., 2003). Therefore, the delineation between Ubiquitous and Pervasive Computing is rather vague. Mattern considers both terms as synonyms (Mattern, 2007). According to a literature study by Ronzani, Ubiquitous Computing is more often used for work and business, while Pervasive Computing is more established in the home and leisure sectors (Ronzani, 2009). Also, Ronzani points out that Ubiquitous Computing is typically used in the sense of anywhere and at any time, whereas Pervasive Computing is used more in the sense of networking.

3. Methodology

In the previous section, we presented the background and historic evolution of the investigated terms. This section describes the methodology we used for our literature review to evaluate how the terms IoT and CPS are used by practitioners and researchers. It further provides an overview of the used data sources and presents statistics on the underlying data set.

3.1. Overview on methodology

The literature review covers academic, industrial, as well as gray statements and is focused on the terms IoT and CPS, as they are most actively used by the research community and in the industry. Accordingly, the delineation in Section 6 focuses on those two terms and distinguish each other as well as describe the relation to the other terms namely Industry 4.0, Industrial Internet of Things (IIoT), Pervasive, and Ubiquitous Computing.

For the literature review, we applied the technique from Webster and Watson (Webster and Watson, 2002). The review process consists of four steps as depicted in Fig. 1.

Keywords. The first step consists of a broad search for statement candidates based on the following keywords and their permutations:

- *Cyber–Physical System*
- *CPS*
- *Internet of Things*
- *IoT*
- *Definition*
- *Statement*

We derived the keywords and the permutations based on the goal of this paper, which is to provide an in-depth analysis of definitions and statements of the two terms IoT and CPS. We build permutations with one term of the set of {Cyber-Physical System,CPS,Internet of Things,IoT} with another term of the set {Definition,Statement} resulting in the following search string: `{Cyber-Physical System OR CPS OR Internet of Thing OR IoT} AND {Definition OR Statement}`.

Hence, we strictly focus on the stated terms and explicitly exclude related terms such as *Industry 4.0*, *Industrial Internet*, *Ubiquitous Computing*, *Pervasive Computing*, *Industrial IoT*, *Cyber–Physical Systems-of-Systems*, *Edge Intelligence*, or *Edge AI* from our literature review. Still, we acknowledge that these terms should be integrated in any future studies aiming at a full overview of the research landscape on IoT and CPS. For now, we did not include them as some of the terms/concepts can be seen as specific applications of either IoT or CPS. Hence, for this first step and to also sharp the focus, we limit this analysis to IoT and CPS.

Data sources. For academic literature, we used the search engine Google Scholar, as well as the digital libraries IEEE Xplore and ACM DL for the search. For statements with origin in industry, we used Google's web search. Since all of the authors work in Germany, also German websites as well as statements on IoT and CPS in German were identified. Then, we tried to switch the website language to English to retrieve the English version of the statement. In case this was not possible, we translated the statement into English and verified our translation by an internal review from all other authors. For each data source, we analyzed the first ten pages with results for each permutation of keywords. We found that this were enough results to cover the most important facets.

Conducting/Filtering. In the second step, we filtered papers that do not explicitly define the terms or include statements that explicitly describe their properties. There, one paper was read by one of the authors. If a paper should be filtered out because it did not provide a defining statement, this had to be confirmed by a second author. We are aware, that this approach can result in human bias. Hence, those decisions were clearly discussed by the authors and in case of disagreement, further researchers of the group were involved. As we later cluster the statements (see step 4), we have a second feedback loop if a paper should be part

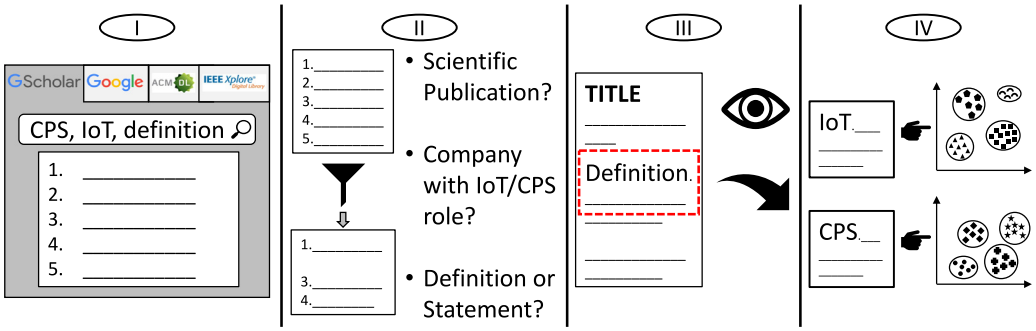

Fig. 1. Methodology for the Literature Review. After the initial search of candidate publications in Google Scholar, Google, IEEExplore, and ACM DL using the predefined keywords (step I), we analyzed the suitability of the publications w.r.t. a provided definition or statement on CPS or IoT (step II) and extracted those (step III). Lastly, we clustered the definitions based on the used wording (step IV).

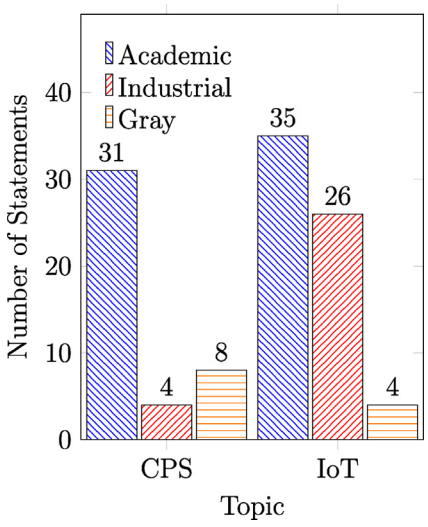

Fig. 2. Break down of statements per topic and application domain.

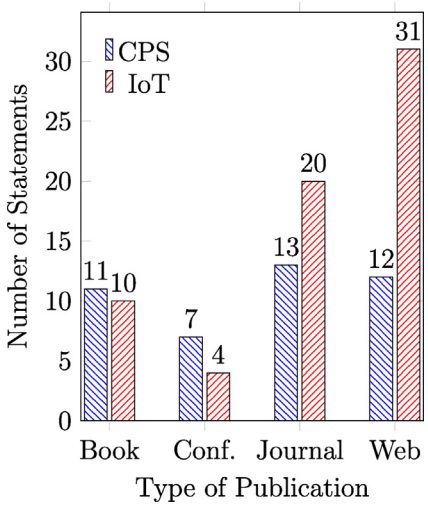

Fig. 3. Number of statements per type of publication and topic.

of the analysis or not. We focused on peer-reviewed scientific publications or publications of companies that have an important role in IoT or CPS related industries. After retrieving these sources, the suitability of each paper or website was analyzed based on the title and abstract (if existent).

Extracting Data. As a third step, we did a detailed review of the selected papers and websites and extracted the relevant statements. This resulted in 108 papers and websites that we studied in more detail collecting 65 statements for IoT and 43 for CPS. From all statements, 66 can be considered as academic, 30 as industrial, and 12 as neutral, resulting from Encyclopedia entries and similar. All extracted statements are listed in Table A.3 in the appendix.

Synthesizing Knowledge. In the fourth step, we clustered all statements on each term on a manual basis. We read the statements identifying similarities and differences and grouped related statements into clusters. Since this step has been performed manually, we did not apply any text mining or coding-based clustering. Rather, we read the statements individually, compared them one by one and tried to identify similarities in the choice of words, the addressed technical level, or common visions for the future. This means, a statement is always assigned exactly to one cluster. After the initial clustering, we further examined the clusters with their according statements in the local research group to gain even more insight into the clustering. This additional group decisions help to reduce the probability for human bias as well as increase the robustness of the results. Here, we identified four major clusters for every term and some outlier statements. These clusters are not necessarily distinct, but may rely on other clusters. However, we decided to treat them as distinct clusters as each has a different focus. The assignment of a statement to a cluster is always unique but some clusters could be merged in case a higher level of detail is desired. We omitted the outliers as they deal with, for example, the vision and history of the terms or business advances, and thus do not provide a clear statement on what IoT and CPS are. The term outliers refers to a single statement that was not assigned to any cluster in the manual clustering phase and is the only statement left in the end. We could have defined a cluster with only one statement, but decided to omit these leftover statements since we want to reflect on the major research streams related to IoT and CPS.

3.2. Overview on identified data

In the following, some statistics on the data set are presented to provide an overview of the used statements. The statistics include the share of statements focusing on IoT and CPS, the portion of statements for both terms grouped by their publication type, and an analysis where the authors of the statements come from.

First of all, the share of the data set focusing either on IoT or CPS is depicted in Fig. 2. The statements are divided into academic, industrial, or neutral, depending on the source from which

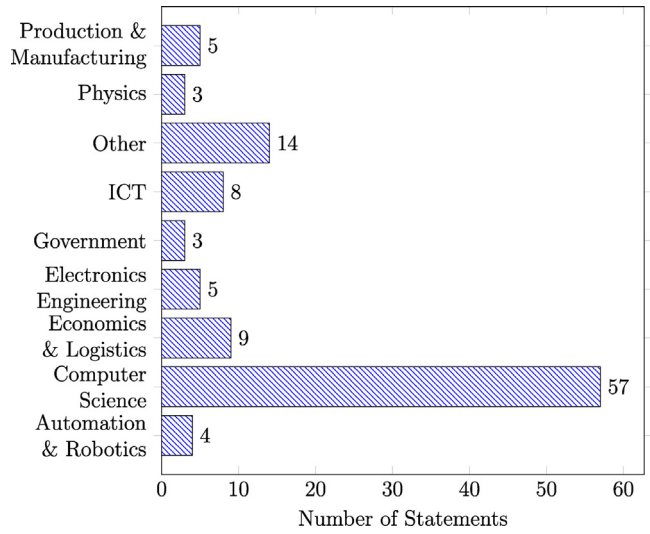

Fig. 4. Break down of statements per research domain.

they originate. As seen from Fig. 2, statements on both terms are found almost equally often in academic publications. However, in industrial sources, statements on CPS are rarer than statements on IoT. Possible reasons could be that IoT was heavily discussed in social media, as well as in European and international politics and initiatives, whereas CPS has been more a topic of academic research projects.

Fig. 3 shows the number of statements on IoT and CPS grouped by the type of publication. For IoT, most statements are published via web, whereas for CPS, statements are more evenly distributed among sources from books, conferences, journals, and the web.

Fig. 4 breaks down the statements by their research area or another origin (i.e., Other). Most statements were published in the area of computer science, followed by economics & logistics and information and telecommunication technologies (ICT). Note that the high count of Other is due, for example, to the fact that statements from different dictionaries were also examined.

Finally, Fig. 5 depicts the institutions' origin of the statements' authors. The institutions of the analyzed statements come from 28 different countries. However, only USA, Germany, Switzerland, France, and Italy have a share larger than 4%, with USA and Germany covering around 32.70% and 16.93%, respectively. As we focused on the languages English and German, other countries may be under-represented.

4. Identified definitions of Internet of Things

Applying the methodology and clustering process described in Section 3, this section addresses the first research question for the term IoT, whether IoT is clearly defined. With this analysis, we want to show that the term IoT is not clearly used in the communities, hence, also not clearly defined. We derive the following four clusters of statements on the term IoT: (i) entity communication, (ii) entity communication, identification, and interaction, (iii) enabling technologies, and (iv) IoT as CPS. Here, the second cluster is handled as a distinct cluster as it groups statements that, in addition to entity communication, name the terms identification and interaction explicitly and are not in the focus of the statements in the first cluster. The names of the clusters are chosen to indicate the main common characteristic of the statements grouped in the respective cluster. In the following, for each cluster, a selection of representative statements are presented, their differences and commonalities are discussed, and possible conflicts with other clusters are highlighted.

