systems

MDPI

Review

Distributed Control of Cyber Physical System on Various Domains: A Critical Review

Muzaffar Hamzah [1], Md. Monirul Islam [2], Shahriar Hassan [3], Md. Nasim Akhtar [4], Most. Jannatul Ferdous [5], Muhammed Basheer Jasser [6,*] and Ali Wagdy Mohamed [7,8]

[1] Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu 88450, Sabah, Malaysia
[2] Department of Computer Science and Engineering, University of Information Technology and Sciences, Baridhara J Block, Dhaka 1212, Bangladesh
[3] Department of Computer Science and Engineering, Gono Bishwabidyalay, Dhaka 1344, Bangladesh
[4] Department of Computer Science and Engineering, Dhaka University of Engineering and Technology, Gazipur 1707, Bangladesh
[5] Department of Computer Science and Engineering, Bangladesh University of business and Technology, Dhaka 1216, Bangladesh
[6] Department of Computing and Information Systems, School of Engineering and Technology, Sunway University, Petaling Jaya 47500, Malaysia
[7] Operations Research Department, Faculty of Graduate Studies for Statistical Research, Cairo University, Giza 12613, Egypt
[8] Applied Science Research Center, Applied Science Private University, Amman 11937, Jordan
* Correspondence:basheerj@sunway.edu.my

Abstract: Cyber-Physical System (CPS) is a symbol of the fourth industrial revolution (4IR) by integrating physical and computational processes which can associate with humans in various ways. In short, the relationship between Cyber networks and the physical component is known as CPS, which is assisting to incorporate the world and influencing our ordinary life significantly. In terms of practical utilization of CPS interacting abundant difficulties. Currently, CPS is involved in modern society very vastly with many uptrend perspectives. All the new technologies by using CPS are accelerating our journey of innovation. In this paper, we have explained the research areas of 14 important domains of Cyber-Physical Systems (CPS) including aircraft transportation systems, battlefield surveillance, chemical production, energy, agriculture (food supply), healthcare, education, industrial automation, manufacturing, mobile devices, robotics, transportation, and vehicular. We also demonstrated the challenges and future direction of each paper of all domains. Almost all articles have limitations on security, data privacy, and safety. Several projects and new dimensions are mentioned where CPS is the key integration. Consequently, the researchers and academicians will be benefited to update the CPS workspace and it will help them with more research on a specific topic of CPS. 158 papers are studied in this survey as well as among these, 98 papers are directly studied with the 14 domains with challenges and future instruction which is the first survey paper as per the knowledge of authors.

Keywords: a critical review; 3C; 5C; NIFU; Cyber Physical System; 14 domains of CPS

check for updates

Citation: Hamzah, M.; Islam, M.M.; Hassan, S.; Akhtar, M.N.; Ferdous, M.J.; Jasser, M.B.; Mohamed, A.W. Distributed Control of Cyber Physical System on Various Domains: A Critical Review. *Systems* **2023**, *11*, 208. https://doi.org/10.3390/systems11040208

Academic Editor: William T. Scherer

Received: 7 February 2023
Revised: 27 March 2023
Accepted: 14 April 2023
Published: 20 April 2023

1. Introduction

The Cyber-Physical System (CPS) is the key concept of Industry 4.0, which the German government advocates for to develop smart factories and fetch in the 4th industrial revolution. When an NFS session was organized in Austin, Texas, the United States in 2006, the concept of CPS officially emerged [1]. Industry 1.0 was about mechanization and steam power, and then mass production and assembly line which was known as Industry 2.0, and digitalization and automation are Industry 3.0, and finally, Industry 4.0 is planned for the distributed engender through shared amenities in the combined global industrial structure for on-demand manufacturing to succeed personalization and resource efficiency [2].

It has far-reaching consequences for both producers and consumers. The term Industry 4.0 refers to a trend in industrial automation that incorporates some new technologies to improve worker health at work, as well as plant productivity and quality.

The smart factory approach is part of Industry 4.0 and is divided into three categories including smart production, smart services, and smart energy. From the previous statement, it is clear that energy conservation is a concern in any sort of factory. This is because the end product must be produced at a low cost while maintaining high quality. As a result, energy conservation boosts productivity and maybe creates job opportunities. The Cyber-Physical System is a major idea in Industry 4.0. [3]. CPS are advanced technologies that connect physical reality operations with computing and network infrastructure [4]. With typically integrated devices, which are supposed to function like independent devices, CPS focuses on connecting multiple devices [5]. A CPS comprises a monitoring system, generally, one or even more microcontrollers that regulate and transmit the information acquired from the sensors and actuators required to deal with the actual environment. A communication interface is also required for such embedded systems to share information with other embedded systems or the cloud. The most significant element of a CPS is information interchange, because information may be connected and analyzed centrally. A CPS, to look at it another way, is an embedded system that can communicate with other devices via a network. The Internet of things [6] is a term used to describe CPS that are hooked up to the internet. With integrated technology, the Internet of Things (IoT) will connect all the company's elements, machinery, and Goods. The contribution of the article is as follows:

- We demonstrated the categories of CPS and the uses of CPS in fourteen domains like health, transportation, industry, vehicle, smart device, robotics, aircraft, energy, education, agriculture, and so on. We have also described the characteristics of CPS including 3C, 5C as well as NIFU together in a tabular form which is not shown in any previous paper. In fine, the contribution in this paper is all about the definition of CPS, categories of CPS, use of CPS, application of CPS, the technology used in CPS, CPS life cycle, and so on.
- Acronym is a significant part of a research paper and this article included many abbreviations. It is important to know the full form of abbreviation to reduce the complexity of any topic. A table is conducted to the paper for a better understanding of acronyms. Almost all the acronyms are listed in the table.
- We are the first to include 14 domains together in a survey paper which is not included in any previous papers. We have also mentioned the challenges and future direction of each paper in all the domains including Aircraft, Energy, Robotics, Vehicular, Education, Agriculture, Mobile Phones, Health care, Battlefield surveillance, Smart home, smart manufacturing, Smart Transportation, Industrial Automation, and Chemical Production. Almost articles have limitations on security, data privacy, and safety. Several projects and new dimensions are mentioned where CPS is the key integration. Consequently, the researchers and academicians will be benefited to update the CPS workspace and it will help them with more research on a specific topics of CPS.
- A total of 157 papers have been conducted to this article. Among them 109 papers are for the CPS applications from the different databases and 98 papers are reviewed for domains directly.

The common acronyms used in CPS field are tabulated in Table 1.

Table 1. Used and known Acronym about Cyber Physical System.

Acronym	Full Form	Acronym	Full Form
CPS	Cyber Physical System	NFS	National Science Foundation
IOT	Internet of Things	IOS	Internet of Services
IOD	Internet of Data	OCS	Oriented Cuckoo Search
3C	Computing, Communication, Control	IDS	Intrusion Detection Systems
RTLS	Real-Time Location Sensing	WoT	Web of Things
NoC	Network-On-Chip	KF	Kalman Filter
ACPS	Aviation Cyber Physical System	UAVs	Unmanned Aerial Vehicles
CPPS	Cyber Physical Production System	ECPS	Energy Cyber Physical System
PHEVs	Plug-in Hybrid Electric Vehicles	HESS	Hybrid Energy Storage System
SeDS	Sensor-Drone-Satellite	ICT	Information & Communication Technology
MDR	Monitoring detecting responding	CCP	Collaborative Control Protocol
MCPS	Medical Cyber-Physical System	EHR	Electronic Health Record
MPPT	maximum power point tracking	IASs	Industrial automation systems
ICPS	Industrial Cyber-Physical Systems	IAS	Industrial Automation and Software
CPSSs	Cyber-physical product-service systems	RE	Requirements Engineering
PHM	prognostics and health management	DTs	Digital Twins
TCPS	Transportation Cyber-Physical Systems	DEDR	Dynamic En-route Decision real-time Route
CF	car-following	EV	Electric Vehicle
ITS	Intelligent Transportation Systems	FC	Fog Computing
SA	Smart Agriculture	SCSAS	Smartphone based construction site safety awareness system
3C	Computation, Communication, and Control	5C	Connection, Conversion,Cyber, Cognition and Configuration
		NIFU	Network, Intelligence, Functionality, and User friendliness)

The rest of the paper is organized as: Section 2 introduces the literature review of CPS. Section 3 considers the existing work of CPS in various fields. Section 4 considers the discussion and guidelines for the future work for the researchers. Lastly, Section 5 provides the conclusion.

2. Literature Review of CPS

This section covers the concept of cyber physical system, 5C & 3C architecture of CPS, characteristics of CPS, technologies, and so on.

2.1. What Is Cyber Physical System?

Cyber refers to Computing, Networking, and controlling that is distinct, switched, and logical. Physical systems are natural and human-made systems that are regulated by physics rules and executed on time [7]. A CPS is characterized as a revolutionary technology for controlling associated systems between their computation capabilities and physical assets [8]. A CPS is a network of interconnected IT components that is used to control physical such as mechanical and electronic items. The Internet is used as an information infrastructure for connectivity. A CPS is made up of two major functional elements.

- Advanced gateways, which helps to ensure real-time data obtained from the physical world as well as info responses from the cyber environment; and
- Intellectual data processing, computer simulation, and data analysis abilities, which build the cyber.

Several technologies are intimately linked to the CPS for instance Sensor networks, IoT, wireless, and cloud computing. Wireless networks are thought to be an important part of CPS [9]. The Internet offers critical techniques for optimizing the productivity of cyber-physical systems. The following parameters are included in internet technology perspectives.

- Internet of Things (IoT): It entails using IP addresses to communicate with smart systems. This allows any physical device to be assigned its IP address [10].
- Internet of Services (IoS): It includes new communication models such as those offered by service-oriented design (SOA) and REST technology [11].
- Internet of Data (IoD): It allows for the efficient transmission and storage of large amounts of data, as well as the creation of innovative analytical techniques for analyzing large amounts of data [12].

We can also say about CPS that it is a convergence of 3C containing computation, communication, and control or 5C or NIFU.

The characteristics of CPS among 3C, 5C [1] and NIFU is discussed in Table 2.

Table 2. Characteristics of CPS.

Name	Description
3C	• Computation in a CPS refers to the processing and analysis of data from physical and computational components to make decisions and control physical processes. • Communication in a CPS refers to the exchange of data between physical and computational components to facilitate control and monitoring of physical processes. This involves the use of communication networks and protocols to ensure that data is transmitted accurately and in a timely manner. Effective communication is critical in a CPS to ensure that physical processes are controlled and monitored accurately and in real-time. • Control in a CPS refers to the ability of the computational components to influence and manipulate physical processes. This involves the use of sensors, actuators, and other physical devices to monitor and manipulate the physical environment. The computational components of a CPS use data analysis and decision-making algorithms to determine the appropriate actions to take to achieve the desired control outcomes.
5C	• Connection in a CPS, the physical and computational components must be connected and integrated with each other to achieve a specific function. This involves establishing communication channels between sensors, actuators, and other physical devices and the computational components, such as processors and communication networks. • Conversion in a CPS refers to the process of converting physical data into digital data that can be processed and analyzed by computational components. For example, in an autonomous vehicle, sensors detect the physical surroundings, and the data from those sensors is converted into digital data that is processed by the onboard computer to make decisions about the vehicle's movement. • The term "cyber" in CPS refers to the computational components of the system, including hardware, software, and communication networks. • Cognition in a CPS refers to the system's ability to process, analyze, and make decisions based on data from physical and computational components. This involves using artificial intelligence and machine learning algorithms to analyze data and make decisions about how to control physical processes. • Configuration in a CPS refers to the arrangement and setup of physical and computational components to achieve a specific function. Configuration is critical in ensuring that the CPS is optimized for its intended application and operates effectively and efficiently.

Table 2. *Cont.*

Name	Description
NIFU	• A CPS is typically composed of multiple physical and computational components that need to communicate with each other to achieve the desired functionality. A network, such as a wired or wireless communication network, is used to establish communication between these components. • The intelligence of a CPS refers to the system's ability to process data, learn from data, and make decisions based on data. This involves using algorithms and techniques such as artificial intelligence, machine learning, and data analytic to analyze data from physical and computational components. The intelligence of a CPS enables it to optimize physical processes, improve safety and efficiency, and enable intelligent automation. • The functionality of a CPS refers to its ability to perform a specific task or achieve a specific goal. The functionality of a CPS can vary widely depending on the application, and can range from simple tasks, such as adjusting temperature and lighting in a smart home, to complex tasks, such as controlling an autonomous vehicle. • User-friendliness in a CPS refers to the ease of use and intuitiveness of the system's interface. This involves designing the system with the user's needs and preferences in mind and providing an interface that is easy to navigate and understand. A user-friendly CPS can help ensure that the system is used effectively and efficiently and can help reduce the potential for errors or accidents.