Entity communication. The first cluster groups statements that focus on IoT as enabler for communication between physical entities also called things or objects in the analyzed statements.

For example, F. Silva and C. Analide describe IoT as follows:

> The Internet of things is a new paradigm in which every device is digitally connected, regardless of their function, and can communicate with other devices and people over communication protocols. Silva and Analide (2016)

In addition to the above statement, this cluster includes 19 further statements on IoT (Kelly et al., 2013; Gillis, 2022w; Anon, 2022g,o,s,n; Ganji et al., 2010; Anon, 2011a, 2012a; Rose et al., 2015; Farash et al., 2016; Voas, 2016; Botta et al., 2016; Qin et al., 2016; Sundmaeker et al., 2010b; Lee, 2016; Anon, 2022m; Sobin, 2020; Tawalbeh et al., 2020), which have in common that IoT is defined as a network of physical entities that are connected and communicate with each other or with the environment. While communication is an important aspect of IoT, these statements do not make any assumptions on how communication is leveraged to achieve additional benefits compared to simple objects that do not communicate. Neither aspects of entity identification and interaction, nor sensing and control, are mentioned. These terms are used in the statements of the following cluster to describe how communication is used.

Entity identification, communication, and interaction. The second cluster includes statements that stress entity identification, communication, and interaction explicitly. For example, J. S. Rellermeyer et al. define IoT as follows:

> The notion of an "Internet of Things" refers to the possibility of endowing everyday objects with the ability to identify themselves, communicate with other objects, and possibly compute. Rellermeyer et al. (2008)

The statement of D. Miorandi et al. is more detailed:

> IoT builds on three pillars, related to the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) communicate (anything communicates) and (iii) interact (anything interacts)– either among themselves, building networks of interconnected objects, or with end-users or other entities in the network. Miorandi et al. (2012)

This cluster consists of four additional statements (Anon, 2012b; Atzori et al., 2010; Anon, 2014a, 2020c). All six definitions of this cluster enhance the aspects of the first cluster – communication between physical entities – by explicitly stating that IoT not only enables physical entities to communicate, but also to sense or interact with each other, with the end-user, or with the environment. With this ability, it is possible to define global goals for the whole system. As devices can interact and identify themselves, they can come to an agreement and influence their mode of operation in order to optimize the system with respect to the global goals. The question arises whether this is a valid interpretation of IoT as devices become more and more sophisticated and powerful.

Enabling technologies. The next cluster groups statements that focus the description how current computing and communication technologies are used as a basis for implementing IoT applications. J. Winter defines IoT using a more technological view:

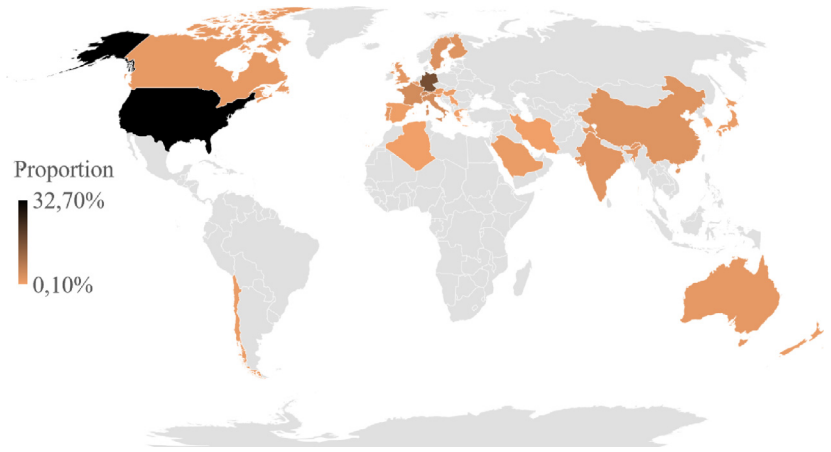

Fig. 5. Distribution of authors' countries of origin.[1]

> IoT relates to the integration of the physical world with the virtual world – with any object having the potential to be connected to the Internet via short-range wireless technologies, such as radio frequency identification (RFID), near field communication (NFC), or wireless sensor networks (WSNs). This merging of the physical and virtual worlds is intended to increase instrumentation, tracking, and measurement of both natural and social processes. Winter (2015)

This cluster consists of eight additional statements that explicitly list the underlying technologies on which IoT applications are based (Anon, 2015; Cosgrove-Sacks, 2014; Taplin, 2016; Minerva et al.; Jammes, 2016; Fahmideh and Zowghi, 2020; Al-Garadi et al., 2020; Tun et al., 2021). Typically mentioned technologies include RESTful services, HTTP, JavaScript, APIs, RFID tags, mobile network, and NFC. This raises the question of whether specific enabling technologies should rather be avoided when defining IoT since they only reflect today's state-of-the-art and new application might require reworked technologies.

IoT as CPS. Interestingly, the last cluster contains statements that are very similar to the statements that were found for CPS. The first representative statement from Bosch Software Innovations defines IoT as follows:

> The physical essence of the Internet of Things (IoT) is billions of connected devices providing data – in many cases in real-time – and sending it back to businesses that can remotely and automatically control this physical infrastructure. Innovations, Bosch Software (2022)

Another representative statement for this cluster is from Z. Shelby and C. Bormann who state that IoT

> encompasses all the embedded devices and networks that are natively IP-enabled and Internet-connected, along with the Internet services monitoring and controlling those devices. Shelby and Bormann (2011)

This cluster consists of twelve further statements that all exhibit many similarities to statements about CPS (Sundmaeker et al., 2010a; Anon, 2022l; Uckelmann et al., 2011; Anon, 2019b; Lee and Lee, 2015; Anon, 2022j; Delic, 2016; Anon, 2022; Mattern and Floerkemeier, 2010a; Yachir et al., 2016; Huberman, 2016; Fjäder, 2016). These statements describe IoT as systems consisting of physical and virtual components where communication between machines and the business IT takes place and the physical infrastructure is controlled and adapted automatically. This cluster shows strong similarities to the statements of CPS, that we analyze in the next section.

5. Identified definitions of Cyber–Physical-Systems

This section presents the collected statements on CPS and addresses the first research question for this term, whether CPS is clearly defined. Similarly to the previous section, also for CPS, the use of the term is highly variable in the research. Hence, we also need to analyze the different meanings of the term and their context. We identified four clusters using the literature review approach as described in Section 3: (i) integration of cyber and physical world, (ii) integration of cyber and physical world with explicit use of communication technologies, (iii) integration of cyber and physical world with explicit use of sensors, and (iv) functions of CPS. Here, the first, second, and third clusters are handled as distinct clusters. The statements in the second cluster focus on communication as an important part of CPS. The statements in the third cluster focus on sensors and name them explicitly, whereas sensors are not mentioned explicitly by statements in the first and second clusters. Speaking of integration between the cyber and physical world might remind the reader of *embedded systems*. An embedded system is a special-purpose computing system integrated into a larger mechanical or electrical system. It is embedded as part of a complete device (often including hardware and mechanical parts) and executes a dedicated function such as monitoring or controlling equipment (Serpanos and Wolf, 2011). As will become more clear in the following, important differences between CPS and embedded systems exist. CPS are distributed systems that monitor, automate, and control complex physical systems and processes as opposed to an encapsulated technical system. Stated in a simplified manner, CPS can be seen as systems of systems where multiple embedded systems can be used as sub-systems within the larger system supporting the integration of physical and cyber components.

Integration of cyber and physical world. The first cluster groups statements that stress the integration of the cyber and physical world as main aspect of CPS. In the first statement from the National Science Foundation, CPS are defined as

[1] Supported by Bing, Copyright GeoNames, MSFT, Microsoft, NavInfo, Navteq, Wikipedia.

> [...] engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Anon (2022d)

The second statement from R. Baheti and H. Gill from the year 2011 defines CPS as follows:

> 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. Baheti and Gill (2011)

This cluster includes five additional statements that define CPS in a similar way (Henkel, 2022b; Sehgal et al., 2014; Tripakis, 2015; Nuzzo, 2015; Yaacoub et al., 2020; Gürdür Broo et al., 2021; Inderwildi et al., 2020; Waschull et al., 2020). Computers monitor and control physical processes by means of computational algorithms and feedback loops. The physical components in CPS refer to physical resources, machines, processes, etc., whereas the cyber components consist of the mentioned computational algorithms (as well as possibly involved communication mechanisms) that control the physical components. For this purpose, the algorithms might reason on monitored data using feedback loops. There is no explicit requirement about where the algorithms are executed, that is, they could run locally on the devices without the need for communication over a network. This does not refer to the information exchange between, e.g., sensors and the computation component within one physical resource, but the communication between different physical resources using a network.

Integration of cyber and physical world with explicit use of communication technologies. This cluster groups statements that are based on the previous cluster but add explicitly the use of communication technologies, which can be seen in the following. The statement from R. Rajkumar et al. defines CPS as

> physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Rajkumar et al. (2010)

The statement from K.-D. Kim and P.R. Kumar defines CPS as systems with computing, communication and control technologies while explicitly mentioning the goals of CPS.

> CPSs refer to the next generation of engineered systems that require tight integration of computing, communication, and control technologies to achieve stability, performance, reliability, robustness, and efficiency in dealing with physical systems of many application domains. Kim and Kumar (2012)

The statement by E.A. Lee from the year 2008 defines CPS as follows:

> Cyber-Physical Systems 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. Lee (2008b)

This cluster includes 21 additional statements (Monostori, 2014; Beetz, 2010; Anon, 2022e; Pasqualetti et al., 2013; Cardenas et al., 2008; Zhang, 2015; Magaia et al., 2015; Estevez et al., 2015; Yao et al., 2015; Dai et al., 2015; Mousavi and Berger, 2015; Rawat and Khanna, 2015; Anon, 2022b; Khaitan and McCalley, 2015; Vogel Communications Group GmbH & Co. K.G., 2017; Tan et al., 2008; Anon, 2013, 2019a; Ara et al., 2015; Rathore et al., 2020), which have in common that communication is one important part in addition to the integration of the cyber and physical world and the use of sensors. In this context, communication means the exchange of information (e.g., monitoring data), but also instructions what to do next or how to reconfigure the system. This additional data enables smart decision making and more complex algorithms in the cyber world to achieve stability, performance, reliability, robustness, and efficiency of CPS. Until now, all statements had an intra-system view. The system consists of cyber and physical parts as well as communication capabilities.

Integration of cyber and physical world with explicit use of sensors. The second cluster groups statements that include sensors explicitly as inherent part of a CPS. The integration of the cyber and physical world is assumed as a basis. This means that all statements in this cluster could also be assigned to be part of the first cluster, that is, this cluster can be seen as a subset of the first cluster. A representative statement for this cluster is written by M. Adhikari et al. in the year 2015. They define CPS as follows:

> Cyber-physical systems (CPS) interconnect the cyber world and the physical world by embedding sensors and computational nodes. Adhikari et al. (2015)

The cluster includes two additional statements besides the mentioned one (Reinheimer and Strahringer, 2014; Tan et al., 2009), which rely on the integration of the cyber and the physical world, but add sensors as an important component for the realization of CPS. When monitoring with sensors, additional data can be gathered. However, the statements in this cluster do not mention how this monitoring data is used. They neither specify what is done with the data nor whether the data is used at all. The statements of the next cluster address this question.

Functions of CPS. The fourth cluster of statements deals with statements from another point of view. These statements see CPS from outside the system and describe them in a more general way. The statement from IBM defines CPS as follows:

> Cyber-physical systems, or CPS for short, are sophisticated computer devices that work together to perform functions, control physical elements, and respond to human control. Anon (2018)

They see CPS as computing devices that work together, control and influence the physical world using actors, and react to information from the physical world. Together with two further statements (Anon, 2022r; Danielis et al., 2014), this statement forms a separate cluster. All three statements see CPS as encapsulated systems (where functions or tasks are executed) that control physical systems and processes.