2.2. Compatibility of CPS with Industry 4.0

A CPS is a highly integrated system of physical components containing sensors, actuators, and diverse equipment, along with cyber components boasting ubiquitous processing and effective communication, which is a rapidly emerging research topic. Addressing demands, challenges, and possibilities across a variety of industrial sectors might help speed CPS research. The focus is to create new systems science and engineering methodologies for designing high-confidence systems that are flexible, synergistic and interconnected at all levels. Industry expenditures in CPS technology and research have been extensive in the past and present, but have primarily concentrated on shorter-term, faster-payoff proprietary solutions. Ministries and some industries have recently made investments in lengthier, pre-competitive technologies and testbeds [13]. CPSs, which include transport systems, power systems, water/gas distribution systems, and autonomous factories, are regarded as the most potential industrial systems from an engineering standpoint. A wide range of industrial robots with an inertial navigation device or other sensors are programmed to move along a predetermined route to fulfill production tasks together [14,15]. The tight coordination of cyber and physical aspects in these systems gives higher freedom, productivity, usability, security, and flexibility. Moreover, industrial CPSs are viewed as a key component of the 4th industrial revolution [16,17] and significant efforts have been undertaken to demonstrate their significance. Industrial CPSs are massive, globally distributed, federated, collaborative, and life-critical systems with a large number of integrated sensors and actuators that are connected to provide real-time inspection and closed-loop control. Furthermore, sensor networks and distributed control networks play a significant role in the execution of industrial CPSs. In other words, in a widely deployed CPS architecture, these two networks are frequently required [18]. Sensor networks are typically implemented in the interior or surrounding plants to collect lots of important information in order to make accurate perceptions of the physical plants. Actuators may be able to respond in real-time to changes in physical plants using this information. As a result, when merging the cyber and physical worlds, a closed loop is produced by both communications between sensors and actuators and controlling plants via actuators [19]. Many industrial sensors and actuators with some communication and data processing capabilities have been made accessible in recent years, due to the efforts of research institutes and enterprises all around the world.

2.3. Cyber and Physical Mapping

The goal of CPS is to provide new features to physical systems by combining computation and communication with physical processes [20]. CPS provides real-time sensing, dynamic control, and information services for complicated processes through strong collaboration between the 3Cs. CPS has placed a heavy emphasis on the cyber world's tremendous communication and computation abilities which could also improve the physical world's precision and efficiency [21,22]. Additionally, whether it is a three-tier, five-tier or service-oriented design all of the CPS designs described by academics concentrate on control instead of mirrored representations [23]. The tasks of CPS are enabled by mutual mapping, real-time communication, and effective collaboration between both the cyber and physical worlds. The computing system may have impacted more than one physical object. For example, a structure may consist of several hardware elements. As a result, the mapping link between the cyber and physical worlds of CPS is a one-to-many connection rather than a one-to-one.

2.4. Integration in CPS

CPS evolves and it becomes more advanced over time as an industrial automation system [24]. To compensate for the limitations among networks, technologies, tools, and devices, and along the value chain, an ever-increasing demand for connectivity is highly suggested [25,26]. With the new problems provided by incorporating cyber-physical systems (CPSs) into commercial applications and the issue of integration is becoming even more important for the introduction of new technologies and their acceptability by professionals when speaking of Industry 4.0 concepts [27].

Technologies in CPS

There are two popular technologies in CPS. They are stated below:

- Communication Technology in CPS: In the digital system, CPS is linked to electronic gadgets, portable devices, and industrial instruments [28]. Communication, networking, processing of data, storage systems, and transmission power are all vary among components [29]. For example, Smartphones have the ability for networking, processing, communicating and data storing. Each of this stuff can be linked using network, communication, and software technologies. A self-configuration technology of humanized CPS algorithm employing simple binary and mathematical operations can shorten convergence time and enhance scalability [30]. The use of state-space approaches in the development of a novel connected cyber-physical system (CPS) framework and the use of feedback control to dynamically change CPS resource utilization and efficiency is discussed [31]. The oriented cuckoo search algorithm (OCS) is a new evolutionary algorithm [32]. In OCS, a mixture of two separate random distributions dominates the global search capabilities. Petri net models have been generalized for creating dynamic manufacturing techniques in order to enable traceability analysis [33]. By using a three-phase design strategy that includes cross association, sensitivity analysis, and a systematic methodology, optimal IDS design for creating intrusion detection systems (IDS) is intended at lowering the number of monitored parameters [34]. A different task may have different CPS needs, such as productivity, power efficiency, and privacy and a real-time issue is also a crucial factor [35]. For example, the efficacy of CPS depends on the ability to select a suitable existing framework for choosing work periods in real-time using predetermined priority controller jobs planned using a rate monotonous algorithm [36]. Specialized real-time location sensing (RTLS) labels provide an effective methodology to enabling bidirectional coordination between physical construction materials and their virtual models, improving real-time construction continuity, and assisting proactive strategic decision-making [37].
- Networks Involved in CPS: Computational and physical resources are closely connected and mutually reliant in cyber-physical systems [38]. It is important to ensure

and enhance performance in various technology-related domains, such as manufacturing, energy, transportation, and healthcare, in order to develop and implement resilient and reliable CPS networks. WSNs, wireless networks, WLANs, cloud-based networks, social networks, and other heterogeneous networks are all used in CPS [39,40]. CPS assesses the applications and technological criteria for effectively blending CPS with sensor network plane from a security perspective, as well as the techniques for transmitting information among remote monitoring locations and widely implemented sensor nodes [41]. Topology regulation by node selection could enhance data transmission performance while conserving energy and extending the network's lifetime [42]. Wireless sensor network topology optimization is a critical topic. A topology optimization approach for wireless sensor networks based on complex network theory and cyber-physical systems is developed using software-defined wireless sensor network architecture [43]. To promote the successful integration of CPS, an Intelligent Control Box transforms diverse wireless signals, including Bluetooth, ZigBee, and RF [44]. As shown in a literature review, discusses the benefits of Web of Things (WoT) and CPS integration. A CPS for structural event observation with WSNs is presented, as well as a novel approach based on network decision in the CPS entitled MODEM [45] proposes a method for coordinating a network of suppliers in a cyber-physical system [46]. The dynamics of the agent are nonlinear, arbitrary in size, and sometimes heterogeneous. In [47], the authors examine the state prediction problem in cyber-physical systems (CPS) where a wireless sensor measures a dynamical physical process and transmits the measurements to a remote state estimator. In addition, in [48], the authors describe a dependable Network-On-Chip (NoC) technique that may be applied to an FPGA-based system. They have looked at the stochastic stability of Kalman filter (KF) based state estimation in geographically distributed cyber-physical systems using a lossy network.

3. Application of CPS

CPS-based technologies are in the primary stage [49]. Therefore, in Industry 4.0, the application of CPS is continually changing and expanding. Many CPS-based applications have been developed or implemented in a wide range of industries, such as aircraft transportation systems [50], battlefield surveillance [51], chemical production [52], energy [53], agriculture (food supply) [54], healthcare [55], education [56], industrial automation [57], manufacturing [58], mobile devices [59], robotics [60], transportation [61], and vehicular [62]. Researchers and practitioners may have to reach a compromise among their aims to create a combination of benefits and cost, based on desired CPS and Industry 4.0. The discussed fields are graphically shown in Figure 1.

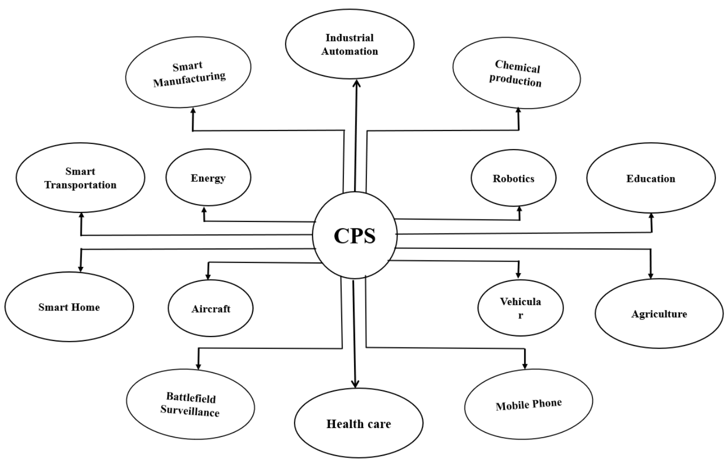

Figure 1. CPS Applications.

The selected papers in the mentioned domain are chosen by searching some keywords including cyber-physical system application, use of the cyber-physical system, application of CPS, current trend in CPS, and so on through the popular search engines platform like Scopus, google scholar, web of science, IEEE, Springer, and MDPI. We read the titles, abstract and methodologies, and conclusion. The papers are listed in Table 3 as per publishers.

Table 3. List of papers based on publication.

Publisher	Count
ACM	4
IEEE	34
Springer	9
Elsevier	26
EMERALD	2
J- STAGE	1
PHM	1
Nature	2
Agronomy	1
HSOA	1
National Academies Press	1
KSII	1
GIG Global	2
World Scientific Publishing Co.	3
Institution of Civil Engineers	1
PACIS Scientific Proceedings 2015	1
Osaka University	1
Institut Teknologi Nasional Bandung	1
Wiley	3
MDPI	3
Total	98

The chosen papers is shown in Table 4 Year-wise.

Table 4. Year-wise Publications.

Year	No. of Paper
2022	1
2021	12
2020	13
2019	15
2018	11
2017	11
2016	15
2015	7
2014	7
2013	3
2012	2
2011	1
Total	98

3.1. CPS in Aircraft

In the next two decades, aviation will have to accommodate a multi-fold increase in air traffic as well as new kinds of manned and unmanned plane categories, all while enhancing passenger satisfaction, ecological consequences, and shareholder business [63]. The conventional aviation system is moving towards the ACPS framework and it has huge advantages, for instance, it approves real-time data analytics, real-time monitoring, and diagnostics. A CPS is worked with network systems because for that reason it has a serious security threat. In CPS false data injection (FDI) is vastly used for cyber-attacks.

In [64], they develop a Nobel Security (NS) algorithm for identifying the FDI attacks by using Artificial Immune System (AIS). NS is based on a negative selection approach, which is detecting the malicious network packets and omitted them. In [65], they discussed another security threat for the communication networks is known as Distributed Denial-of-Service (DDOS). Nonlinear Autoregressive Exogenous (NARX) model is used to defend from DDOS attacks where NARX keeps the network packet secure. The Internet often interacts us with several threats that leads security and privacy of CPS in risk zone [66]. Mash networks are vastly accepted because of their flexibility in communication including UAS (Unmanned Aerial System). In [67], a block-chain based strategy for UAS in mesh networks is proposed to securely gather, analyze, and disseminate routing information. Aviation security is at the forefront of society, mostly as a protection against terrorism and national security threats in the physical world [50]. The ACPS (Aviation Cyber-Physical System) principle is to integrate the cyber layer with the physical world [68]. The Application Layer, Network Layer, and Physical Layer are the three core components of the ACPS. In [69], the authors discussed many limitations of the aviation sector and the practice possibilities. The source description of the above-mentioned paper is given in Table 5.

Table 5. Research Category and Journal Details of CPS in Aircraft.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Aircraft	Aerospace Conference	IEEE	2012	[63]
	Computational Science and Computational Intelligence	IEEE	2020	[64]
	Advances in Artificial Intelligence and Applied Cognitive Computing	Springer	2021	[65]
	International Conference on Smart Computing	IEEE	2016	[66]
	IEEE Communications Surveys & Tutorials	IEEE	2019	[67]
	Proceedings of the IEEE	IEEE	2013	[50]
	Electronics and Mechatronics Conference	IEEE	2021	[68]
	Computers & Security	Elsevier	2022	[69]

However, the literature discussed above lacks a thorough evaluation of the suggested remedies in practical situations. Little thought has been given to how the suggested solutions will affect the effectiveness and performance of the system as a whole. Also, Security and safety mechanisms in aviation cyber-physical systems are not integrated with enough care. The development of a comprehensive strategy that considers both security and safety elements in aviation cyber-physical systems may be a future research focus. This could entail the creation of stronger frameworks for risk assessment and management as well as the design of intrusion detection and prevention systems that are more effective and efficient. In order to confirm these solutions' efficacy and viability, more thorough testing and evaluation are required in real-world settings.

3.2. CPS in Battlefield Surveillance

Unmanned Aerial Vehicles (UAVs) have become commonplace in both military and civilian applications. Additionally, UAV security issues are increasingly becoming more visible and attracting a lot of attention. UAVs are a type of Cyber-Physical System because they combine compute, control, and communication components (CPS) [70]. UAVs are a type of a CPS that consists of various components such as sensors, communications, compute, and control systems, each of which could be the target of a cyber-attack, leading to unwanted states and significant faults in the physical system. We can name this type of cyber-attack with physical repercussions a cyber-physical attack, according to with concept in [71]. It has terrible effects on UAVs and other CPS. One example is technological advancements in Unmanned Aerial Surveillance Systems, also known as drones, for surveillance, real-time supervising, and emergency augmentation for an actionable response, safety, and enabling environment of connected communities to establish new levels of possibility and development, security, and safety, health and well-being, and therefore improve the quality of life [72]. These works are shown in tabular form in Table 6.

Table 6. Research Category and Journal Details of CPS in Battlefield Surveillance.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Battlefield Surveillance	International Conference on Computer Engineering and Application	IEEE	2020	[70]
	Internet of Things	IEEE	2021	[71]
	Nanoscience and Nanotechnology in Security and Protection against CBRN Threats.	Springer	2020	[72]

Instead of offering a thorough examination of all potential attack scenarios, there is a limited focus on particular cyber-physical assault and threat types in the above-mentioned literature. Little thought has been given to how proposed solutions would really be implemented, including aspects like scalability, cost-effectiveness, and user-friendliness. The moral and legal ramifications of utilizing drones for monitoring and spying have received little consideration. Creating a single framework for identifying, assessing, and mitigating cyber-physical hazards in drone-based systems could be a future research focus. This might entail combining several security and privacy tools, like secure communication protocols, intrusion detection systems, and access control protocols. The ethical and legal ramifications of utilizing drones for surveillance and monitoring, including concerns over privacy, data protection, and civil liberties, also require further study.

3.3. CPS in Chemical Production

Method of the smart chemical industry depends on CPS is proposed in response to technological advancements and growing trends in the chemical industry. A CPS framework for the smart chemical industry is developed, followed by important approaches such as big data and rigorous digital modeling. For instance, the intelligent correction column is developed followed by several crucial technologies including robust online modeling and big data techniques as well as a case study is dealt with named smart rectification column [73]. Chemical processes are currently becoming wider and much more sophisticated. Proper understanding of heterogeneity, non-linearity, non-equilibrium, various scales, and various temporal-spatial knowledge areas of chemical processes is one topic of scientific work in the domains of engineering; this understanding is also important for the improvement of the chemical industry [74]. It is expected that by carefully integrating new industry 4.0 technologies into the physical system, a more effective, better, ecologically friendly, and competitive system will emerge. The disruptive nature of these emerging technologies was highlighted at the 2016 Davos Forum. As a result, deploying CPS in the chemical industry is a great opportunity to meet with the industry's ongoing and prospective difficulties [75–77]. The source description of the above-mentioned paper is given in Table 7.

Table 7. Research Category and Journal Details of CPS in Chemical Production.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Chemical production	Advances in Engineering Software	Elsevier	2016	[73]
	Computers & Chemical Engineering	Elsevier	2020	[74]
	AI	MDPI	2021	[75]
	Smart Village Technology	Springer	2020	[76]
	Process Control	Elsevier	2000	[77]

However, in the literature there is an absence of testing and real-world application of proposed methods in the chemical sector. Cybersecurity and data privacy issues are not given enough attention when cyber-physical systems are implemented in the chemical industry. There is little information on the social and economic effects of using cyber-physical systems in the chemical sector. Future research might focus on overcoming the aforementioned constraints and creating workable implementation and testing plans for cyber-physical systems in the chemical sector, all the while addressing cybersecurity and data privacy issues. The economic and social effects of these systems on business and the environment could also be the subject of investigation.

3.4. CPS in Energy

In the domain of engineering, the CPS and its uses have attracted a lot of attention. The cyber-physical production system (CPPS) is advocated in process automation and control of dynamic systems, as well as the current position and progress of CPS in the industry, which have been studied [78]. A structure based on real-time manufacturing big data, a methodology for big data-driven evaluation, and a structure of CPS-based smart showroom is presented to distribute resources and energy in manufacturing companies efficiently using the latest techniques [79–81]. The energy cyber-physical system (ECPS), also known as the cyber-physical energy system, is another application area for CPS. The authors surveyed ECPS and its uses on smart grids in [82] and outlined the benefits of using ECPS. ECPS has a lot of potential for achieving energy preservation and lowering emissions. Authors offered data-driven modeling, control, and techniques for ECPS in [83]. ECPS in manufacturing is a new multidisciplinary CPS, manufacturing, and energy study topic [84].

The adoption of a hybrid energy storage system (HESS) offers a bright future for plug-in hybrid electric vehicles' overall economy (PHEVs). In [85], the author offers a unique energy management strategy that uses the energy storage potential of HESS to optimize the overall economy of PHEVs. To begin, a cyber-physical energy management model is being developed to extract the best power transmission approach for PHEVs with HESS. This framework allows for the synergistic scheduling of the gasoline engine, battery, and super capacitor. Because of the rapid use of renewable energy, electric power systems networks are confronted with new opportunities and challenges [86]. With energy flowing in the physical system and information flowing in the cyber-network, the power generation system is inherently a CPS. Testbeds are essential for gaining a better understanding of cyber-physical interactions and providing venues for prototyping new applications. In [87], a CPS testbed for threat detection in power systems is presented. In [88], the authors proposed a toolbox for security research on CPS networks that connects CPS software and hardware to examine cyber-attacks and responses. One of the most common applications of CPS is energy monitoring. Any Flow is an intelligent energy management service that allows to see how much energy we are using. This technology gathers energy consumption data from machine sensors every second, records it in a central database, and returns the information on a mobile app [89]. Table 8 is provided with the source description of the above-mentioned papers.

Table 8. Research Category and Journal Details of CPS in Energy.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Energy	Procedia CIRP	Elsevier	2014	[78]
	Ambient Intelligence and Humanized Computing	Springer	2019	[79]
	Rapid Prototyping Journal	EMERALD	2018	[80]
	Cleaner Production	Elsevier	2017	[81]
	conference on innovative smart grid technologies Latin America	IEEE	2011	[82]
	International Conference on Cyber-Physical Systems	IEEE	2016	[83]
	cleaner production	Elsevier	2019	[84]
	Energy	Elsevier	2021	[85]
	IET Energy Systems Integration	WILEY	2020	[86]
	PES General Meeting∣ Conference & Exposition.	IEEE	2014	[87]
	workshop on cyber-physical systems-security and/or privacy	ACM	2015	[88]
	Procedia CIRP	Elsevier	2018	[89]

Certain common limitations can be found despite the fact that each of the aforementioned publications focuses on a distinct component of cyber-physical systems and their applications. First off, without taking into account the offered solutions' interoperability and scalability, the majority of studies are concentrated on creating frameworks or models for particular applications. Second, the bulk of studies fail to address the security and privacy issues raised by the gathering and use of large amounts of data in cyber-physical systems. The paucity of research on the economic and social effects of cyber-physical systems, particularly their potential to increase sustainability and offer new job possibilities, is another issue. Given these limits, future research should concentrate on creating comprehensive and integrated strategies for creating, putting into use, and managing cyber-physical systems that take the aforementioned concerns into account. This could entail the creation of interoperability standards and protocols as well as the incorporation of security and privacy safeguards into the planning of cyber-physical systems. In order to ensure that cyber-physical systems are implemented in a way that benefits society as a whole, study should also be done on the economic and social implications of such systems.

3.5. CPS in Agriculture

In the recent two decades, there has been a significant shift from advanced mechatronic systems to CPS. CPS will play a vital role in precision agriculture, and it is projected to boost output and help grow more food and prevent starvation. In [90,91], the authors created a CPS agricultural model for the potato crop. This study discusses agriculture's integrated precision agriculture management. It continuously investigates and acts on physical entities e.g., soil, weather, pumps, etc. By building data-driven systems for diagnosing soil health issues and tracking changes that occur, this phase seeks to provide efficient and accessible decision services and support. To improve soil crop (SC) sustainability and improve farming activities, precise SC condition monitoring is critical [92]. Agriculture has been one of the most common uses of drones for agricultural health monitoring [93]. These studies have been based on the calibration data as well as the selected soil test results being associated with the crop reaction to forecast the change in production that will arise as a result of applied fertilizers. While these assumptions are frequently true in practice, there have been concerns about existing alarms' capacity to sustain micronutrient levels like: nitrogen (N), phosphorus (P), and potassium (K) or NPK concentrations [94,95]. With farming precision, a new method for climate-smart agriculture for CPS (ACPS) is introduced. The major goal is to use multivariate data to identify the position of the problem and monitor the field. The classification approach proposes a novel hybrid classification that blends place with node classifiers. Using sensor data and position prediction, their proposal detects irrigation, soil quality, and nutrients [96]. The source description of the above-mentioned paper is given in Table 9.

Table 9. Research Category and Journal Details of CPS in Agriculture.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Agriculture	Agriculture and Agricultural Science Procedia	Elsevier	2015	[90]
	ICOSEC	IEEE	2020	[91]
	Nature plants	NATURE	2016	[92]
	Technology and Society Magazine	IEEE	2018	[93]
	Soil and environment quality	AGRONOMY	2018	[94]
	Scientific reports	NATURE	2017	[95]
	Environ. Sci. Curr. Res	HSOA	2020	[96]

The lack of standardization and interoperability in cyber-physical systems used in agriculture, the need for better data administration and analysis, and the low knowledge and implementation of organic agricultural practices are the limitations of the aforementioned publications. The development of more integrated and standardized cyber-physical systems that can gather and analyze data from multiple sources, such as sensors, drones, and satellite imaging, in order to give farmers real-time information and decision support could be a potential future research focus. This may also entail investigating the application of machine learning and artificial intelligence to enhance the precision and dependability of data analysis and prediction models. The promotion of organic and sustainable farming methods, as well as the development of more effective and environmentally friendly fertilizing and pest control techniques, could also be emphasized.

3.6. CPS in Healthcare

The fourth industrial revolution (Industry 4.0) is also bringing the fourth revolution in healthcare technologies (Healthcare 4.0) [97]. The CPS which is an integration of computing, encompassing the cyber world (i.e., computers and the Internet) and physical methods through computer networks, is the technical underpinning of healthcare 4.0 [98]. Today, CPS for healthcare is more than just a network of linked medical devices; it's also a key component of enormous medical big data systems. The Medical Cyber-Physical System (MCPS) [99] is a CPS specialized in medical use that integrates smart medical equipment, embedded systems, and remote network technology including cloud computing technology. The Electronic Health Record (EHR) [100] could be kept and communicated via cloud servers for these other big data-based applications in a cloud-based MCPS. Collecting EHR data can assist patients in receiving better treatment from better hospitals while also providing information for medical insurance processing. EHR data is highly sensitive, and when developing data sharing and processing systems, security must be considered [101]. A broad range of medical sensors are implemented in the CPS healthcare application, but these sensors create a substantial number of false alarms. These false alerts confuse and decrease the overall performance of healthcare. Although some CPS healthcare designs for healthcare applications have been presented, they all struggle to implement false alarm detection. In [102], a novel false alarm detector framework for healthcare systems has been proposed in CPS. The notion is a battery-free and wirelessly powered wireless sensor for Cyber-Physical Systems devoted to Structural Health Monitoring applications in severe settings. The system is built on a smart mesh Wireless Sensor Network with Sensing Nodes and Communicating Nodes. Sensing Nodes are used to detect physical objects. They do not require batteries and are powered wirelessly by a specific radiofrequency source via a far-field Wireless Power Transmission system. The data collected by the Sensing Nodes is transferred to the Communicating Nodes, which, among other things, use the Internet to connect the real and digital worlds [103]. Ulcerative Colitis is a chronic or long-term inflammation of the large intestine that is rather prevalent. It is debilitating, and it can lead to life-threatening consequences. As a result, early detection in the fledgling phases is critical. Healthcare services based on Fog-Cloud enabled Cyber-Physical Systems are gaining traction as a proactive and effective way to provide remote monitoring of persons for disease identification and control. Using a Nave Bayes classifier and a Deep Neural Network, a novel IoT-Fog-Cloud supported CPS for detection and level classification of Ulcerative Colitis [104]. Recent breakthroughs in tracking and data analysis, as well as a CPS-enabled rehabilitative system architecture for improved recovery rate in gait instructional programs, have opened the way for the transformation of healthcare systems from experience-based to scientific proof. A rehabilitation system with CPS capabilities that receives, analyses, and models data from patients and rehabilitation training devices. A series of sensors collects different physiological data as well as machine parameters in this system. The sensors and data collection devices are linked to an edge computing unit that conducts data processing, analysis, and display of the results [105]. These works are shown in tabular form in Table 10.