6. Delineation of CPS and IoT

During our literature search and analysis, we identified that the terms CPS and IoT are often used interchangeably for similar meanings. Obviously, this fuzziness contradicts the accurate scientific work. Hence, we want to investigate further the differences between both concepts. The presented clusters of statements show a tendency towards the control and influence of the cyber world on the physical world. This property is missing when looking at most of the IoT statements. So the question arises whether this is one of the important properties that distinguish CPS from IoT? Which further possible differences and which similarities between the two terms can be identified?

We now present a more in-depth analysis of the statements on IoT and CPS by examining how often various words are used

Table 1
Identified synonym groups extracted from all statements with one representative which is used in the automated statement analysis.

Representative	Group of terms
Actuate	act, actor, actuator, execute
Autonomous	automatically, self-*
Communication	communicate, intranet, IP, network, transfer
Compute	computation, computational
Control	–
Cyber	virtual
Entity	component, device, item, node, object, part, resource, system, thing
Environment	–
Identify	address, barcode, identifiable, NFC, RFID, tag
Integration	convergence, depend
Interaction	cooperate, interact, interoperate, together
Interconnection	connect, connection, connectivity, interconnectedness, interoperability, interoperable, Machine-to-machine
Internet	–
Monitor	collect, sensor
Physical	real
Process	computer, dataprocessing, processor
Software	algorithm, code, function

when speaking about these terms. We address the second research question: What is the common interpretation of the terms, and can this be used to propose refined definitions? This question is answered by summarizing the important properties that were identified during the clustering process and discussing how they are reflected in IoT and CPS statements. However, the reasons why exactly these properties are used in the statements identified during the literature review are not examined. Furthermore, we propose new refined definitions for IoT and CPS that reflect the core intuition of the terms as the literature review identified as practical usage. Here, we aim for a clear delineation of the two terms. Finally, we discuss the proposed definitions using several use cases to demonstrate the distinction between the two terms.

6.1. Statement analysis

As a first step, the words used in the statements are analyzed. To this end, we read a csv-file into R. Each row in this file contains a statement with its reference and with information about whether it defines IoT or CPS and its origin (academic or industry). Then, we cleaned each statement, represented by a string, by removing punctuation, numbers, and non-words with string functions, and setting all words to lowercase. Afterwards, we use a lexicon for stemming[2] to reduce each word to its stem. After stemming, we remove prepositions, articles, pronouns, etc. The remaining words are essential and descriptive. These words are then grouped to find words with similar meaning. This grouping is based on a lexical analysis of each word done by four authors of the paper independent of each other. Differing understandings were discussed and a common understanding was built. Table 1 presents the identified term groups that are considered synonyms and represented by a single term for the coding-based statement analysis. The terms of a group are extracted from all statements, and this set has no claim to be complete. Then, the occurrences of the grouped words are counted in all statements of each type (i.e., CPS or IoT, academic or industry) and the proportion of all statements of the respective type is computed.

Finally, Fig. 6 presents an overview of the most frequent and important words. The words from statements on CPS are plotted as red dots, the ones from statements on IoT as blue triangles. As an example, a red dot in the industry area and a value of 0.50 means that the respective word appears in 50% of the CPS statements extracted from industrial sources.

An analysis of Fig. 6 shows similarities but also contradicting results when comparing words used to describe IoT and CPS. Note that an overview of all representative words can be found in Table 1. In the following, the most important findings are discussed. The first important representative word for IoT with a frequency of nearly 100% is *entity*. It is very frequent for IoT statements but also occurs in statements on CPS in about 75% of the cases. Other words that are grouped under *entity* are: *component*, *device*, *item*, *node*, *object*, *part*, *resource*, *system*, and *thing*. Another frequent word for IoT is *environment*, as it only appears in IoT statements. However, its frequency is between 10% and 15% for both areas. The next word when defining IoT is *identify*. Alternative words, also grouped under *identify*, are: *address*, *barcode*, *identifiable*, *NFC*, *RFID*, and *tag*. Identify appears in the academic area only in IoT statements and is nearly twice as frequent as in CPS statements in the industry area. *Interaction* is another frequent word with a frequency of more than 40% in the academic area. In contrast, for CPS statements it is only used in 15%–30% of the statements and is not as frequent. Other words grouped under *interaction* are: *cooperate*, *interact*, *interoperate*, and *together*. Finally, *interconnection* is an often used word for IoT as it appears in about 40% of all statements for IoT, but only in around 10% of CPS statements. Alternative words include: *connect*, *connection*, *connectivity*, *interconnectedness*, *interoperability*, *interoperable*, and *machine-to-machine*. These findings are in line with the identified characteristics of IoT during the clustering process. The clusters found in the analysis cover these terms and support this finding. To actuate, to identify and interaction were important terms in the statements on IoT, while they had a subordinate role in the statements on CPS.

When looking at the frequencies of words in CPS statements, *compute* is one of the first outstanding terms. It has a frequency of around 60% in the academic area and does not appear in IoT statements. Similar behavior can be seen in the industry area, where its frequency is twice as high for statements on CPS. Alternative words for compute are: *computation* and *computational*. The next word *control* does not appear in statements on IoT at all and has a frequency of about 40% for CPS in both the academic and industry area. *Physical* is the next word from CPS statements that stands out. The alternative word *real* is also grouped together with it. Physical appears twice as frequent in CPS statements as in IoT statements. And finally, *process* (to which *computer*, *data processing*, and *processor* are grouped) appears in the academic area only in CPS statements and appears in the industry area more often in CPS statements than in IoT statements. As seen for the IoT statements, the important words for CPS statements that are less important in IoT statements go in line with the clusters identified during our literature review.

However, there are also some commonalities for CPS and IoT statements. The first important word that appears in both statements nearly equally often is *communication*. The words *communicate*, *intranet*, *IP*, *network*, and *transfer* are grouped under *communication*. *Entity* also appears in statements on both terms and is therefore an essential word for both terms, even if it occurs in nearly every statement on IoT and in comparison only around 80% of CPS statements. A word that appears less frequently but is seen in IoT and CPS statements nearly equally often is *integration*. Alternative words for integration include: *convergence* and *depend*. Finally, the word *monitor*, under which also *collect* and *sensor* are grouped, appears in about 30% of the statements on

[2] http://www.lexiconista.com/Datasets/lemmatization-en.zip

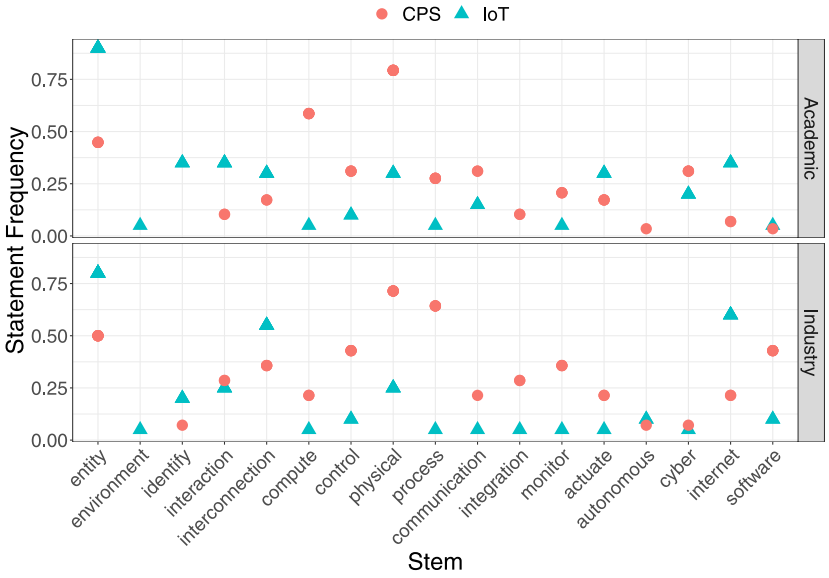

Fig. 6. Frequency of words used in statements on IoT and CPS.

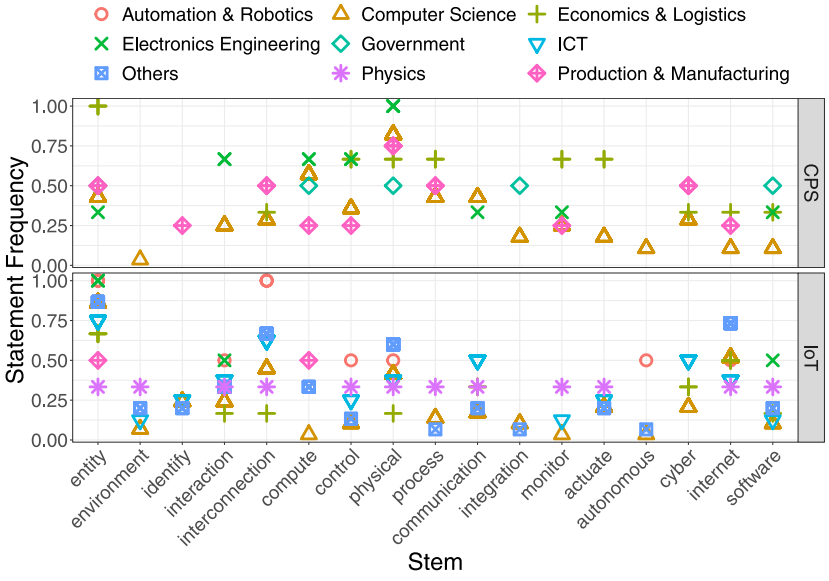

Fig. 7. Frequency of words used in statements on IoT and CPS across different domains.

both terms. The identified commonalities between CPS and IoT statements go in line with the identified clusters as communication, entity, integration, and monitor play an important role in the statements for IoT as well as for CPS.

To investigate how the words from Fig. 6 are used in different domains, we analyze their frequency across these domains in Fig. 7. For example, the pink rhombus in the CPS panel for the word *entity* with a value of 50% means that half of the statements from the domain production & manufacturing contain this word. Please note that we have omitted statements that occur only once per domain in CPS or IoT. While for IoT, almost all terms across all domains are below 50%, CPS is more consistent (i.e., the terms range between 25% and 75%). The highest degree of similarity of definitions is found for CPS in the domains economics & logistics and electronics engineering. In contrast, the lowest level of agreement for IoT is found in the domain of computer science. In summary, the domains are quite divided on the definition of CPS and IoT, making a unified definition even more important.

7. Developing a common understanding of IoT and CPS

After comparing the most frequent words used in statements on IoT and CPS, we now analyze which important terms capture the essence of each concept. This helps to better distinguish the concepts and to derive a more precise definition. These terms are derived from the discussion of the clusters and the analysis of word frequencies. So, not all terms discussed in the following occur in Fig. 6. We now explain the terms and clarify their usage in the statements. Table 2 summarizes whether the respective terms should be used in a refined definition for IoT and/or CPS. Section 7.1 proposes new refined definitions for both terms reflecting the core intuition of the terms. Those definitions reflect the results of our literature study and analysis. Section 7.2 presents the relation of IoT and CPS to the terms Information Technology (IT) and Information and Communication Technology (ICT) for better differentiating those concepts. Section 7.3 discusses the usage of the new definitions based on three typical use cases for the

terms. This helps to show the interplay of IoT and CPS in real and relevant scenarios. Finally, Section 7.4 delineates IoT and CPS from other related terms such as Industry 4.0, Industrial Internet, and Pervasive and Ubiquitous Computing.

Communication via a network. The first term we identified is communication via a network. It implies that any type of data can be transferred via a network. This could be monitoring data or data used for identification or triggering actions. The communication takes place over the Internet or any other network. This property can be found in most statements for both CPS and IoT, and therefore, it should be explicitly stated in a refined definition of these terms.

Integration of virtual and physical world. The second term we identified is the integration of the virtual and the physical world. This means that the monitored data from the physical world is transferred to the virtual world. In the virtual world, it is used to analyze the system and eventually plan corresponding actions to optimize the physical system. This term is only used in the CPS context as, the analyzed IoT statements do not cover this aspect.

Computation/process. Our analysis of the definitions shows that the terms computation and process are very important for CPS. These terms mean that normally a more complex algorithm is applied on the monitored data. The algorithm evaluates the system states and analyzes possible actions to improve the performance of the system. These terms are the main part of the virtual component in CPS statements and, hence, they play an important role in the differentiation between IoT and CPS. Accordingly, they should be included in a refined CPS definition. In contrast, a refined IoT definition should not include these terms as, according to the analyzed statements, complex computations are not necessarily applied in IoT use cases.

Control. Control is the logical consequence of the terms computation and process. The control of the physical system is required to realize the recommended actions determined as part of the computation and process activities. Here, these actions are sent to the physical system and it adapts according to the received instructions. With this, the virtual component controls the physical component. Similarly to the terms computation and process, the term control is only found in CPS statements and, hence, we will only use it in our refined CPS definition.

Identification/interaction. The next terms are identification and interaction. Identification means that the entities can identify themselves against other entities or a central unit. While identification is an action of the entity that sends information to other entities, interaction is a bidirectional action. Here, information is sent from one entity to another and back. This means that the entities can exchange information about their state and cooperate to achieve a global goal. In IoT, identification and interaction are fundamental terms and should be included in the definition. In CPS statements, the identification and interaction are not stated explicitly, but are in general assumed implicitly, as these functionalities are required for communication via a network.

Environment. The environment is a very important term in IoT statements. Authors describe with environment that the systems not only interact with each other but also with the surroundings of the system, e.g., the user. This means that the entities can sense the environment and can act according to the gathered data. As the environment plays an important role in IoT statements, it should be included in the refined definition. In contrast, when looking at the CPS statements, the environment is not stated explicitly and therefore, this term should not be mentioned explicitly in the proposed definition.

Table 2
Important terms for definitions of IoT and CPS.

Term	IoT	CPS
Communication via a network	Yes	Yes
Integration of virtual and physical world	No	Yes
Computation/process	No	Yes
Control	No	Yes
Identification/interaction	Yes	No
Environment	Yes	No

7.1. Refined Definitions of IoT and CPS

Now that we analyzed the key terms that capture the essential features of IoT and CPS, we propose new refined definitions for IoT and CPS that reflect the core intuition of the terms as seen in their statements provided by researchers from academia and industry. We aim for a clear demarcation of the two terms.

IoT. *The Internet of Things (IoT) consists of physical entities (things) that were not necessarily intended for communication with each other and with the environment. In IoT, these things are able to identify themselves, communicate, and interact via a network, based on Internet technologies. They can act depending on external triggers or local logic.*

CPS. *CPS are systems consisting of tightly integrated physical and cyber components interconnected through one or more networks. The cyber components consist of computing and communication facilities (local or remote, e.g., embedded systems or cloud services) used for monitoring, automating and controlling physical systems and processes. CPS are normally based on complex feedback and control loops, where the physical components affect the cyber components and vice versa.*

7.2. Delineation of IoT and CPS from Information Technology and Information and Communication Technology

After the presentation of the refined definitions for IoT and CPS in the previous section, we now present the relation to the historically older terms *IT* and *ICT*. Fig. 8 visualizes the development of IoT and CPS with regards to their technical basis terms IT and ICT.

The oldest concept is Information Technology (IT). IT is based on the use of general purpose computing systems and includes anything related to computing technology.[3] Besides others, this includes hardware and embedded systems, software, networking, or the Internet. So, IT is the basis for all computing systems and technologies that were developed later.

The invention of the network technology (and first prototypes of the Internet) created a new category of computing systems: ICT. In addition to the technology on which IT is referred, ICT adds the possibility to access information via telecommunication and is focused on communication technologies. The Internet, wireless networks, and mobile phones are used in this area.

IoT is developed using both technologies as basis and starts connecting physical entities that were not intended for communication with each other and the environment. Additional sensors and actuators enable them to sense their environment and act accordingly. These entities can identify themselves and interact with each other. As also used by IT and ICT, the communication is based on Internet technology.

Finally, according to our analysis of the use of the terms IoT and CPS, one can conclude that CPS is based on IoT. It refers to the

[3] https://techterms.com/definition/it accessed: October 2022.

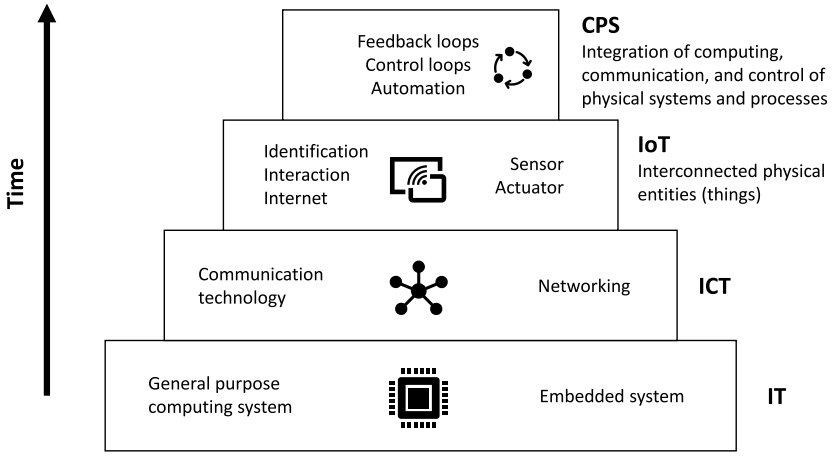

Fig. 8. Visualization of the technological development from IT to CPS.

integration of computing, communication, and control of physical systems and processes. It integrates feedback and control loops to enable the physical components to affect the cyber components and vice versa. According to our analysis, another important property of CPS is the ability to automate the complete process in which they are deployed.

7.3. Use case discussion

In the following, the proposed definitions of IoT and CPS are discussed by considering typical use cases for IoT and CPS that are available in literature to illustrate that IoT and CPS inherently belong together and cannot always be clearly distinguished. Further, the use cases show how the new definitions help to better understand the type of technical support delivered by IoT and CPS within many different use case scenarios. We look at three use cases: one that can be classified as IoT, one as CPS, and one where the classification is not as clear as in the other use cases.

An example of a system that is classified as IoT, regarding the introduced definitions, is the smart home. Smart devices at home, such as heating or shutters, can be seen as IoT devices, as they are distributed entities that were not built originally with the intention to communicate. In a smart home, such devices can now communicate via a network, identify themselves, and interact with the environment. They may also have built-in sensors that monitor the environment. Based on instructions received from users (e.g., the residents of the house), the monitoring information can be used in a local logic to control, e.g., the temperature in a room or the solar irradiation. So, the important aspects for IoT – communication via a network, identification/interaction, and monitoring of the environment – are satisfied, and therefore, the system can be classified as IoT. With regards to the proposed definitions in this paper, smart home cannot be classified as CPS, as there are no complex feedback and control loops where physical components affect the cyber components and vice versa.

An example that is classified as CPS, regarding the introduced definitions, is a multi-purpose assembly robot. This intelligent robot may be used in a production line where it receives working pieces from previous robots or machines. The robot is equipped with different sensors, for example, an optical sensor used to identify the work piece. The robot communicates with the central station, for example, via an intranet, and requests the tasks for every identified work piece. The central station uses the received information and knowledge of the work piece to calculate the next tasks and sends them to the robot. The robot receives the tasks, executes them with its multi-purpose tools and sends feedback about its state and the state of the processed work piece to the central station. If the central station decides that the tasks are executed correctly, it transfers a command to send the work piece to the next machine. This system, including both the robot and the central station, can be classified as CPS, as it exhibits all important properties discussed earlier. The robot communicates with the central station via a network; it integrates the virtual and the physical world, as computation is run on the central station and used to control the robot. According to the above proposed definitions this example is not only an IoT system, as it integrates the cyber and virtual components and uses complex feedback loops and logic to determine the next tasks.

One example that cannot be classified clearly as CPS or IoT can be found in the domain of intelligent transportation systems. Connected vehicles exchange information, such as environmental conditions or the traffic status. However, the vehicles do not necessarily autonomously react on such information, hence, it is part of the IoT. Still, the car can identify itself against other cars and can monitor and interact with the environment. Contrary, the self-driving car can drive on its own. Such a car is composed of several physical entities that monitor the current states and send them to a central control unit in the car. Information exchange through direct communication with other vehicles is optional. The control unit computes and processes this data and controls, e.g., the breaking and steering behavior. Therefore, a connection between the virtual and the physical world is present and the vehicle actively controls this connection. Based on this view, the self-driving car can be classified as CPS. As we have seen in the example of intelligent transportation systems the functionalities of a system must be analyzed in detail to decide whether it is part of the IoT or can be classified as CPS.

7.4. Delineation of related terms

In the previous sections, we used the results of our literature review to derive refined definitions for CPS and IoT, capturing the core elements of these terms as they are used in practice. In this section, we extend the analysis to the other terms mentioned in the beginning of the paper: Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing. The following discussion addresses the third research question from Section 1 on how to distinguish the terms from each other.

Industry 4.0 and Industrial Internet. The German "Plattform Industrie 4.0" supported by the German government defines Industry 4.0 as follows:

> Industry 4.0 refers to the intelligent networking of machines and processes in the industry with the aid of information and communication technology. Anon (2022u)

Similar to the definition of Industry 4.0, A.-R. Sadeghi et al. define the Industrial Internet as:

> Industrial Internet means to integrate more sophisticated electronics into production systems, interconnect them, and to integrate into conventional business IT system. Sadeghi et al. (2015)

The above definitions are quite similar as they both stress the interconnection of physical machines and production processes in industry. The interconnectivity allows to improve communication in both directions, from machines to automation systems and vice versa. Based on this, Cyber-physical Production Systems (CPPS) (Monostori, 2014) have emerged as a special type of CPS. In the context of CPPS, special focus is given to *digital twins*, which are the virtual representations of objects in the physical world. The digital twins are necessary to enable advanced automation and control of machines and production processes.

The concepts Industry 4.0 and Industrial Internet integrate most of the properties present in our refined definitions for CPS and IoT. However, Industry 4.0 applies the concepts of CPS and IoT in a production system context (Kagermann et al., 2011). It introduces adaptive factoring approaches where, e.g., the product defines its next steps in the factoring process. The Industrial Internet, on the other hand, is mainly the application of IoT and CPS in an industrial context as the self-management of machines seems to play a less prominent role.

Pervasive and Ubiquitous Computing. As mentioned in Section 2, based on a literature review, D. Ronzani concluded that Ubiquitous Computing is typically used in the sense of *anywhere* and *at any time*, whereas Pervasive Computing is used more in the sense of networking. Similarly, I. Horvath et al. distinguish the two terms as follows:

> [Ubiquitous Computing] is used when the emphasis is put on the opportunity of humans to have access to computing and to use multiple computing devices from anywhere, any time, and in any form, also nomadically, while [Pervasive Computing] is used to express that computing is (invisibly) embedded in everything in an all-embracing connectivity. Horváth and Vroom (2015)

All statements and definitions presented in this paper have several characteristics in common. First of all, the traditional computer is no longer considered as the only device for computation. The computer vanishes and computation takes place on entities that are not recognizable as traditional computers. Second, the omnipresence of these entities leads to an omnipresence of computation/computing. Lastly, especially in the context of Pervasive Computing, these entities are connected with each other but also with humans.