Table 10. Research Category and Journal Details of CPS in Healthcare.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Healthcare	IEEE Access	IEEE	2021	[97]
	Transactions on Sustainable Computing	IEEE	2018	[98]
	medical systems	Springer	2018	[99]
	IEEE Access	IEEE	2019	[100]
	Information Sciences	Elsevier	2019	[101]
	Aasri Procedia	Elsevier	2013	[102]
	IEEE Access	IEEE	2019	[103]
	Microprocessors and Microsystems	Elsevier	2020	[104]
	Prognostics and Health Management	PHM	2021	[105]

The above-mentioned literature covers diverse topics on the use of CPS in healthcare. However, some potential drawbacks can be noted, such as the absence of standardized protocols for connecting different CPS components, the requirement for strong security measures to safeguard private patient information, and the difficulty of managing and analyzing huge amounts of data produced by healthcare CPSs. The development and evaluation of more thorough and integrated cyber-physical healthcare systems that can deliver individualized and real-time monitoring, diagnosis, and treatment could be a future research focus. In addition to developing and putting into practice more complex machine learning algorithms and decision-making models that can better forecast and prevent non-communicable diseases, this could entail investigating novel techniques for data gathering, analysis, and sharing. Future studies might also concentrate on creating mechanisms that are more secure and protect privacy for healthcare CPSs, as well as addressing the ethical and social ramifications of these systems.

3.7. CPS in Education

As CPS becomes more prevalent in our daily lives, the demand for a well-trained workforce emerges, necessitating innovative ways and test-beds for incorporating CPS principles into schools at all levels. As our society evolves to rely more on CPS, education and training encounter some issues. The surveillance system is increasing as a means of ensuring security and safety. The role of smart surveillance in the school system serves a variety of criteria, including general campus surveillance, class recording, teacher and student behavior monitoring, student monitoring, administration surveillance, and security surveillance, among others. The traditional cloud/fog-based cyber-physical system (CPS) and surveillance system offer real-time monitoring, machine learning, analysis, and advanced decision-making for real-time tasks in the current educational system [106]. Surveillance systems are being used in classrooms and labs to monitor students' behavior in the classroom and observe teacher performance [107]. This technology is being used as a cutting-edge option in educational institutes to help educators and students in advancing their learning processes [108]. The current situation has had an impact on CPS deployment in the field of education. When CPS is used effectively, it can deliver more dynamic instructional content and interactions between students and the educational environment. Moreover, colleges and universities should address CPS in education [109]. Intelligent CPS have been enabled by recent developments in control systems and modern communications to satisfy the rising needs of renewable energy, micro-grids, electric vehicles, and the internet of things (IoT) [110]. A powerful CPS platform, as well as the usage of the system to increase university students' interest in and knowledge of renewable energy. The maximum power point tracking (MPPT) charge controller delivered loads with electricity from the solar panel and utilized extra power to charge the rechargeable battery, according to experimental results in [111]. Students learned and acquired key ideas and skills in a variety of disciplines, like data sampling and collection, analog to digital conversion, solar power, battery charging, control, embedded systems, and software programming, thanks to the system. It is an excellent teaching resource for students in CPS who are studying renewable energy. The learning CPS design works well with flipped classroom-based instruction [112,113]. It limits students' time in the classroom to what is necessary for laboratories and collaboration. As a result, during epidemics, this method of education suffers less than lecture-based education. A method to designing a cyber-physical system for controlling virtual plants using a real DC motor is described in [114]. PLC controls the DC motor, and LabVIEW simulates the virtual plant. Students can learn how to generate control laws like PID and LQR and how to integrate them into controllers based on this work (PLC). The students will learn about CPSs and how they work. They will be able to create this and other CPSs on their own. These works are shown in tabular form in Table 11.

Table 11. Research Category and Journal Details of CPS in Education.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Education	Computer Applications in Engineering Education	WILEY	2020	[106]
	Law & Society Review	WILEY	2016	[107]
	Research in Innovative Teaching & Learning	EMERALD	2017	[108]
	Computer	IEEE	2017	[109]
	Emerging and Selected Topics in Power Electronics	IEEE	2021	[110]
	Electronics	MDPI	2021	[111]
	European Workshop on Microelectronics Education	IEEE	2014	[112]
	Embedded and Cyber-Physical Systems Education	ACM	2016	[113]
	Global Engineering Education Conference	IEEE	2018	[114]

However, the studies have a variety of constraints, including the need for better design and execution of CPS for education, privacy concerns with surveillance systems, and a lack of creative teaching approaches. Future research could focus on the creation of creative and efficient teaching strategies for CPS that can incorporate cutting-edge technologies like flipped classrooms and offer an inclusive learning environment that takes surveillance systems' privacy and moral issues into account. More practical and hands-on projects must be created in order to make it easier to design, build, and evaluate CPS for education. A more effective and engaging learning environment for students can be developed as a result of this research, better preparing them for the difficulties of the impending digital age.

3.8. CPS in Industrial Automation

Conventional industrial automation models have been increasingly inadequate in recent decades to handle the growing technology and commercial requirements of manufacturing companies. Sudden changes impose constraints on industrial businesses operations since they are under intense pressure to reduce costs, improve quality, and customize products in extremely flexible and dynamic production processes [115]. Industrial automation systems (IASs) are made up of a physical plant that executes physical operations and a network of microcontrollers that constantly monitor the physical phenomena [116]. The German Industry 4.0 initiative under the tag of Cyber-Physical Systems (CPS) and, more exactly, their applicability in the industrial domain, thus referred to as Industrial Cyber-Physical Systems (ICPS) [117,118]. IEC 61499 is a formal model for the industrial automation system which is a distributed control-based system and assists time-aware computations for better adaptation to the circumstance [119]. The University of Stuttgart's Institute of Industrial Automation and Software Engineering (IAS) has created a situation for the advancement of CPS. The industrial coffee machine at the IAS, which was originally a microcontroller, was converted to a CPS during the procedure. For the modification, a microcontroller board was employed as a cloud gateway. With the assistance of hardware add-ons, the coffee machine was linked to the web. Different cloud-based functions, including remote diagnostics and software updates, are now available. This will allow us to locate the closest coffee machine capable of delivering the appropriate product [4]. For fast and low-cost production, advanced manufacturing processes require better degrees of automation, as well as high levels of flexibility and responsiveness to changing production demands. By combining the capabilities of robotic systems with the flexibility and agility of human employees, human-robot interaction enables better interaction in manufacturing jobs that demand higher productivity. A cyber-physical system is proposed for facilitating and controlling safe human-robot collaborative assembly processes [120]. The method assumes a shared, fence-free working space where humans, industrial robots, and other vehicles, including self-driving cars, can function. This intelligent system is known as CPS, according to [78], and it realizes the connections among interconnected computing systems and the physical world. A robotic CPS that allows humans and robots to collaborate and coexist should be adaptable, autonomous, and highly automated [121]. Through a variety of electronics, computing, communications, sensing, actuation, microcontrollers, and sensor technologies [122], physical systems monitor the changing state of real-world factors [123]. In [124], authors investigate the architecture of a robotic CPS as well as the risk evaluation, which covers both security and safety considerations about human operators. These works are shown in tabular form in Table 12.

Table 12. Research Category and Journal Details of CPS in Industrial Automation.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Automation	Computers in industry	Elsevier	2016	[115]
	Computers in Industry	Elsevier	2015	[116]
	German National Academy of Science and Engineering	Technical Report	2013	[117]
	Ministry of Education and Research	REPORT	2014	[118]
	Industrial Electronics Society	IEEE	2021	[119]
	International conference on automation, quality and testing, robotics.	IEEE	2014	[4]
	Robotics and Computer-Integrated Manufacturing	Elsevier	2019	[120]
	Procedia CIRP	Elsevier	2014	[78]
	International Conference on Fourth Industrial Revolution (ICFIR)	IEEE	2019	[121]
	Computers & Industrial Engineering	Elsevier	2020	[122]
	Sensors	MDPI	2021	[123]
	Reliability engineering & system safety	Elsevier	2019	[124]

However, the limitations of the aforementioned papers include the need to ensure safety and security in such systems, the difficulty of integrating legacy systems into the Industry 4.0 framework, and the lack of standardization in the implementation of cyber-physical systems in industrial automation. The development of standardized methods for the integration of cyber-physical systems in industrial automation, including the migration of old systems, could thus be the subject of future study. Furthermore, research might focus on creating efficient ways to guarantee security and safety in cyber-physical systems for industrial automation. This can entail creating integrated safety and security strategies or utilizing machine learning and artificial intelligence to recognize and stop cyberattacks.

3.9. CPS in Smart Manufacturing

Due to the modernization of the industry fueled by developments in technology and communication, cyber-physical systems (CPS) are becoming increasingly crucial in production. Nevertheless, the wide range of geometric and non-geometric procedure eligibility criteria used throughout the major groups of manufacturing methods, such as additive, subtractive, and deformation, makes smart manufacturing process sequence selection difficult to implement, which is a necessary step to achieving an autonomous CPS [125]. In [126], Manufacturing is the application of integrated software and hardware systems to increase productivity in the production of goods or the delivery of services. CPS is a core element of Intelligent Manufacturing. Automated storage systems are an important component of these systems, and they have managed a system named hierarchical and centralized control frameworks, as well as traditional automation coding methodologies. In [127], the authors presented first outcomes from combining Function Blocks and a CPS approach to design a flexible, modular, and distributed control technique for automated storage systems. The manufacturing CPS studies are still in their early stages, with most studies focusing on modeling, ideation, and exploitation strategies rather than reality [128]. An overview of cyber-physical product-service systems (CPSSs) and their use in a real-world scenario. They underline the importance of multimodal requirements engineering (RE) for hardware, software, and service components in successful and dynamic improvements to CPSSs in the industry [129]. Cyber-physical systems (CPS) of many high-tech manufacturing methodologies have presented new problems to service management in today's highly competitive Era of automation [130]. Effective Prognostics and health management (PHM) programs that can combine both individual machine degradation and diverse manufacturing models are essential. The author presented the ontological technology to describe the infrastructure of a smart manufacturing system [131]. The suggested framework has four layers: resource layer, rule layer, knowledge layer, and data layer. That relates to ideas, examples, logical processes, and real information, respectively. Additionally, it successfully exhibits smart resource reconstruction in manufacturing and related smart services. Cyber-physical integration, which is rapidly being accepted by manufacturers, is a key requirement for smart production. Cyber-physical systems (CPS) and digital twins (DTs) have gotten a lot of concern from practitioners and researchers in the business as the preferred method of integration [132]. Both CPS and DTs have two aspects in manufacturing: the physical portion and the cyber or digital portion. CPS and DTs can provide manufacturing systems with higher efficiency, resilience, and intelligence by creating feedback mechanisms in which physical processes influence cyber components and vice versa. These physical resources carry out production activities. The cyber or digital component includes intelligent data management, analysis, and computing skills as well as a variety of ubiquitous services and apps [133]. A broad survey of CPS in smart manufacturing as a combination of IoT and IoS is presented [134]. The authors suggested an adaptive production scheduling system for smart industries that is big data driven and CPS based. Also, they described four steps: PDA (production data acquisition), DDI (dynamic disturbance identification), SSA (scheduling strategy adjustment), and SSG (scheduling scheme generation) (SSG). The PDA and DDI phases continually monitor the manufacturing situation. A data-driven GA-KNN technique is used in the SSA and SSG phases to modify the original schedule in order to accommodate unpredictable disturbances and accomplish multi-objective optimization [135]. The source description of the above-mentioned papers is presented in Table 13.

Table 13. Research Category and Journal Details of CPS in Smart Manufacturing.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Manufacturing	Manufacturing Letters	Elsevier	2018	[125]
	Transactions on Internet and Information Systems	KSII	2014	[126]
	Emerging Technologies & Factory Automation	IEEE	2015	[127]
	Precision Engineering and Manufacturing-Green Technology	Springer	2016	[128]
	Automation Technology	J- STAGE	2017	[129]
	Intelligent Manufacturing	Springer	2019	[130]
	Transactions on Mechatronics	IEEE/ASME	2018	[131]
	Engineering	Elsevier	2019	[132]
	CIRP Annals	Elsevier	2016	[133]
	Journal of Intelligent Manufacturing	Springer	2019	[134]
	International Journal of Production Research	Taylor & Francis	2021	[135]

The shortcomings of the aforementioned papers are as follows:

- The dearth of standardization and interoperability between various systems and components in cyber-physical manufacturing systems;
- The requirement for effective and efficient process selection methods; and
- The difficulty of integrating cyber-physical product-service systems.

Future research could concentrate on creating frameworks and standards for standardization and interoperability to allow seamless integration and communication across various systems and components in cyber-physical manufacturing systems. More studies may also be conducted in the areas of creating sophisticated process selection techniques and combining cyber-physical product-service systems.

3.10. CPS in Smart Transportation

Transportation Cyber-Physical Systems (TCPS) have progressed in tandem with the global transportation industry. The rapid spread of TCPS presents us with a wealth of information and limitless opportunities for analyzing and comprehending the intricate intrinsic mechanism that drives the novel intelligence universe. TCPS also opens up several new application scenarios, including car safety, energy consumption, pollution reduction, and smart maintenance services [136]. Road traffic congestion is a fairly typical concern in our daily lives. A Dynamic En-route Decision Real-time Route guiding (DEDR) strategy was proposed to successfully minimize traffic problems due to sudden surges in car traffic while also reducing travel time and fuel usage [137]. DEDR considers the generation and transmission of actual traffic data via vehicle networks. In [138], it is concerned with traffic measuring in the field of transportation technology. They use the characteristics afforded by smart cyber-physical road systems to automatically collect traffic data to measure the number of cars moving from one geographical area to another. In [139], the authors investigate paramedic route selection with the help of a CPS that includes vehicular communications, alternative route optimization, and user interaction components for the optimal administration of intelligent transportation systems. This study can ensure alternative routing for paramedics with minimum latency, low price, and great resilience by using the minimum Steiner tree technique. In [140], the authors proposed a new car-following (CF) model that incorporates the impacts of lateral gaps and roadside device communication to describe the characteristics of EV traffic streams in transportation-cyber-physical systems. The perturbation techniques are used to assess the robustness of the suggested CF framework. Moreover, the energy usage of the EV traffic stream is analyzed, based on the drive cycles generated by the proposed design. Transportation-based cyber-physical systems (TCPS), usually called intelligent transportation systems (ITS). A model change from centralized cloud-scale computing to edge-centered fog computing (FC) models is required for geo-distributed ITS elements. In [141], the authors define the task processing needs of next-generation ITS systems and discuss the potential of FC-based approaches to satisfy those needs. The authors outline scenarios in which interconnected cars' unused communication and processing capability could be used to fill the role of FC structures. After that, the authors provide a SOA for FC-based Big Data Analytics in ITS systems. The authors also go through the potential drawbacks of employing linked automobiles as FC structures, as well as forthcoming research topics. While TCPSs have numerous advantages, one important hurdle that must be overcome for them to spread is their vulnerability to cyber-attacks. Using experimental models of TCPSs, the authors illustrate how Dynamic Watermarking can protect them from arbitrary sensor assaults [142]. The author used the Dynamic Watermarking methods to protect two transportation cyber-physical systems of recent interest such as (i) an adaptive cruise control system, and (ii) a self-driving vehicle system. The source description of the above-mentioned papers is presented in Table 14.

Table 14. Research Category and Journal Details of CPS in Transportation.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Transportation	Secure and Trustworthy Transportation Cyber-Physical Systems	Springer	2017	[136]
	Transactions on Vehicular Technology	IEEE	2016	[137]
	Transactions on Vehicular Technology	IEEE	2016	[138]
	Wireless Communications and Networking Conference	IEEE	2015	[139]
	Transactions on Intelligent Transportation Systems	IEEE	2017	[140]
	International Journal of Software Science and Computational Intelligence	GIG Global	2019	[141]
	Transactions on Cyber-Physical Systems	ACM	2019	[142]

The following are the limitations of the papers previously mentioned:

- CPS for transportation has given security and privacy concerns insufficient thought.
- Insufficient cyber-physical transportation system defenses against cyberattacks.
- Fog computing for vehicle networks in transportation cyber-physical systems has limited utility.
- Integration of electric vehicles in cyber-physical transportation networks has received little attention.

Creating more thorough security and privacy frameworks for transportation cyber-physical systems may be a future research focus. This may entail investigating novel defense techniques like fog computing for vehicle networks and defense based on dynamic watermarking. Future studies may also concentrate on the integration of electric vehicles and their effects on cyber-physical transportation networks.

3.11. CPS in Vehicular

Nowadays, CPS made huge responds in vehicle sectors. Vehicles and infrastructure have been modernized and connected to new physical sensors, coordinated sensors, self-driving cars and coordinated information exchange which led to some new security and privacy issues [143]. CPS has entered in autonomous vehicle for controlling and operation as well as consider the autonomous vehicle security, car functionalities, increased exposer to potential attackers and interaction with other systems. Additionally, Independent and overlapping CPS systems is installed in a car internally by many manufacturers reasoning of adaptive cruise control, anti-lock braking system, assistive parking system and so on. It also made the car more productive and technologically upgrade for using autonomous functionalities which enabled by the internal CPS controller technology [144]. Relatively, CPS proposed a framework for co-design optimization of the plant and controller parameters for an automated electric vehicle depends on vehicle's dynamic performance, drivability, and energy along with different driving styles, task time, actuator characteristics, energy consumption and processor workload which referees the use of CPS and the possibility is widely spread day by day in vehicle industry [145]. The period of digitalization, Vehicle distance changes into a cyber- process and a physical process which defines the notions of minimum safety distance, safety constants and then improves the dynamic vehicle safety distance calculation scheme using the vehicle velocity, acceleration, velocity difference and other parameters on the basis of CPS in the consecutive vehicle distance for scenarios of staying in the same lane and changing to a different lane [146]. Last but not least, CPS integrates the vehicular cyber system with the vehicular physical system for the optimization of the cooperative driving at traffic intersections which is controlling with network technology, electrical communication and automatic control for real-time monitoring the interconnection of network systems and computer components [147]. The source description of the above mentioned papers is presented in Table 15.

Table 15. Research Category and Journal Details of CPS in Vehicular.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
Vehicular	Journal of Industrial Integration and Management	World Scientific Publishing Co	2017	[143]
	7th International Symposium on Embedded Computing and System Design	IEEE	2017	[144]
	IEEE Transactions on Industrial Electronics	IEEE	2018	[145]
	Proceedings of the Institution of Civil Engineers—Transport	Institution of Civil Engineers	2016	[146]
	International Journal of Intelligent Transportation Systems Research	Springer	2019	[147]

Lack of established security frameworks for CPS-based systems, a lack of scalability and adaptability, and the need for more effective and efficient evaluation and optimization methodologies are some of the shortcomings of the aforementioned publications. The creation of comprehensive, standardized security frameworks for CPS-based systems that are scaleable and adaptable to multiple domains and applications may be a future research focus. In order to increase the performance and dependability of CPS-based systems for autonomous vehicles and industrial automation, there is also a need for more effective evaluation and optimization tools, such as machine learning and artificial intelligence.

3.12. CPS in Robotics

Robotics or Intelligence has a great relationship with CPS. CPS is going very fascinating and trending research in robotics form. We propose a new robot development methodology based on the abstraction of software and hardware components in the multi-tiered architecture of cyber physical robot systems that combine computing and physical resources [143]. Lots of industrial robot manufacturers like: ABB, Fanuc, Kawasaki, Kuka, and Yaskawa enabled a set of business model patterns for transforming product innovation in the industrial robot domain using CPS. Using industrial robots to their full capacity allows for the development of novel, supplementary goods and services as well as the creative use of industrial robots, which is defined as CPS in the framework of analysis [148]. Additionally, CPS is going to act as controllers using hardware and software for modular structure in different mobile robots for smart and automatic robotic system in a smart environment and provides for the full flexibility of modular robot cells to be used, each of which has a unique virtual representation of the needs and capabilities. The ability of the needed assembly tasks to be completed with the tools present in the robot cell is assessed based on the communication between the CPS and the fusion of the models [149]. By fusing the efficiency of robotic systems with the adaptability and dexterity of human man powers, human-robot interaction enables closer collaboration in assembly processes that need improved productivity. The biggest difficulty, meanwhile, is ensuring human safety when working close to robots. CPS should be used to integrate numerous hardware and software components to enable safe human-robot collaboration [120]. Authors dealt with a human robot collaborative application based on cognitive cyber-physical system [150]. The source description of the above-mentioned papers is presented in Table 16.

Table 16. Research Category and Journal Details of CPS in Robotics.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
CPS in Robotics	Journal of Industrial Integration and Management	World Scientific Publishing Co	2017	[143]
	19th Pacific Asia Conference on Information Systems	PACIS 2015 Proceedings	2015	[148]
	Mechatronics	Elsevier	2016	[149]
	Robotics and Computer-Integrated Manufacturing	Elsevier	2019	[120]
	IEEE International Conference on System of Systems Engineering (SoSE)	IEEE	2019	[150]

However, the above-mentioned papers have limitations including

- Lack of standardization in CPS platforms and designs for industrial robots, which inhibits interoperability and restricts scalability, is one of the shortcomings of the aforementioned publications.
- Paying insufficient attention to security and safety concerns with industrial robots based on CPS, which could have grave repercussions.
- There is a need for additional study on human-robot collaboration in shared workspaces, including the creation of CPS-based systems for effective and secure collaboration. The development of standardized CPS platforms and architectures for industrial robots that incorporate cutting-edge security and safety measures to enable safe and effective human-robot collaboration in shared workspaces could be one future research direction. The performance and scalability of industrial robots could be improved while assuring their security and safety by investigating new CPS technologies like edge computing and AI.

In order to ensure the dependability and performance of industrial robots based on CPS in real-world settings, research may also concentrate on developing novel techniques for verification and validation.

3.13. CPS in Mobile Devices

Two Smartphones are categorized in CPS-based smart devices for interpret data and communication. A growing mobile cyber-physical system that enables mobile users to efficiently perform mobile cloud sensing activity [143]. A cyber-physical system (CPS) approach is expected to prevent potential contact collisions by issuing warnings to construction entities that exhibit a high probability of imminent hazardous proximity and created SCSAS, a proximity warning application that works on a client-server approach between smartphone application clients and a central server to notify construction workers and equipment operators of potentially dangerous circumstances [151]. Additionally, Vehicular networking systems (VNS) have been a prominent study field in mobile CPS as a typical application domain in ITS. Yet because mobile CPS is mobile by nature, VNS in mobile CPS may have more varied application features, and with the aid of mobile CPS, MES may be applied in more application fields than the e-learning platform [152]. A model-based signature analysis, which integrates models of physical processes, networks, and computing resources, may be used to model and simulate CPS's performance. Smartphones, which have a broad range of applications given the computing power and memory resources, as well as a host of different sensors like an accelerometer, gyroscope, and GPS, are examples of mobile CPS that have inherent mobility in physical systems and are growing in popularity. In the IT business, simulating acceleration profiles for various automobile types and road characteristics is becoming more and more common [153]. The source description of the above-mentioned papers is given in Table 17.

Table 17. Research Category and Journal Details of CPS in Mobile Devices.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
CPS in devices	Journal of Industrial Integration and Management	World Scientific Publishing Co	2017	[143]
	ICCCBE2016.	Osaka University	2016	[151]
	IEEE ACCESS	IEEE	2017	[152]
	2012 Sixth International Conference on Sensing Technology (ICST)	IEEE	2012	[153]

The combined constraints of these publications include issues with data security, privacy, and scalability as well as a lack of defined frameworks and protocols for creating and integrating mobile cyber-physical systems. The development of standardized frameworks and protocols, as well as addressing the security and privacy issues related to gathering and processing sensitive data on mobile devices, could be the main areas of future research. This will enable the seamless integration of mobile cyber-physical systems. Moreover, research might concentrate on creating scalable solutions that would enable the widespread deployment of mobile cyber-physical systems.