Taking these considerations into account, we can observe different characteristics of our refined definitions for CPS and IoT in the domain of Pervasive and Ubiquitous Computing.

The integration of computation into entities represents the computation aspect of CPS. These entities might perform extensive computations to enable a smooth user experience in changing environments through adaptation, which renders them similar to CPS according to our definition.

The required context-awareness implies a model of the environment and the system resources. On the other hand, some use cases – such as smart peer groups – integrate various connected things with limited computing power. As these things perform simple computations (basic reaction on events), they better fit our IoT definition. In general, Pervasive and Ubiquitous Computing neither belong to IoT or CPS, nor the other way round. One can say, that pervasive or ubiquitous systems are composed of interconnected and interacting entities and therefore, IoT can be seen as enabling technology for these terms.

8. Threats to validity

We applied a literature review as recommended by Webster and Watson. We analyzed the collected statements on IoT and CPS and carefully formulated refined definitions based on the practical usage of these terms. Nonetheless, the results may be slightly biased due to the manual steps of our methodology. For example, the grouping of words and the clustering process might introduce a subjective bias of the researchers. However, we try to minimize the risk of such effects as always several researches confirmed the grouping of words. In addition, there could be a slight bias towards publications from Germany as we only considered sources in English or German language. As the statements extracted from web pages did not pass a review process, these might be biased towards the web page editors. We are aware of the fact that some formulations allow different interpretations and the actual meaning of the statements as intended by their authors cannot be verified. Additionally, it might be feasible that statements have a domain-specific meaning. We did not include the specifics of the domain from which a statement roots, as we focused on a cross-case analysis. This might be an interesting aspect for future work. Finally, given that there are many different perspectives on the terms, what appears to be a contradiction might simply be a different view on the same concept, in some cases.

As a proceeding step, it might be feasible to perform a validating survey with employees in industry to analyze their accordance with the derived definitions. This might also offer the chance for a domain-specific analysis of the found statements and the derived definitions.

9. Conclusion

In the past three decades, many concepts such as CPS, IoT, Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing emerged and became highly-used buzzwords. However, often these terms are either used interchangeably or used in an inconsistent and contradicting manner. So, the question arises whether the existence of all these terms is justified. In this paper, we looked at the origin of these concepts and discussed their initial intention as well as their practical use today. We then focused on IoT and CPS for which we did a literature review extracting 98 statements on these terms. The statements were classified into four clusters for IoT statements and four clusters for CPS statements. We identified the most important terms for defining both concepts and proposed two refined definitions reflecting the core intuition of the terms as found in the literature while providing a clear delineation.

The basis for both concepts is the communication via a network. In IoT, the communicating entities can identify themselves and interact with each other and with the environment. The most critical difference between IoT and CPS is that CPS assume the integration of the cyber and physical world. This means that the cyber components of the system analyze the data monitored

Table A.3
Found and identified 108 statements.

Source	Statement
Danielis et al. (2014)	"CPS are systems with embedded software as part of, e.g., manufacturing facilities but can also comprise buildings and devices, which collect physical data by means of sensors and influence physical processes with actors."
Lee (2008b)	"Cyber-Physical Systems 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."
Rajkumar et al. (2010)	"Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core."
Monostori (2014)	"Cyber-Physical Systems (CPS) are systems of collaborating computational entities which are in intensive connection with the surrounding physical world and its on-going processes, providing and using, at the same time, data-accessing and data-processing services available on the internet."
Mousavi and Berger (2015)	"Cyber physical systems combine computing and networking power with physical components."
Reinheimer and Strahringer (2014)	"[...] in cyber–physical systems, sensors and actuators in technical devices are in charge of fusing the physical world with the virtual world."
Nuzzo (2015)	"A cyber–physical system is a system that combines physical and computer or cyber components."
Dai et al. (2015)	"Cyber-physical systems (CPS) are engineering systems that integrate computational, communication, and control elements with the physical dynamics of the system."
Tripakis (2015)	"Systems where the physical subsystem is tightly integrated with the cyber subsystem are usually referred to as cyber–physical systems (CPS)."
Yao et al. (2015)	"[...] cyber–physical systems (CPS) integrate cyber parts (the computer or computers in the system), physical parts [...], and various other interfacing and connecting components (sensors, actuators, networks)."
Estevez et al. (2015)	"[...] These are systems that still interact with the physical world and perform specific tasks, as embedded systems do, but are much more versatile and powerful in terms of processing capabilities. Cyber-physical systems are able to communicate within an intranet, but are not necessarily connected to the Internet."
Magaia et al. (2015)	"[...] a cyber–physical system is typically designed as a network of physically distributed embedded sensor and actuator devices equipped with computing and communicating capabilities to process and react to stimuli from the physical world and make decisions that also impact the physical world."
Zhang (2015)	"The primary concept of cyber–physical systems is to integrate computing (sensing, analyzing, predicting, understanding), communication (interaction, intervene, interface management), and control (inter-operate, evolve, evidence-based certification) together to make intelligent and autonomous systems."
Rawat and Khanna (2015)	"A cyber–physical system integrates computing, communication, and storage capabilities along with monitoring and controlling the entities of the physical world."
Adhikari et al. (2015)	"Cyber-physical systems (CPS) interconnect the cyber world and the physical world by embedding sensors and computational nodes."
Sehgal et al. (2014)	"Cyber Physical Systems (CPS) are fusion of cyber world and physical world."
Ara et al. (2015)	"Cyber Physical Systems are large scaled, closely integrated and resource constrained, collection of distributed cyber and physical systems respectively. In CPS, the physical systems and its processes are monitored, coordinated and controlled by the computation and communication cores."
Wang et al. (2015)	"CPS can be characterised as a thematic subject as opposed to a disciplinary topic."
Cardenas et al. (2008)	"Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world."
Tan et al. (2008)	"Cyber-Physical Systems are a next-generation networkconnected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws."
Pasqualetti et al. (2013)	"Cyber Physical systems integrate physical processes, computational resources, and communication capabilities."
Kim and Kumar (2012)	"CPSs refer to the next generation of engineered systems that require tight integration of computing, communication, and control technologies to achieve stability, performance, reliability, robustness, and efficiency in dealing with physical systems of many application domains."
Tan et al. (2009)	"CPS is envisioned to be a heterogeneous system of systems, which consists of computing devices and embedded systems including distributed sensors and actuators."
Baheti and Gill (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."
Atzori et al. (2010)	"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, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals."
Haller et al. (2008)	"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."
Kelly et al. (2013)	"'Internet of Things (IoT)' is all about physical items talking to each other, machine-to-machine communications and person-to-computer communications will be extended to 'things'."
Sundmaeker et al. (2010a)	"Internet of Things (IoT) is an integrated part of Future Internet and could be defined 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 and use intelligent interfaces, and are seamlessly integrated into the information network."
Zhu et al. (2010)	"The Internet of Things is regarded as the third wave of information technology after Internet and mobile communication network, which is characterized by more thorough sense and measure, more comprehensive interoperability and intelligence."
Gubbi et al. (2013)	"Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications."
Lee and Lee (2015)	"The Internet of Things (IoT), also called the Internet of Everything or the Industrial Internet, is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other."
Sanchez et al. (2014)	"The Internet of Things refers to a virtual representation of a broad variety of objects on the Internet and their integration into Internet or Web based systems and services. Based on interaction and communication interfaces such as RFID, NFC, barcodes or 2D codes they expose information, features and functionalities which can be integrated into systems and services."
Uckelmann et al. (2011)	"The Internet of Things is a concept in which the virtual world of information technology integrates seamlessly with the real world of things."

(*continued on next page*)

Table A.3 (*continued*).

Source	Statement
Miorandi et al. (2012)	"IoT builds on three pillars, related to the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) to communicate (anything communicates) and (iii) to interact (anything interacts)– either among themselves, building networks of interconnected objects, or with end-users or other entities in the network."
Gillis (2022w)	"A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low – or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network."
Anon (2019b)	"The term 'internet of things' describes the increasing interconnectedness of intelligent objects among each other as well as to the internet. Various objects, everyday objects or machines are equipped with processsors and embedded sensors, to have the ability to communicate with each other via the IP network."
Innovations, Bosch Software (2022)	"The physical essence of the Internet of Things (IoT) is billions of connected devices providing data – in many cases in real-time – and sending it back to businesses that can remotely and automatically control this physical infrastructure."
Anon (2022j)	"The internet of things is a network of physical entities - vehicles, machines, home appliances or other items - that are, equipped with sensors and APIs, connected to the internet and exchange data."
Anon (2022d)	"Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components."
Anon (2022a)	"The Internet of Things (IoT) is a term coined by Kevin Ashton, a British technology pioneer working on radio-frequency identification (RFID) who conceived a system of ubiquitous sensors connecting the physical world to the Internet."
Anon (2022i)	"The Internet of Things (IoT) is a robust network of devices, all embedded with electronics, software, and sensors that enable them to exchange and analyze data. The IoT has been transforming the way we live for nearly two decades, paving the way for responsive solutions, innovative products, efficient manufacturing, and ultimately, amazing new ways to do business."
Anon (2022g)	"A 'thing' is any object with embedded electronics that can transfer data over a network — without any human interaction."
Anon (2022f)	"The internet of things offers new possibilities for improving efficiency, customer relationship and development of new business opportunities using better insights at the intelligent edge."
Anon (2022p)	"While the early focus of IoT has been on consumer-driven use cases such as internet gadgets, smartwatches, and connected cars, enterprise verticals such as manufacturing, transportation and logistics, healthcare, and utilities will see a bigger and faster return on investment from IoT."
Anon (2022e)	"Cyber-physical systems are systems, where data processing, software and mechanical components are interconnected, and data transfer, data exchange as well as monitoring and control are executed via a network, e.g. the internet, in real-time."
Henkel (2022b)	"Cyber-physical systems are the technological basis for many innovations. They combine IT with the physical world and play an ever more important role in areas such as automotive, avionics, transport, energy, production, health, infrastructure, and entertainment."
Anon (2019a)	"Based on the concept of Internet of things describe cyber physical systems (CPS) the coupling of physical, biological and or structurally engineered components, that are integrated, monitored and or controlled using a processing unit."
Beetz (2010)	"Cyber-physical systems, are the interaction of local information, data processing and large systems that asses this information. This is used as a basis to execute tasks efficiently, self-sufficiently and autonomous: control, regulation, monitoring, communication or signal processing."
Anon (2018)	"Cyber-physical systems, or CPS for short, are sophisticated computer devices that work together to perform functions, control physical elements, and respond to human control."
Anon (2022q)	"Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, and electric power generation and delivery, as well as in many other areas now just being envisioned."
Anon (2022r)	"Robots and other complex cyber–physical systems (CPS) sense, process, and react to information from the physical world."
Anon (2013)	"Cyber-physical systems represent the connection of physical and data processing point of view and arise by a complex interaction of embedded systems, application systems and infrastructures via the internet of things based on their interconnectedness, integration, human-machine-interaction in application processes and communication channels."
Anon (2022b)	"Cyber-physical systems can be identified by their connection of real world (physical) entities and processes with data processing (virtual) objects and processes via open, partly global and always interconnected information networks."
Lee (2008a)	"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."
Anon (2022h)	"Cyber-physical systems (CPS) are systems with embedded software and electronic systems, that are connected to the outside world through sensors and actuators (machine actuators). Increasingly, they are interconnected and connected to the internet. With the use of sensors, these systems process data from the physical (natural) world and make them available for network based services, that can influence processes of the physical world directly through their actuators."
Vogel Communications Group GmbH & Co. K.G. (2017)	"Cyber-physical systems, often shortened CPS, consist of mechanical components, software and modern communication technology. complex infrastructures can be controlled, managed and monitored using the interconnection of single components through networks, e.g. the internet. The exchange of informations of the interconnected entities and systems can be realized in real-time wireless or tethered."
Anon (2022o)	"The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."
Anon (2022s)	"[…] a network of everyday devices, appliances, and other objects equipped with computer chips and sensors that can collect and transmit data through the Internet."
Anon (2022)	"[..] a network of objects that are fitted with microchips and connected to the internet, enabling them to interact with each other and to be controlled remotely."
Anon (2022n)	"[…] connections between objects of all kinds via the internet that enable them to communicate with people and with each other."
Khaitan and McCalley (2015)	"CPSs are defined as the systems that offer integrations of computation, networking, and physical processes [2]– [3] [4] [5] or, in other words, as the systems where physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context [6]."
Sundmaeker et al. (2010b)	"The Internet of Things links the objects of the real world with the virtual world, thus enabling anytime, any place connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time."
Anon (2011b)	"The basic idea is that IoT will connect objects around us (electronic, electrical, non electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoT which interact and co-operate each other to make the service better and accessible anytime, from anywhere."

(*continued on next page*)

Table A.3 (*continued*).

Source	Statement
Mattern and Floerkemeier (2010a)	"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."
Ganji et al. (2010)	"IoT can be understood as an enabling framework for the interaction between a bundle of heterogeneous objects and also as a convergence of technologies."
Anon (2011a)	"It means that any physical thing can become a computer that is connected to the Internet and to other things. IoT is formed by numerous different connections between PCs, human to human, human to thing and between things. This creates a self-configuring network that is much more complex and dynamic than the conventional Internet. Data about things is collected and processed with very small computers (mostly RFID tags) that are connected to more powerful computers through networks."
Evans (2011)	"IoT is simply the point in time when more 'things or objects' were connected to the Internet than people."
Rellermeyer et al. (2008)	"The notion of an 'Internet of Things' refers to the possibility of endowing everyday objects with the ability to identify themselves, communicate with other ob-jects, and possibly compute."
Anon (2012a)	"The Internet of Things refers to a virtual representation of a broad variety of objects on the Internet and their integration into Internet or Web based systems and services. Based on interaction and commuication interfaces such as RFID, NFC, barcodes or 2D codes they expose information, features and functionalities which can be integrated into systems and services."
Easterling (2012a)	"An 'internet of things' describes a world embedded with so many digital devices that the space between them consists not of dark circuitry but rather the space of the city itself. The computer has escaped the box, and ordinary objects in space are carriers of digital signals."
Talbot (2011)	"At the core of this evolution of the Internet is the idea that the Internet becomes more sensory — more proactive and less reactive. It also takes into account that the world has hit a point where there are more devices connecting to the Internet than people doing so."
Anon (2012b)	"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."
Shelby and Bormann (2011)	"Encompasses all the embedded devices and networks that are natively IP-enabled and Internet-connected, along with the Internet services monitoring and controlling those devices."
Rose et al. (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."
Winter (2015)	"Although there is no single definition for the Internet of Things, competing visions agree that it relates to the integration of the physical world with the virtual world – with any object having the potential to be connected to the Internet via short-range wireless technologies, such as radio frequency identification (RFID), near field communication (NFC), or wireless sensor networks (WSNs). This merging of the physical and virtual worlds is intended to increase instrumentation, tracking, and measurement of both natural and social processes"
Huberman (2016)	"Industrial Internet of Things (IOT) is a distributed network of smart sensors that enables precise control and monitoring of complex processes over arbitrary distances."
Farash et al. (2016)	"The concept of Internet of Things (IOT) […] is that every object in the Internet infrastructure is interconnected into a global dynamic expanding network."
Voas (2016)	"In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet."
Makhoul et al. (2015)	"The main idea behind the IoT is to bridge the gap between the physical world of humans and the virtual world of electronics via smart objects. These smart objects allow the interactions between humans and their environment by providing, processing, and delivering any sort of information or command. Sensors and actuators will be integrated in buildings, vehicles, and common environments and can tell us about them, their state, or their surroundings."
Jammes (2016)	"We must first define what we mean by 'things.' It could be very simple objects or complex objects. Things do not need to be connected directly to the public Internet, but they must be connectable via a network (which could be a LAN, PAN, body area network, etc.). The IoT is the network of physical objects that contain embedded technology to communicate and interact with the external environment. The IoT encompasses hardware (the 'things' themselves), embedded software (software running on, and enabling, the connected capabilities of the things), connectivity/communications services, and information services associated with the things (including services based on analysis of usage patterns and sensor or actuator data). An IoT solution is a product (or set of products) combined with a service either a one-to-one or a one-to-many relation. Meaning one service is combined with one (set of) product(s), or one service is combined with multiple (sets of) products."
Delic (2016)	"At the very high level of abstraction, the Internet of Things (IoT) can be modeled as the hyper-scale, hyper-complex cyber–physical system."
Botta et al. (2016)	"The Internet of Things (IoT) paradigm is based on intelligent and self-configuring nodes (things) interconnected in a dynamic and global network infrastructure."
Qin et al. (2016)	"The Internet of Things (IoT) […] connecting everyday objects to the Internet and facilitating machine-to-human and machine-to-machine communication with the physical world."
Fjäder (2016)	"Whilst the definition of 'Internet of Things' is elusive in general, the use of the term refers to the use of sensors and data communications technology built into physical objects in order to track, coordinate or control the functioning of those objects based on data over the network or the Internet."
Silva and Analide (2016)	"The internet of things is a new paradigm in which every device is digitally connected, regardless of their function, and can communicate with other devices and people over communication protocols."
Minnick (2016)	"The Internet of Things is a term used to describe the ever-growing number of devices connecting to a network, including televisions and appliances."
Taplin (2016)	"[…] the interconnectness of all systems through the internet [is known as] 'the internet of things'."
Yachir et al. (2016)	"The Internet of Things (IoT) envisions a world where smart objects connected to the Internet, share their data, exchange their services and cooperate together to provide value-added services that none of these objects could provide individually."
Lee (2016)	"Although many standardization groups such as IEEE, ITU, 3GPP, and IETF have presented various definitions, in its broadest sense, Internet of the Things means 'technology through which additional values can be provided to users by linking things or devices to the Internet.'"

(*continued on next page*)

Table A.3 (*continued*).

Source	Statement
Anon (2014a)	"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."
Anon (2022l)	"[…] 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."
Cosgrove-Sacks (2014)	"System where the Internet is connected to the physical world via ubiquitous sensors."
Anon (2015)	"The Web of Things includes sensors and actuators, physical objects and locations, and even people. The Web of Things is essentially about the role of Web technologies to facilitate the development of applications and services for things and their virtual representation. Some relevant Web technologies include HTTP for accessing RESTful services, and for naming objects as a basis for linked data and rich descriptions, and JavaScript APIs for virtual objects acting as proxies for real-world objects."
Anon (2020a)	"The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer–based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber–physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020."
Anon (2022k)	"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."
Anon (2022m)	"The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. IoT Extends Internet Connectivity: The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet."
Anon (2020c)	"The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes. The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to you, but is now connected to surrounding objects and database data. When many objects act in unison, they are known as having 'ambient intelligence.'"
Minerva et al.	"The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones make it possible to materialize IoTwhich interact and co-operate each other to make the service better and accessible anytime, from anywhere."
Anon (2022c)	"Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components."
Anon (2017b)	"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."
Anon (2017a)	"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)."
Koç (2018)	"A cyber–physical system is a complex set of systems and subsystems requiring communication channels among the cooperative entities and tasks, for example, a coordinated platoon of interconnected vehicles or a countrywide power system of different generating and consuming plants."
Chandler and Munday (2020)	"Internet of things: The embedding of computer hardware and software into everyday objects which can then be organized into a virtual network of 'terminals', providing configurable information about their status and location, remotely controlling or being controlled by smartphones and computers. The term was proposed by Kevin Ashton in 1999. The ubiquity and low cost of microprocessors have led increasingly to their incorporation into a range of everyday objects."
Anon (2020b)	"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."
Ranger (2020)	"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."
Gorse et al. (2020)	"Internet of Things (IoT): A system of interrelated computing devices, machines, objects, etc. that have the ability to transmit data over a network without the need for human intervention."
Ince (2019)	"Internet of Things: A term used to describe the collection of computer-based objects that can be controlled by the user and which are connected to the Internet. Often the collection is associated with the home. Examples include: intelligent coffee makers, smart clothing, smart electrical switches, and burglar alarms."
Hassan (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."

from the physical components by using complex algorithms. The results of the algorithms are actions to control and optimize the behavior of the physical entities. We illustrated this understanding of CPS and IoT by presenting several use cases where a clear classification can be done and one use case where the classification depends on the system model. Finally, we returned to the terms Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing and differentiated them from the concepts of IoT and CPS. In this paper, we focused on IoT and CPS and showed that the terms are sometimes used interchangeably. With our revised definitions, based on the literature review results, we try to distinguish the concepts better as understood by most definitions. Widening the scope by also integrating the other terms – Industry 4.0, Industrial Internet, Pervasive Computing, and Ubiquitous Computing – will be part of future work.

As future work, it might be interesting to perform a validating study with employees from industry to analyze their understanding of IoT and CPS in more detail. Further, this could validate our results or sharpen them.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix. Extracted and analyzed statements

Table A.3 shows all statements that have been extracted and analyzed during the literature review.

References

Adhikari, M., Kar, S., Banerjee, S., Biswas, U., 2015. Big Data Analysis for Cyber-Physical Systems. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 493–525.

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M., 2020. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Commun. Surv. Tutor. 22 (3), 1646–1685. http://dx.doi.org/10.1109/COMST.2020.2988293.

Anon, 2011a. Future Internet. URL http://www.svegritet.se/emergin-technologies/future-internet/, (Accessed 30 May 2022).

Anon, 2011b. Internet Task Force. URL https://datatracker.ietf.org/doc/html/draft-lee-iot-problem-statement-00%20Internet%20Research%20Task%20Force%22, (Accessed 30 May 2022).

Anon, 2012a. Internet of Things - Research and Development Working Group Wiki. URL https://www.w3.org/WAI/RD/wiki/Internet_of_Things, (Accessed 30 May 2022).

Anon, 2012b. Internet of Things Defined - Tech Definitions by Gartner. Gartner IT Glossary URL https://www.gartner.com/en/information-technology/glossary/internet-of-things, (Accessed 30 May 2022).

Anon, 2012c. The third industrial revolution. The Economist URL https://www.economist.com/leaders/2012/04/21/the-third-industrial-revolution, (Accessed 30 May 2022).

Anon, 2013. Cyber-Physical Systems - Fraunhofer FIT. (Accessed 30 May 2022),

Anon, 2014a. IERC-European Research Cluster on the Internet of Things. URL http://www.internet-of-things-research.eu/about_iot.htm, (Accessed 30 May 2022).

Anon, 2015. Web of Things Community Group. URL https://www.w3.org/community/wot/wiki/Main_Page, (Accessed 30 May 2022).

Anon, 2016. Internet of things: At a glance. (Tech. Rep. c45-73147-01), Cisco, URL http://www.audentia-gestion.fr/cisco/pdf/at-a-glance-c45-731471.pdf.

Anon, 2017a. ACM Transactions on Cyber-Physical Systems. URL https://dl.acm.org/journal/tcps/about (Accessed 30 May 2022).