3.14. CPS in Smart Home

Cyber physical system (CPS) is widely using in smart hut day by day. Smart home equipped with sensors and electronic devices as a CPS offers great research perspective to explore communication, computation and controlling of physical devices by using real-time processing and analytic. Soundly, CPS provides different sort of features for smart home. Voice control home is one of them where includes stream processing, data collection, identification of actions from voice utterance and event-based real-time decision making and also deployment of various sensors and actuators for performing various actions based on voice commands [154]. For integrating items in a networked smart home, there is also an application known as a CPS framework. To enhance surveillance, healthcare, and security, numerous sensors and input devices are installed in the residences within a community. Also, studies have revealed that a significant amount of the energy utilized in buildings occurs at night and is mostly needed to run networking equipment. The quantity of greenhouse gas emissions can be decreased by designing a cyber-physical energy system that optimizes energy use by scheduling and implementing sleep modes for equipment in accordance with real-time price transmissions [155]. During to make an autonomous system for smart home faced challenges during the design and implementation of such a system, such as Portability, Timing, Prediction, and Integrity which is also solved by the cyber physical system interface [156]. However, for integrating CPS, a comprehensive architecture and platform is still attractive which is the concept of Smart Cyber Society, propelling the concept of smart home. Smart Cyber Society consists of three networked domains, such as cyber home domain (networked-home), cyber society domain (networked of various societies, like: hospitals, police station, and fire brigade), and cyber mobile domain (networked of vehicles). Overall, the use of CPS for smart home is growing drastically [157]. The source description of the above-mentioned papers is presented in Table 18.

Table 18. Research Category and Journal Details of CPS in Smart Home.

Category of Research	Journal/Conference Name	Publisher	Year of Publication	Source
CPS in Smart Home	REKA ELKOMIKA: Jurnal Pengabdian kepada Masyarakat	Institut Teknologi Nasional Bandung	2020	[154]
	19th International Conference on Distributed Computing and Networking	ACM Digital Library	2018	[155]
	IEEE 37th International Conference on Distributed Computing Systems Workshops	IEEE	2017	[156]
	Future Generation Computer Systems	Elsevier	2016	[157]

The stated papers' shortcomings include the absence of standards in CPS design and implementation, the difficulty of achieving interoperability between multiple CPS components, and the requirement for more effective security and privacy controls in CPS. The development of standardized design frameworks and guidelines for CPS as well as the investigation of new technologies and methods for interoperability and security in CPS may be the subject of future study. The usefulness and user acceptance of CPS in other applications, such as smart homes and smart cities, can also be investigated in future studies.

4. Discussion and Guideline for the Future Work

The convergence of control, communication, computation, and information is known as a cyber-physical system. CPS has lots of amenities including creativity in various services and Applications, smart features in technology, lower cost in operation, and less time-consuming. In this paper, 14 applications of CPS were discussed which means in the processing of digitalization has a very effective consideration. Adobe researches in CPS have a wide range of goals, including enhancing the process safety and reliability, minimizing resource consumption, and boosting their productivity. On the other hand, CPS also has many obstacles on the way to implementation such as real-time data transmission and collaboration between multiple hardware and software components are extremely difficult for cyber-physical systems. However, the most popular keyword combination was CPS and design, even though there is no established concept or approach for creating a CPS, only a few traits and broad layouts have been offered. A competent CPS design technique will standardize and have a favorable impact on the major issues, allowing any form of system to be interconnected.

CPS is also facing challenges in terms of security, privacy, and efficacy issue because of its vulnerability. There are many characteristics behind insecurity issues including accessing the internet, implementation of unsecured connection protocols, and frequent use of the legacy system.

All the pieces of literature in this paper introduce many new technologies like big data, IoT, cloud computing, WAN, WSN, and so on. All these smart innovation technologies are strongly connected. However, they lack in considering and incorporating the most recent technologies, standardizing, and integrating and many of them need extensive testing.

Day by day, CPS has become the heart of Industry 4.0 due to its flexibility and many other beneficial perspectives. In the near future, CPS will be very obvious in every smart thing, including smart cities, smart homes, smart vehicles, robotics, and many other appliances in the industry. In global digitization, CPS has played a great role in every aspect. By deploying CPS with production, services, and logistics in the conventional factories and transforming it into the industry 4.0 factory as a result they are getting economic advancement. Many countries in the world started to do CPS research and its application for example "Made in China 2025" project in China and also Germany has a huge implementation of CPS in Industry 4.0. In the future, CPS will accumulate the information from the factory appliance and every aspect of the industrial environment, including smart machines, warehouse systems, manufacturing facilities, business operations, and so on, will be able to automatically share data, triggering actions, and monitoring each other. Cloud computing is a very fancy technology in the modern world and it offers people to access various perspectives on the internet. In the future, CPS based cloud give manifold services to the people including cost analysis, forecast monitoring, traffic congestion, and so on. To provide this type of service, high level of cloud computing is much needed. Table 19 shows the comparison of studies in advantages and disadvantages.

Table 19. Comparison study of several areas of CPS.

Papers	Uses	Advantages	Disadvantages
[64]	A modelling approach for Potential Cyber Attack Detection	• Can protect data both in rest and transit • Provides real-time threat detection and mitigation techniques	• The System will be quite costly • Can be very complex for large systems
[65]	A modelling approach for Potential Cyber Attack Detection	• Can identify nonlinear relationships among inputs and outputs which is suited for aviation • Exogenous variables help considering external factors • Easy maintenance	• Can be computationally expensive and so without careful designing it can be inappropriate for real time systems
[68]	A comprehensive approach to protect the whole system	• Besides of providing protections it can improve operational efficiency • Provides real time protection	• Unable to handle novel attacks • High maintenance cost
[85]	A modelling approach for efficient and robust energy management system	• Considers multiple objectives such as energy efficiency, battery life, driving performance, to optimize Energy Management System • Robust against uncertainties	• Complex to implement • Computationally expensive and not feasible for real-time systems
[87]	A modelling approach for intrusion Detection	• More realistic solution for intrusion detection in power sector • Provides improved security	• Can only detect intrusion; no prevention or mitigation strategy • Test bed simulation can be biased
[88]	A software toolkit for energy efficiency	• Easy to implement and user friendly • Supports modularity and customizability	• Not suitable for large scale systems • Has limited scope
[137]	A real time route guidance system	• Provides flexible real time route guidance • Scalable and can be integrated with other CPS • Cost effective	• Efficiency depends on real time traffic data • Less reliable as decisions may be affected by external factors
[138]	A privacy preserving traffic measuring system	• Preserves privacy • Real time data transmission using wireless technologies • Low cost and easy implementation	• Limited accuracy in urban area due to dependency on GPS • Not always efficient as efficiency depends on sufficient number of vehicles' cooperation

Table 19. *Cont.*

Papers	Uses	Advantages	Disadvantages
[139]	A safe and customizable alternating route suggesting system for paramedics in urban condition	• Suggests safest alternating route • Fast suggestion • Customizable according to specific needs	• Depends on accurate real time traffic data • Designed only for urban paramedics
[140]	Helps electric vehicle (EV) for efficient movement	• Ensures energy efficiency in EV and real time adaptable • Improves traffic flow and reduce travel time	• May raise safety concern as it tries to reduce gaps among vehicles • Not easy to implement
[141]	Brings vehicles in a fog computing system for transportation	• Supports efficient real time systems as it uses fog technology • Optimizes resources and environment friendly	• Limited computational resources available in vehicle may be problematic • Low coverage issues
[142]	Protects transportation CPS from cyber attacks	• Uses robust technology to prevent from cyber attack • Low computational overhead	• May introduce false positives • Only designed for specific systems

5. Conclusions

Cyber-physical systems are the building blocks for the next generation of smart systems with enormous economic implications. The cyber and physical worlds enable the development of technologies that stimulate innovation across a wide range of industries, resulting in the formation of totally new marketplaces and infrastructures. This article highlights the background of CPS and existing research on CPS from an education, industry, and corporate standpoint. This paper elucidates 14 applications of CPS that are playing a very crucial role in modern technology and all the application's content are summarized. Subsequently, the research challenges and future research work are described as well, which will help the scholars and practitioners for further study. This paper selected several databases for extensive reviews of CPS because it's a new area of research where lots of queries are arising and facing new challenges that CPS needs to solve. The main purpose of this article is to the discussion about CPS applications, figure out the problems, and provide a significant approach to the professionals.

Author Contributions: Conceptualization, M.M.I.; Methodology and software, M.M.I. and S.H.; validation and formal analysis, M.M.I., M.H. and M.N.A.; resources, M.M.I. and S.H.; data curation, M.M.I. and S.H.; writing—original draft preparation, M.M.I., S.H. and M.B.J.; writing—review and editing, M.B.J., A.W.M., M.M.I., M.J.F. and S.H.; visualization, M.B.J., A.W.M., M.J.F. and M.M.I.; supervision, M.N.A.; Funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the grant Universiti of Malaysia Sabah: DFK2005.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jiang, J.R. An improved cyber-physical systems architecture for Industry 4.0 smart factories. *Adv. Mech. Eng.* **2018**, *10*, 1687814018784192. [CrossRef]
2. Cicconi, P.; Russo, A.C.; Germani, M.; Prist, M.; Pallotta, E.; Monteriu, A. Cyber-physical system integration for industry 4.0: Modelling and simulation of an induction heating process for aluminium-steel molds in footwear soles manufacturing. In Proceedings of the 2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI), Modena, Italy, 11–13 September 2017; pp. 1–6.
3. Brettel, M.; Friederichsen, N.; Keller, M.; Rosenberg, M. How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. *FormaMente* **2017**, *12*, 37–44.
4. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
5. Darwish, A.; Hassanien, A.E. Cyber Physical Systems Design, Methodology, and Integration: The Current Status and Future Outlook. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1541–1556. [CrossRef]
6. Pivoto, D.G.; de Almeida, L.F.; da Rosa Righi, R.; Rodrigues, J.J.; Lugli, A.B.; Alberti, A.M. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *J. Manuf. Syst.* **2021**, *58*, 176–192. [CrossRef]
7. Czekster, R.M.; Metere, R.; Morisset, C. Incorporating Cyber Threat Intelligence into Complex Cyber-Physical Systems: A STIX Model for Active Buildings. *Appl. Sci.* **2022**, *12*, 5005. [CrossRef]
8. Lee, J.; Bagheri, B.; Kao, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
9. Kos, A.; Tomažič, S.; Salom, J.; Trifunovic, N.; Valero, M.; Milutinovic, V. New benchmarking methodology and programming model for big data processing. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 271752. [CrossRef]
10. Islam, M.M.; Uddin, J.; Kashem, M.A.; Rabbi, F.; Hasnat, M.W. Design and implementation of an IoT system for predicting aqua fisheries using arduino and KNN. In Proceedings of the Intelligent Human Computer Interaction: 12th International Conference, IHCI 2020, Daegu, Republic of Korea, 24–26 November 2020; Springer: Berlin, Germany, 2021; pp. 108–118.
11. Reis, J.Z.; Gonçalves, R.F. The role of internet of services (ios) on industry 4.0 through the service oriented architecture (soa). In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Seoul, Republic of Korea, 26–30 August 2018; pp. 20–26.
12. Shafiq, S.I.; Szczerbicki, E.; Sanin, C. Manufacturing data analysis in internet of things/internet of data (IoT/IoD) scenario. *Cybern. Syst.* **2018**, *49*, 280–295. [CrossRef]
13. Kocabay, A.; Javadi, H. Cyber-Physical Systems—Manufacturing Applications. In *Industry 4.0*; Springer: Berlin, Germany, 2023; pp. 35–56.
14. Turygin, Y.; Božek, P.; Nikitin, Y.; Sosnovich, E.; Abramov, A. Enhancing the reliability of mobile robots control process via reverse validation. *Int. J. Adv. Robot. Syst.* **2016**, *13*, 1729881416680521. [CrossRef]
15. Božek, P.; Bezák, P.; Nikitin, Y.; Fedorko, G.; Fabian, M. Increasing the production system productivity using inertial navigation. *Manuf. Technol.* **2015**, *15*, 274–278. [CrossRef]
16. Colombo, A.W.; Karnouskos, S.; Kaynak, O.; Shi, Y.; Yin, S. Industrial cyberphysical systems: A backbone of the fourth industrial revolution. *IEEE Ind. Electron. Mag.* **2017**, *11*, 6–16. [CrossRef]
17. Leitao, P.; Karnouskos, S.; Ribeiro, L.; Lee, J.; Strasser, T.; Colombo, A.W. Smart agents in industrial cyber–physical systems. *Proc. IEEE* **2016**, *104*, 1086–1101. [CrossRef]
18. Ding, D.; Han, Q.L.; Wang, Z.; Ge, X. A survey on model-based distributed control and filtering for industrial cyber-physical systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 2483–2499. [CrossRef]
19. Jiang, X.; Li, S. Plume front tracking in unknown environments by estimation and control. *IEEE Trans. Ind. Inform.* **2018**, *15*, 911–921. [CrossRef]
20. Wang, L.; Törngren, M.; Onori, M. Current status and advancement of cyber-physical systems in manufacturing. *J. Manuf. Syst.* **2015**, *37*, 517–527. [CrossRef]
21. Cassoli, B.B.; Jourdan, N.; Nguyen, P.H.; Sen, S.; Garcia-Ceja, E.; Metternich, J. Frameworks for data-driven quality management in cyber-physical systems for manufacturing: A systematic review. *Procedia CIRP* **2022**, *112*, 567–572. [CrossRef]
22. Napoleone, A.; Negri, E.; Macchi, M.; Pozzetti, A. How the technologies underlying cyber-physical systems support the reconfigurability capability in manufacturing: A literature review. *Int. J. Prod. Res.* **2022**, *61*, 3122–3144. [CrossRef]
23. Zhu, Q.; Rieger, C.; Başar, T. A hierarchical security architecture for cyber-physical systems. In Proceedings of the 2011 4th International Symposium on Resilient Control Systems, Boise, ID, USA, 9–11 August 2011; pp. 15–20.
24. Senyondo, H. Formal Analysis and Verification of Cyber-Physical Systems for the Smart Grid. Ph.D. Thesis, University of Miami, Coral Gables, FL, USA, 2015.
25. Chen, S.; Ma, M.; Luo, Z. An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems. *Secur. Commun. Netw.* **2016**, *9*, 1146–1157. [CrossRef]
26. Kalogeras, G.; Anagnostopoulos, C.; Alexakos, C.; Kalogeras, A.; Mylonas, G. Cyber Physical Systems for Smarter Society: A use case in the manufacturing sector. In Proceedings of the 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), Jeju, Republic of Korea, 13–15 August 2021; pp. 371–376.