Anon, 2017b. IEEE Technical Committee on Cyber-Physical Systems (CPS). URL http://www.ieee-cps.org/index.html, (Accessed 30 May 2022).

Anon, 2018. Cyber-physical systems that allow devices to interact and communicate. IBM Blog Research URL https://www.ibm.com/blogs/research/2018/01/designing-cyber-physical-systems, (Accessed 30 May 2022).

Anon, 2019a. Cyber-physische Systeme – Enzyklopaedie der Wirtschaftsinformatik. URL https://wi-lex.de/index.php/lexikon/inner-und-ueberbetriebliche-informationssysteme/sektorspezifische-anwendungssysteme/cyber-physische-systeme, (Accessed 30 May 2022).

Anon, 2019b. Internet of Things Definition. GrÜnderszene Magazin URL https://www.businessinsider.de/gruenderszene/lexikon/begriffe/internet-of-things/ (Accessed 30 May 2022).

Anon, 2020a. Internet of Things. URL https://en.wikipedia.org/wiki/Internet_of_Things, (Accessed 30 May 2022).

Anon, 2020b. The Internet of Things at the IETF. URL https://www.ietf.org/topics/iot/, (Accessed 30 May 2022).

Anon, 2020c. What is the Internet of Things (IoT)? - Definition from Techopedia. Techopedia.Com URL https://www.techopedia.com/definition/28247/internet-of-things-iot, (Accessed 30 May 2022).

Anon, 2022. The Internet of Things definition and meaning | Collins English Dictionary. URL https://www.collinsdictionary.com/dictionary/english/the-internet-of-things, (Accessed 30 May 2022).

Anon, 2022a. AWS IoT. URL https://aws.amazon.com/de/iot/, (Accessed 30 May 2022).

Anon, 2022b. Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation. URL https://www.plattform-i40.de/IP/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html (Accessed 30 May 2022).

Anon, 2022c. Cyber-Physical Systems (CPS). URL https://beta.nsf.gov/funding/opportunities/cyber-physical-systems-cps (Accessed 30 May 2022).

Anon, 2022d. Cyber-Physical Systems (CPS) (nsf15541) | NSF – National Science Foundation. URL https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm, (Accessed 30 May 2022).

Anon, 2022e. Definition: Cyber-physische Systeme. Gabler WirtschaftslexikonURL https://wirtschaftslexikon.gabler.de/definition/cyberphysische-systeme-54077, (Accessed 30 May 2022).

Anon, 2022f. HPE Lösungen für das Internet der Dinge. URL https://www.hpe.com/de/de/solutions/internet-of-things.html (Accessed 30 May 2022).

Anon, 2022g. IBM Watson Internet of Things (IoT). URL https://www.ibm.com/cloud/internet-of-things (Accessed 30 May 2022).

Anon, 2022h. Ideen 2020 - Ein Rundgang durch die Welt von morgen. URL https://www.helmholtz.de/ueber-uns/wer-wir-sind/presse-medien/ausstellungen/ideen-2020/, (Accessed 30 May 2022).

Anon, 2022i. Intelligent Decisions with Intel Internet of Things (IoT). URL https://www.intel.com/content/www/us/en/internet-of-things/overview.html?_ga=2.226146202.1475812677.1526389220-1750294542.1526389220, (Accessed 30 May 2022).

Anon, 2022j. Internet der Dinge | Industrie 4.0 | SAP. SAP URL https://www.sap.com/germany/insights/what-is-iot-internet-of-things.html, (Accessed 30 May 2022).

Anon, 2022k. Internet of Things. URL https://www.gartner.com/it-glossary/internet-of-things/ (Accessed 30 May 2022).

Anon, 2022l. Internet of Things Global Standards Initiative. URL https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx, (Accessed 30 May 2022).

Anon, 2022m. Internet of things (IoT) definition ˜ webopedia. URL https://www.webopedia.com/definitions/internet-of-things/, (Accessed 30 May 2022).

Anon, 2022n. Internet of Things (noun) definition and synonyms | Macmillan Dictionary. URL https://www.macmillandictionary.com/dictionary/british/internet-of-things, (Accessed 30 May 2022).

Anon, 2022o. Internet | Definition of Internet in English by Oxford Dictionaries. Oxford Dictionaries | English URL https://en.oxforddictionaries.com/definition/internet, (Accessed 30 May 2022).

Anon, 2022p. IoT at work. URL https://blogs.oracle.com/oraclemagazine/iot-at-work, (Accessed 30 May 2022).

Anon, 2022q. IoT Devices and Infrastructures Group. URL https://www.nist.gov/el/cyber-physical-systems, (Accessed 30 May 2022).

Anon, 2022r. Robotics and Cyber-Physical Systems | Computer Science Research at Max Planck Institutes. URL https://www.cis.mpg.de/robotics, (Accessed 30 May 2022).

Anon, 2022s. The definition of Internet of Things. www.dictionary.com URL https://www.dictionary.com/browse/internet-of-things, (Accessed 30 May 2022).

Anon, 2022u. Was ist Industrie 4.0?. URL https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html, (Accessed 30 May 2022).

Ara, A., Al-Rodhaan, M., Tian, Y., Al-Dhelaan, A., 2015. A secure service provisioning framework for cyber physical cloud computing systems. arXiv preprint arXiv:1611.00374.

Ashton, K., 2009. That 'Internet of Things' Thing. RFID J. URL https://www.rfidjournal.com/that-internet-of-things-thing, (Accessed 30 May 2022).

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: A survey. Comput. Netw. 54 (15), 2787–2805.

Baheti, R., Gill, H., 2011. Cyber-physical systems. Impact Control Technol. 12 (1), 161–166.

Beetz, K., 2010. Die Wirtschaftliche Bedeutung von Cyberphysical Systems aus der Sicht Eines Global Players. In: Cyber-Physical Systems. Springer, pp. 59–66.

BMBF-Internetredaktion, 2016. Industrie 4.0 - BMBF. Bundesministerium FÜR Bildung Und Forschung - BMBF URL https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html, (Accessed 30 May 2022).

Botta, A., De Donato, W., Persico, V., Pescapé, A., 2016. Integration of cloud computing and Internet of Things: a survey. Future Gener. Comput. Syst. 56, 684–700.

Cardenas, A.A., Amin, S., Sastry, S., 2008. Secure control: Towards survivable cyber-physical systems. In: 28th International Conference on Distributed Computing Systems Workshops, 2008. ICDCS'08.. IEEE, pp. 495–500.

Chandler, D., Munday, R., 2020. A Dictionary of Media and Communication. Oxford University Press.

Cosgrove-Sacks, C., 2014. Open Protocols for an open interoperable Internet of Things. URL https://www.oasis-open.org/presentations/open-protocols-and-internet-of-things-oasis.ppt, (Accessed 30 May 2022).

Dai, S., Lattmann, Z., Koutsoukos, X., 2015. Compositional Design of Cyber-Physical Systems Using Port-Hamiltonian Systems. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 33–60.

Danielis, P., Skodzik, J., Altmann, V., Schweissguth, E.B., Golatowski, F., Timmermann, D., Schacht, J., 2014. Survey on real-time communication via ethernet in industrial automation environments. In: Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA). pp. 1–8.

Data Bridge Market Research, 2020. Global Cyber-Physical Systems Market – Industry Trends and Forecast to 2028. URL https://www.databridgemarketresearch.com/reports/global-cyber-physical-systems-market, (Accessed 10. November 2022).

Delic, K.A., 2016. On resilience of IoT systems: The Internet of Things (ubiquity symposium). Ubiquity 2016 (February), 1.

Easterling, K., 2012a. An Internet of Things. URL https://www.e-flux.com/journal/31/68189/an-internet-of-things/, (Accessed 30 May 2022).

Estevez, C., Azurdia, C., Céspedes, S., 2015. The Internet of Interlaced Cyber-Physical Things. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 343–371.

Evans, D., 2011. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Tech. rep., CISCO, URL https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Fahmideh, M., Zowghi, D., 2020. An exploration of IoT platform development. Inf. Syst. 87, 101409. http://dx.doi.org/10.1016/j.is.2019.06.005.

Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Netw. 36, 152–176.

Fjäder, C.O., 2016. National security in a hyper-connected world. In: Exploring the Security Landscape: Non-Traditional Security Challenges. Springer, pp. 31–58.

Ganji, F., Kluge, E.M., Scholz-Reiter, B., 2010. Bringing agents into application: intelligent products in autonomous logistics. In: Artificial Intelligence and Logistics (AiLog)-Workshop At ECAI. pp. 37–42.

Gillis, A.S., 2022w. What is internet of things (IoT)? IoT Agenda URL https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT, (Accessed 30 May 2022).

Gorse, C., Johnston, D., Pritchard, M., 2020. A Dictionary of Construction, Surveying, and Civil Engineering. Oxford University Press.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 29 (7), 1645–1660.

Gürdür Broo, D., Boman, U., Törngren, M., 2021. Cyber-physical systems research and education in 2030: Scenarios and strategies. J. Ind. Inform. Integr. 21, 100192. http://dx.doi.org/10.1016/j.jii.2020.100192.

Haller, S., Karnouskos, S., Schroth, C., 2008. The internet of things in an enterprise context. In: Future Internet Symposium. Springer, pp. 14–28.

Hansmann, U., Merk, L., Nicklous, M.S., Stober, T., 2003. Pervasive computing: The mobile world. Springer Science & Business Media.

Hassan, Q.F., 2018. Internet of Things a to Z: Technologies and Applications. John Wiley & Sons.

Henkel, T., 2022b. Cyber-Physical-Systems. Fraunhofer SIT URL https://www.sit.fraunhofer.de/en/offers/fields-of-expertise/cyber-physical-systems, (Accessed 30 May 2022).

Horváth, I., Vroom, R.W., 2015. Ubiquitous computer aided design: A broken promise or a sleeping beauty? Comput. Aided Des. 59, 161–175.

Huberman, B.A., 2016. Ensuring Trust and Security in the Industrial IoT: The Internet of Things (Ubiquity symposium). Ubiquity 2016 (January), 2.

Ince, D., 2019. A Dictionary of the Internet. Oxford University Press.

Inderwildi, O., Zhang, C., Wang, X., Kraft, M., 2020. The impact of intelligent cyber-physical systems on the decarbonization of energy. Energy Environ. Sci. 13 (3), 744–771.

Innovations, Bosch Software, 2022. Was ist das Internet der Dinge? Bosch Software Innovations URL https://bosch-iot-suite.com/, (Accessed 30 May 2022).

Jammes, F., 2016. Internet of Things in Energy Efficiency: The Internet of Things (Ubiquity symposium). Ubiquity 2016 (February), 2.

Kagermann, H., Lukas, W.-D., Wahlster, W.,

Kelly, S.D.T., Suryadevara, N.K., Mukhopadhyay, S.C., 2013. towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sens. J. 13 (10), 3846–3853.

Khaitan, S.K., McCalley, J.D., 2015. Design techniques and applications of cyberphysical systems: A survey. IEEE Syst. J. 9 (2), 350–365.

Kim, K.-D., Kumar, P.R., 2012. Cyber–physical systems: A perspective at the centennial. Proc. IEEE 100, 1287–1308, Special Centennial Issue.

Koç, Ç.K., 2018. Cyber-Physical Systems Security. Springer.

Lee, E.A., 2008a. Cyber Physical Systems: Design Challenges. Tech. Rep. UCB/EECS-2008-8, EECS Department, University of California, Berkeley, URL http://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html.

Lee, E.A., 2008b. Cyber physical systems: Design challenges. In: 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing. ISORC, IEEE, pp. 363–369.

Lee, D.-W., 2016. A Study on Actual Cases & Meanings for Internet of Things. Int. J. Softw. Eng. Appl. 10 (1), 287–294.