27. Passarini, R.F.; Farines, J.M.; Fernandes, J.M.; Becker, L.B. Cyber-physical systems design: Transition from functional to architectural models. *Des. Autom. Embed. Syst.* **2015**, *19*, 345–366. [CrossRef]
28. Zhang, Y.; Xu, Q.; Guan, X.; Chen, C.; Li, M. Wireless/wired integrated transmission for industrial cyber-physical systems: Risk-sensitive co-design of 5G and TSN protocols. *Sci. China Inf. Sci.* **2022**, *65*, 1–16. [CrossRef]
29. Hasan, M.K.; Habib, A.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *J. Netw. Comput. Appl.* **2022**, *209*, 103540. [CrossRef]
30. Bordel, B.; Alcarria, R.; Martín, D.; Robles, T.; de Rivera, D.S. Self-configuration in humanized cyber-physical systems. *J. Ambient Intell. Humaniz. Comput.* **2017**, *8*, 485–496. [CrossRef]
31. Bradley, J.M.; Atkins, E.M. Optimization and control of cyber-physical vehicle systems. *Sensors* **2015**, *15*, 23020–23049. [CrossRef] [PubMed]
32. Abdel-Basset, M.; Mohamed, R.; Mohammad, N.; Sallam, K.; Moustafa, N. An Adaptive Cuckoo Search-Based Optimization Model for Addressing Cyber-Physical Security Problems. *Mathematics* **2021**, *9*, 1140. [CrossRef]
33. Huang, J.; Zhu, Y.; Cheng, B.; Lin, C.; Chen, J. A PetriNet-based approach for supporting traceability in cyber-physical manufacturing systems. *Sensors* **2016**, *16*, 382. [CrossRef]
34. Niggemann, O.; Frey, C. Data-driven anomaly detection in cyber-physical production systems. *at-Automatisierungstechnik* **2015**, *63*, 821–832. [CrossRef]
35. Yang, Q.; Liu, Y.; Yu, W.; An, D.; Yang, X.; Lin, J. On data integrity attacks against optimal power flow in power grid systems. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 1008–1009.
36. Du, C.; Tan, L.; Dong, Y. Period selection for integrated controller tasks in cyber-physical systems. *Chin. J. Aeronaut.* **2015**, *28*, 894–902. [CrossRef]
37. Bai, Y.; Park, J.; Tehranipoor, M.; Forte, D. Real-time instruction-level verification of remote IoT/CPS devices via side channels. *Discov. Internet Things* **2022**, *2*, 1–19. [CrossRef]
38. Chen, L.; Yue, D.; Dou, C.; Cheng, Z.; Chen, J. Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters. *Int. J. Electr. Power Energy Syst.* **2020**, *114*, 105374. [CrossRef]
39. Shakshuki, E.M.; Malik, H.; Sheltami, T. WSN in cyber physical systems: Enhanced energy management routing approach using software agents. *Future Gener. Comput. Syst.* **2014**, *31*, 93–104. [CrossRef]
40. Zeng, J.; Yang, L.T.; Ma, J. A system-level modeling and design for cyber-physical-social systems. *ACM Trans. Embed. Comput. Syst. (TECS)* **2016**, *15*, 1–26. [CrossRef]
41. Ali, S.; Qaisar, S.B.; Saeed, H.; Farhan Khan, M.; Naeem, M.; Anpalagan, A. Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring. *Sensors* **2015**, *15*, 7172–7205. [CrossRef] [PubMed]
42. Huang, S.; Tao, M. Competitive swarm optimizer based gateway deployment algorithm in cyber-physical systems. *Sensors* **2017**, *17*, 209. [CrossRef] [PubMed]
43. Huang, R.; Chu, X.; Zhang, J.; Hu, Y.H. Scale-free topology optimization for software-defined wireless sensor networks: A cyber-physical system. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717713626. [CrossRef]
44. Singh, H. Big data, industry 4.0 and cyber-physical systems integration: A smart industry context. *Mater. Today: Proc.* **2021**, *46*, 157–162. [CrossRef]
45. Bhuiyan, M.Z.A.; Wu, J.; Wang, G.; Cao, J. Sensing and decision making in cyber-physical systems: The case of structural event monitoring. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2103–2114. [CrossRef]
46. De Persis, C.; Postoyan, R. A Lyapunov redesign of coordination algorithms for cyber-physical systems. *IEEE Trans. Autom. Control* **2016**, *62*, 808–823. [CrossRef]
47. Cao, X.; Cheng, P.; Chen, J.; Ge, S.S.; Cheng, Y.; Sun, Y. Cognitive radio based state estimation in cyber-physical systems. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 489–502. [CrossRef]
48. Deshmukh, S.; Natarajan, B.; Pahwa, A. State estimation over a lossy network in spatially distributed cyber-physical systems. *IEEE Trans. Signal Process.* **2014**, *62*, 3911–3923. [CrossRef]
49. Park, K.J.; Zheng, R.; Liu, X. Cyber-physical systems: Milestones and research challenges. *Comput. Commun.* **2012**, *36*, 1–7. [CrossRef]
50. Sampigethaya, K.; Poovendran, R. Aviation cyber–physical systems: Foundations for future aircraft and air transport. *Proc. IEEE* **2013**, *101*, 1834–1855. [CrossRef]
51. Huang, Y.; Zhao, M.; Xue, C. Joint WCET and update activity minimization for cyber-physical systems. *ACM Trans. Embed. Comput. Syst. (TECS)* **2015**, *14*, 1–21. [CrossRef]
52. Squire, R.; Song, H. Cyber-physical systems opportunities in the chemical industry: A security and emergency management example. *Process Saf. Prog.* **2014**, *33*, 329–332. [CrossRef]
53. Hassan, B.H.; Narayan, A.; Babazadeh, D.; Klaes, M.; Lehnhoff, S. Performance assessment of state estimation in cyber-physical energy systems. In Proceedings of the 2021 IEEE Madrid PowerTech, Madrid, Spain, 28 June–2 July 2021; pp. 1–6.
54. Cheng, P.; Shi, L.; Sinopoli, B. Guest editorial special issue on secure control of cyber-physical systems. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 1–3. [CrossRef]
55. Akter, F.; Kashem, M.A.; Islam, M.M.; Chowdhury, M.A.; Rokunojjaman, M.; Uddin, J. Cyber-Physical System (CPS) Based Heart Disease's Prediction Model for Community Clinic Using Machine Learning Classifiers. *J. Hunan Univ. Nat. Sci.* **2021**, *48*, 86–93.

56. Broo, D.G.; Boman, U.; Törngren, M. Cyber-physical systems research and education in 2030: Scenarios and strategies. *J. Ind. Inf. Integr.* **2021**, *21*, 100192.
57. Dafflon, B.; Moalla, N.; Ouzrout, Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. *Int. J. Adv. Manuf. Technol.* **2021**, *113*, 2395–2412. [CrossRef]
58. Jen-Yi, C.; Chuan-His, L.; Yi-Hsin, Y. The Study of Indigenous Students' Learning Effect on Geometry Course with CPS Mobile Learning and Atayal Culture. *Situations* **2020**, *5*, 7. [CrossRef]
59. Zhou, J.; Zhou, Y.; Wang, B.; Zang, J. Human-cyber-physical systems (HCPSs) in the context of new-generation intelligent manufacturing. *Engineering* **2019**, *5*, 624–636. [CrossRef]
60. Jain, P.; Aggarwal, P.K.; Chaudhary, P.; Makar, K.; Mehta, J.; Garg, R. Convergence of IoT and CPS in Robotics. In *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*; Springer: Berlin, Germany, 2021; pp. 15–30.
61. Feng, Y.; An, X.; Li, S. Application of context-aware in intelligent transportation CPS. In Proceedings of the 2017 36th Chinese Control Conference (CCC), Dalian, China, 26–28 July 2017.
62. Naufal, J.K.; Camargo, J.B.; Vismari, L.F.; de Almeida, J.R.; Molina, C.; González, R.I.R.; Inam, R.; Fersman, E. A 2 cps: A vehicle-centric safety conceptual framework for autonomous transport systems. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 1925–1939. [CrossRef]
63. Sampigethaya, K.; Poovendran, R. Cyber-physical system framework for future aircraft and air traffic control. In Proceedings of the 2012 IEEE Aerospace Conference, Big Sky, MT, USA, 4–10 March 2012; pp. 1–9.
64. Alsulami, A.A.; Zein-Sabatto, S. Detection and Defense from False Data Injection Attacks In Aviation Cyber-Physical Systems Using Artificial Immune Systems. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 69–75.
65. Alsulami, A.A.; Zein-Sabatto, S. Defending Aviation Cyber-Physical Systems from DDOS Attack Using NARX Model. In *Advances in Artificial Intelligence and Applied Cognitive Computing*; Springer: Berlin, Germany, 2021; pp. 1107–1122.
66. Nur, A.Y.; Tozal, M.E. Defending cyber-physical systems against dos attacks. In Proceedings of the 2016 IEEE International Conference on Smart Computing (SMARTCOMP), St Louis, MO, USA, 18–20 May 2016.
67. Wang, H.; Zhao, H.; Zhang, J.; Ma, D.; Li, J.; Wei, J. Survey on unmanned aerial vehicle networks: A cyber physical system perspective. *IEEE Commun. Surv. Tutorials* **2019**, *22*, 1027–1070. [CrossRef]
68. Alrefaei, F.; Alzahrani, A.; Song, H.; Zohdy, M.; Alrefaei, S. Cyber Physical Systems, a New Challenge and Security Issue for the Aviation. In Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021; pp. 1–5.
69. Dave, G.; Choudhary, G.; Sihag, V.; You, I.; Choo, K.K.R. Cyber security challenges in aviation communication, navigation, and surveillance. *Comput. Secur.* **2022**, *112*, 102516. [CrossRef]
70. Rong-xiao, G.; Ji-wei, T.; Bu-hong, W.; Fu-te, S. Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective. In Proceedings of the 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 27–29 March 2020.
71. Bera, B.; Das, A.K.; Garg, S.; Piran, M.J.; Hossain, M.S. Access control protocol for battlefield surveillance in drone-assisted IoT environment. *IEEE Internet Things J.* **2021**, *9*, 2708–2721. [CrossRef]
72. Vaseashta, A.; Kudaverdyan, S.; Tsaturyan, S.; Bölgen, N. Cyber-Physical Systems to Counter CBRN Threats–Sensing Payload Capabilities in Aerial Platforms for Real-Time Monitoring and Analysis. In *Proceedings of the Nanoscience and Nanotechnology in Security and Protection against CBRN Threats*; Springer: Berlin, Germany, 2020; pp. 3–20.
73. Ji, X.; He, G.; Xu, J.; Guo, Y. Study on the mode of intelligent chemical industry based on cyber-physical system and its implementation. *Adv. Eng. Softw.* **2016**, *99*, 18–26. [CrossRef]
74. He, G.; Dang, Y.; Zhou, L.; Dai, Y.; Que, Y.; Ji, X. Architecture model proposal of innovative intelligent manufacturing in the chemical industry based on multi-scale integration and key technologies. *Comput. Chem. Eng.* **2020**, *141*, 106967. [CrossRef]
75. Oliveira, L.M.; Dias, R.; Rebello, C.M.; Martins, M.A.; Rodrigues, A.E.; Ribeiro, A.M.; Nogueira, I.B. Artificial Intelligence and Cyber-Physical Systems: A Review and Perspectives for the Future in the Chemical Industry. *AI* **2021**, *2*, 429–443. [CrossRef]
76. Sánchez, A.S.; Oliveira-Esquerre, K.P.; dos Reis Nogueira, I.B.; de Jong, P.; Filho, A.A. Water loss management through smart water systems. In *Smart Village Technology*; Springer: Berlin, Germany, 2020; pp. 233–266.
77. Ohshima, M.; Tanigaki, M. Quality control of polymer production processes. *J. Process Control* **2000**, *10*, 135–148. [CrossRef]
78. Monostori, L. Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia Cirp* **2014**, *17*, 9–13.
79. Ren, S.; Feng, D.; Sun, Z.; Zhang, R.; Chen, L. A framework for shopfloor material delivery based on real-time manufacturing big data. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 1093–1108. [CrossRef]
80. Majeed, A.; Lv, J.; Peng, T. A framework for big data driven process analysis and optimization for additive manufacturing. *Rapid Prototyp. J.* **2018**, *24*, 735–747. [CrossRef]
81. Zhang, Y.; Ren, S.; Liu, Y.; Sakao, T.; Huisingh, D. A framework for Big Data driven product lifecycle management. *J. Clean. Prod.* **2017**, *159*, 229–240. [CrossRef]
82. Macana, C.A.; Quijano, N.; Mojica-Nava, E. A survey on cyber physical energy systems and their applications on smart grids. In Proceedings of the 2011 IEEE PES Conference on Innovative Smart Grid Technologies Latin America (ISGT LA), Medellin, Colombia, 19–21 October 2011; pp. 1–6.