Lee, I., Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horizons 58 (4), 431–440.

Lee, E.A., Seshia, S.A., 2017. Introduction to Embedded Systems - a Cyber-Physical Systems Approach. MIT Press.

Magaia, N., Pereira, P., Correia, M., 2015. Security in Delay-tolerant Mobile Cyber-Physical Applications. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 373–394.

Makhoul, A., Guyeux, C., Hakem, M., Bahi, J., 2015. Using an epidemiological approach to maximize data survival in the Internet of Things. ACM Trans. Internet Technol. 16 (1), 1–5.

Mattern, F., 2007. Was bedeuten pervasive und ubiquitous computing? Asut-Bulletin (4), 33.

Mattern, F., Floerkemeier, C., 2010a. From the Internet of Computers to the Internet of Things. In: From Active Data Management to Event-Based Systems and more. Springer, pp. 242–259.

Mattern, F., Floerkemeier, C., 2010b. Vom internet der computer zum internet der dinge. Informatik-Spektrum 33 (2), 107–121.

Minerva, R., Biru, A., Rotondi, D., Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative URL https://iot.ieee.org/definition.html, (Accessed 30 May 2022).

Minnick, J., 2016. Web Design with HTML & CSS3: Complete. Cengage Learning.

Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I., 2012. Internet of Things: Vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516.

Monostori, L., 2014. Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia Cirp 17, 9–13.

Mousavi, M.R., Berger, C., 2015. Cyber Physical Systems. Design, Modeling, and Evaluation: 5th International Workshop, CyPhy 2015, Amsterdam, the Netherlands, October 8, 2015, Proceedings, vol. 9361. Springer.

Nuzzo, P., 2015. Compositional design of cyber-physical systems using contracts (Ph.D. thesis). Ph. D. dissertation, EECS Department, University of California, Berkeley.

Palermo, F., 2014. Internet of Things Done Wrong Stifles Innovation - InformationWeek. InformationWeek URL https://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157, (Accessed 30 May 2022).

Pasqualetti, F., Dörfler, F., Bullo, F., 2013. Attack detection and identification in cyber-physical systems. IEEE Trans. Automat. Control 58 (11), 2715–2729.

Prith Banerjee, Accenture Technology Labs, 2014. Driving unconventional growth through the industrial internet of things. URL https://www.iot-inc.com/wp-content/uploads/2015/11/10-Prith.pdf, (Accessed 30 May 2022).

Qin, Y., Sheng, Q.Z., Falkner, N.J., Dustdar, S., Wang, H., Vasilakos, A.V., 2016. When things matter: A survey on data-centric Internet of Things. J. Netw. Comput. Appl. 64, 137–153.

Raji, R.S., 1994. Smart networks for control. IEEE Spectr. 31 (6), 49–55. http://dx.doi.org/10.1109/6.284793.

Rajkumar, R., Lee, I., Sha, L., Stankovic, J., 2010. Cyber-physical systems: the next computing revolution. In: Design Automation Conference (DAC), 2010 47th ACM/IEEE. IEEE, pp. 731–736.

Ranger, S., 2020. What is the IoT? Everything you need to know about the Internet of Things right now. URL https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/, (Accessed 30 May 2022).

Rathore, H., Mohamed, A., Guizani, M., 2020. A survey of blockchain enabled cyber-physical systems. Sensors 20 (1), 282.

Rawat, A., Khanna, A., 2015. Integration of the Cloud for Cyber-Physical Systems. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 473–492.

Reinheimer, S., Strahringer, S., 2014. Cyber-physical Systems–Von jeder mit jedem zu alles mit allem. Springer.
Rellermeyer, J.S., Duller, M., Gilmer, K., Maragkos, D., Papageorgiou, D., Alonso, G., 2008. The software fabric for the Internet of Things. In: The Internet of Things. Springer, pp. 87–104.
Ronzani, D., 2009. The battle of concepts: Ubiquitous computing, pervasive computing and ambient intelligence in mass media. Ubiquitous Comput. Commun. J. 4 (2), 9–19.
Rose, K., Eldridge, S., Chapin, L., 2015. The Internet of Things: An overview. Internet Soc. (ISOC) 1–50.
Sadeghi, A.-R., Wachsmann, C., Waidner, M., 2015. Security and privacy challenges in Industrial Internet of Things. In: 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015. IEEE, pp. 1–6.
Sanchez, L., Muñoz, L., Galache, J.A., Sotres, P., Santana, J.R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E., et al., 2014. SmartSantander: IoT experimentation over a smart city testbed. Comput. Netw. 61, 217–238.
Schoenberger, C.R., 2002. The Internet of Things. Forbes URL https://www.forbes.com/global/2002/0318/092.html#8caf27c3c3ef, (Accessed 30 May 2022).
Sehgal, V.K., Patrick, A., Rajpoot, L., 2014. A comparative study of cyber physical cloud, cloud of sensors and Internet of Things: Their ideology, similarities and differences. In: Advance Computing Conference (IACC), 2014 IEEE International. IEEE, pp. 708–716.
Serpanos, D., Wolf, T., 2011. Chapter 1 - Architecture of network systems overview. Archit. Netw. Syst. 1–9. http://dx.doi.org/10.1016/B978-0-12-374494-4.00001-3.
Shelby, Z., Bormann, C., 2011. 6LoWPAN: The Wireless Embedded Internet, vol. 43. John Wiley & Sons.
Silva, F., Analide, C., 2016. Sensorization to promote the well-being of people and the betterment of health organizations. In: Applying Business Intelligence to Clinical and Healthcare Organizations. IGI Global, pp. 116–135.
Sobin, C., 2020. A survey on architecture, protocols and challenges in IoT. Wirel. Pers. Commun. 112 (3), 1383–1429.
Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., 2010a. Vision and challenges for realising the Internet of Things. Clust. Eur. Res. Projects Internet Things Eur. Commision 3 (3), 34–36.
Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., 2010b. Vision and challenges for realising the internet of things. Cluster Eur. Res. Projects Internet Things Eur Commision 3 (3), 34–36.
Talbot, C., 2011. Cisco chief futurist: The Internet of Things is here. URL https://channelbuzz.ca/2011/05/cisco-chief-futurist-the-internet-of-things-is-here-1887/, (Accessed 30 May 2022).
Tan, Y., Goddard, S., Perez, L.C., 2008. A prototype architecture for cyber-physical systems. ACM Sigbed Rev. 5 (1), 26.
Tan, Y., Vuran, M.C., Goddard, S., 2009. Spatio-temporal event model for cyber-physical systems. In: Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on. IEEE, pp. 44–50.
Taplin, R., 2016. Risk management and cyber risk in the financial services sector: An overview. In: Managing Cyber Risk in the Financial Sector. Routledge, pp. 17–35.
Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., 2020. IoT privacy and security: Challenges and solutions. Appl. Sci. 10 (12), http://dx.doi.org/10.3390/app10124102, URL https://www.mdpi.com/2076-3417/10/12/4102.
Tripakis, S., 2015. Controller Redundancy Design for Cyber-Physical Systems. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 61–87.
Tun, S.Y.Y., Madanian, S., Mirza, F., 2021. Internet of things (IoT) applications for elderly care: a reflective review. Aging Clin. Experim. Res. 33 (4), 855–867.
Uckelmann, D., Harrison, M., Michahelles, F., 2011. An architectural approach towards the future Internet of Things. In: Architecting the Internet of Things. Springer, pp. 1–24.
Voas, J., 2016. De-Mystifying IoT. Networks 36, 1.
Vogel Communications Group GmbH & Co. K.G., 2017. Was ist ein Cyber-physisches System (CPS)?. URL https://www.bigdata-insider.de/was-ist-ein-cyber-physisches-system-cps-a-668494, (Accessed 30 May 2022).
Wang, L., Törngren, M., Onori, M., 2015. Current status and advancement of cyber-physical systems in manufacturing. J. Manuf. Syst. 37, 517–527.
Waschull, S., Bokhorst, J., Molleman, E., Wortmann, J., 2020. Work design in future industrial production: Transforming towards cyber-physical systems. Comput. Ind. Eng. 139, 105679. http://dx.doi.org/10.1016/j.cie.2019.01.053.
Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS Quart. xiii–xxiii.
Weiser, M., 1991. The computer for the 21 st century. Sci. Am. 265 (3), 94–105.
Weiser, M., 1993. Some computer science issues in ubiquitous computing. Commun. ACM 36 (7), 75–84.
Winter, J., 2015. Algorithmic discrimination: Big data analytics and the future of the internet. In: The Future Internet. Springer, pp. 125–140.
Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. Microprocess. Microsyst. 77, 103201.
Yachir, A., Amirat, Y., Chibani, A., Badache, N., 2016. Event-aware framework for dynamic services discovery and selection in the context of ambient intelligence and Internet of Things. IEEE Trans. Autom. Sci. Eng. 13 (1), 85–102.
Yao, J., Liu, X., Zhu, G., Sha, L., 2015. Foundations of Compositional Model-Based System Design. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 89–114.
Zhang, Z., 2015. Unified Framework toward Solving Sensor Localization, Coverage, and Operation Lifetime Estimation Problems in Cyber-Physical Systems. In: Rodrigues, J.J., Rawat, D.B., Stojmenovic, I. (Eds.), Cyber-Physical Systems: From Theory to Practice. pp. 417–436.
Zhu, Q., Wang, R., Chen, Q., Liu, Y., Qin, W., 2010. Iot gateway: Bridgingwireless sensor networks into internet of things. In: 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Ieee, pp. 347–352.
Zurier, S., 2016. Five IIoT companies prove value of internet-connected manufacturing. IoT Agenda URL https://www.techtarget.com/iotagenda/feature/Five-IIoT-companies-prove-value-of-internet-connected-manufacturing, (Accessed 30 May 2022).

Veronika Lesch is a post-doctoral researcher and head of the Cyber-Physical Systems research group at the chair of software engineering at the University of Würzburg. Her research topics include selfaware computing systems and self-adaptive systems. She researches in the field of IoT and CPS concerning Industry 4.0 and Logistics as well as Platooning and Intelligent Transportation Systems.

Marwin Züfle received his Ph.D. degree from the University of Würzburg in 2022. His research topics include time series forecasting, data analytics, and critical event prediction. He received the University Award of the Main-Franconian Economy 2018.

André Bauer is the head of the Software Engineering for Applied Data Analytics Research Group at the Software Engineering Chair headed by Prof. Samuel Kounev, University of Würzburg. His research is focused on predictive data analytics, dataops, green AI, and synthetic data generation. He received the Ph.D. degree in computer science from the University Würzburg, Würzburg, Germany, in 2020.

Lukas Iffländer received his bachelor's, master's and Ph.D. degree in computer science from the University of Würzburg. There, he continues to support the Chair of Software Engineering as an associated group leader for the Security Testing & Benchmarking Group. His main occupation lies with the German Center for Railway Traffic Research (DZSF) where he takes the role of a scientific desk officer for cybersecurity. His main research topics are software-defined networking, network function virtualization, and the combination of safety and security.

Christian Krupitzer received a bachelor's, master's, and Ph.D. degree from the University of Mannheim, Germany, in 2010, 2012, and 2018, respectively. Since October 2020, he is tenure track professor and leads the Department of Food Informatics at the University of Hohenheim in Stuttgart, Germany. His research interests include applying principles of adaptive systems and machine learning for IIoT (focusing on food production), intelligent transportation, and sports.

Samuel Kounev is a professor and chair of software engineering at the University of Würzburg. His research is focused on the engineering of dependable and efficient software systems, systems benchmarking and experimental analysis; as well as autonomic and self-aware computing. He received a Ph.D. in computer science from TU Darmstadt. He is a member of ACM, IEEE, and the German Computer Science Society.