83. Behl, M.; Jain, A.; Mangharam, R. Data-driven modeling, control and tools for cyber-physical energy systems. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016.
84. Ma, S.; Zhang, Y.; Lv, J.; Yang, H.; Wu, J. Energy-cyber-physical system enabled management for energy-intensive manufacturing industries. *J. Clean. Prod.* **2019**, *226*, 892–903. [CrossRef]
85. Li, S.; He, H.; Zhao, P. Energy management for hybrid energy storage system in electric vehicle: A cyber-physical system perspective. *Energy* **2021**, *230*, 120890. [CrossRef]
86. Cui, H.; Li, F.; Tomsovic, K. Cyber-physical system testbed for power system monitoring and wide-area control verification. *IET Energy Syst. Integr.* **2020**, *2*, 32–39. [CrossRef]
87. Adhikari, U.; Morris, T.; Pan, S. A cyber-physical power system test bed for intrusion detection systems. In Proceedings of the 2014 IEEE PES General Meeting | Conference & Exposition, Calgary, AB, Canada, 26–30 July 2009.
88. Antonioli, D.; Tippenhauer, N. MiniCPS: A toolkit for security research on CPS networks. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy*; Association for Computing Machinery: New York, NY, USA, 2015.
89. Thiede, S. Environmental sustainability of cyber physical production systems. *Procedia CIRP* **2018**, *69*, 644–649. [CrossRef]
90. Rad, C.R.; Hancu, O.; Takacs, I.; Olteanu, G. Smart monitoring of potato crop: A cyber-physical system architecture model in the field of precision agriculture. *Agric. Agric. Sci. Procedia* **2015**, *6*, 73–79. [CrossRef]
91. Ahmad, I.; Pothuganti, K. Smart Field Monitoring using ToxTrac: A Cyber-Physical System Approach in Agriculture. In Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 10–12 September 2020.
92. Reganold, J.; Wachter, J. Organic agriculture in the twenty-first century. *Nat. Plants* **2016**, *2*, 1–8. [CrossRef]
93. PytlikZillig, L.M.; Duncan, B.; Elbaum, S.; Detweiler, C. A drone by any other name: Purposes, end-user trustworthiness, and framing, but not terminology, affect public support for drones. *IEEE Technol. Soc. Mag.* **2018**, *37*, 80–91. [CrossRef]
94. Fulford, A.; Culman, S. Over-fertilization does not build soil test phosphorus and potassium in Ohio. *Agron. J.* **2018**, *110*, 56–65. [CrossRef]
95. Carmo, M.; Garcia-Ruiz, R.; Ferreira, M.I.; Domingos, T. The NPK soil nutrient balance of Portuguese cropland in the 1950s: The transition from organic to chemical fertilization. *Sci. Rep.* **2017**, *7*, 1–14. [CrossRef]
96. Mirkouei, A. A cyber-physical analyzer system for precision agriculture. *J. Environ. Sci. Curr. Res* **2020**, *3*, 016. [CrossRef] [PubMed]
97. Ferdousi, R.; Hossain, M.; El Saddik, A. Early-stage risk prediction of non-communicable disease using machine learning in health cps. *IEEE Access* **2021**, *9*, 96823–96837. [CrossRef]
98. Gai, K.; Qiu, M.; Zhao, H.; Sun, X. Resource management in sustainable cyber-physical systems using heterogeneous cloud computing. *IEEE Trans. Sustain. Comput.* **2017**, *3*, 60–72. [CrossRef]
99. Dey, N.; Ashour, A.S.; Shi, F.; Fong, S.J.; Tavares, R.S. Medical cyber-physical systems: A survey. *J. Med Syst.* **2018**, *42*, 1–13. [CrossRef] [PubMed]
100. Riad, K.; Hamza, R.; Yan, H. Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access* **2019**, *7*, 86384–86393. [CrossRef]
101. Huang, Z.; Lai, J.; Chen, W.; Li, T.; Xiang, Y. Data security against receiver corruptions: SOA security for receivers from simulatable DEMs. *Inf. Sci.* **2019**, *471*, 201–215. [CrossRef]
102. Haque, S.; Aziz, S. False alarm detection in cyber-physical systems for healthcare applications. In Proceedings of the Aasri Procedia, Singapore, 30 June–5 July 2013; Volume 5, pp. 54–61.
103. Loubet, G.; Takacs, A.; Dragomirescu, D. Implementation of a battery-free wireless sensor for cyber-physical systems dedicated to structural health monitoring applications. *IEEE Access* **2019**, *7*, 24679–24690. [CrossRef]
104. Verma, P.; Sood, S.; Kaur, H. A Fog-Cloud based cyber physical system for Ulcerative Colitis diagnosis and stage classification and management. *Microprocess. Microsystems* **2020**, *72*, 102929. [CrossRef]
105. Feng, J.; Zhu, F.; Li, P.; Davari, H.; Lee, J. Development of An Integrated Framework for Cyber Physical System (CPS)-Enabled Rehabilitation System. *Int. J. Progn. Health Manag.* **2021**, *12*, 1–10. [CrossRef]
106. Singh, K.; Sood, S. Optical fog-assisted cyber-physical system for intelligent surveillance in the education system. *Comput. Appl. Eng. Educ.* **2020**, *28*, 692–704. [CrossRef]
107. Perry-Hazan, L.; Birnhack, M. Privacy, CCTV, and school surveillance in the shadow of imagined law. *Law Soc. Rev.* **2016**, *50*, 415–449. [CrossRef]
108. Serdyukov, P. Innovation in education: What works, what doesn't, and what to do about it? *J. Res. Innov. Teach. Learn.* **2017**, *10*, 4–33. [CrossRef]
109. Stankovic, J.A.; Sturges, J.W.; Eisenberg, J. A 21st Century Cyber-Physical Systems Education. *Computer* **2017**, *50*, 82–85. [CrossRef]
110. Mazumder, S.K.; Kulkarni, A.; Sahoo, S.; Blaabjerg, F.; Mantooth, H.A.; Balda, J.C.; Zhao, Y.; Ramos-Ruiz, J.A.; Enjeti, P.N.; Kumar, P.R.; et al. A review of current research trends in power-electronic innovations in cyber-physical systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 5146–5163. [CrossRef]
111. Guo, L.; Kors, J. Design of a laboratory scale solar microgrid cyber-physical system for education. *Electronics* **2021**, *10*, 1562. [CrossRef]

112. Marwedel, P.; Engel, M. Flipped classroom teaching for a cyber-physical system course-an adequate presence-based learning approach in the internet age. In Proceedings of the 10th European Workshop on Microelectronics Education (EWME), Tallinn, Estonia, 14–16 May 2014.
113. Taha, W.; Hedstrom, L.; Xu, F.; Duracz, A.; Bartha, F.Y.; David, J.; Gunjan, G. Flipping a first course on cyber-physical systems: An experience report. In *Proceedings of the 2016 Workshop on Embedded and Cyber-Physical Systems Education*; Association for Computing Machinery: New York, NY, USA, 2016.
114. Veljovic, A.; Matijevic, M.; Nedeljkovic, M.; Cantrak, D. An approach to design of the cyber-physical systems for engineering-education. In Proceedings of the 2018 IEEE Global Engineering Education Conference (EDUCON), Santa Cruz de Tenerife, Spain, 17–20 April 2018.
115. Leitão, P.; Colombo, A.; Karnouskos, S. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Comput. Ind.* **2016**, *81*, 11–25. [CrossRef]
116. Thramboulidis, K. A cyber–physical system-based approach for industrial automation systems. *Comput. Ind.* **2015**, *72*, 92–102. [CrossRef]
117. Kagermann, H.; Wahlster, W.; Helbig, J. Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0. *Final. Rep. Ind.* **2013**, *4*, 82.
118. Governement, G. *The New High-Tech Strategy-Innovations for Germany*; The Federal Government, Germany, 2014.
119. Drozdov, D.; Dubinin, V.; Patil, S.; Vyatkin, V. A Formal Model of IEC 61499-Based Industrial Automation Architecture Supporting Time-Aware Computations. *IEEE Open J. Ind. Electron. Soc.* **2021**, *2*, 169–183. [CrossRef]
120. Nikolakis, N.; Maratos, V.; Makris, S. A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace. *Robot. Comput.-Integr. Manuf.* **2019**, *56*, 233–243. [CrossRef]
121. Zawra, L.; Mansour, H.; Messiha, N. Migration of Legacy Industrial Automation Systems in the Context of Industry 4.0-A Comparative Study. In Proceedings of the 2019 International Conference on Fourth Industrial Revolution (ICFIR), Manama, Bahrain, 19–21 February 2019.
122. Waschull, S.; Bokhorst, J.A.; Molleman, E.; Wortmann, J.C. Work design in future industrial production: Transforming towards cyber-physical systems. *Comput. Ind. Eng.* **2020**, *139*, 105679. [CrossRef]
123. Hoffmann, M.W.; Malakuti, S.; Gruner, S.; Finster, S.; Gebhardt, J.; Tan, R.; Schindler, T.; Gamer, T. Developing Industrial CPS: A Multi-Disciplinary Challenge. *Sensors* **2021**, *21*, 1991. [CrossRef] [PubMed]
124. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A survey of approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [CrossRef]
125. Ndip-Agbor, E.; Cao, J.; Ehmann, K. Towards smart manufacturing process selection in Cyber-Physical Systems. *Manuf. Lett.* **2018**, *17*, 1–5. [CrossRef]
126. Gunes, V.; Peter, S.; Givargis, T.; Vahid, F. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Trans. Internet Inf. Syst. (TIIS)* **2014**, *8*, 4242–4268.
127. Basile, F.; Chiacchio, P.; Coppola, J.; Gerbasio, D. Automated warehouse systems: A cyber-physical system perspective. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015.
128. Kang, H.S.; Lee, J.Y.; Choi, S.; Kim, H.; Park, J.H.; Son, J.Y.; Kim, B.H.; Noh, S.D. Smart manufacturing: Past research, present findings, and future directions. *Int. J. Precis. Eng. Manuf.-Green Technol.* **2016**, *3*, 111–128. [CrossRef]
129. Wiesner, S.; Marilungo, E.; Thoben, K. Cyber-physical product-service systems–challenges for requirements engineering. *Int. J. Autom. Technol.* **2017**, *11*, 17–28. [CrossRef]
130. Xia, T.; Xi, L. Manufacturing paradigm-oriented PHM methodologies for cyber-physical systems. *J. Intell. Manuf.* **2019**, *30*, 1659–1672. [CrossRef]
131. Wan, J.; Yin, B.; Li, D.; Celesti, A.; Tao, F.; Hua, Q. An ontology-based resource reconfiguration method for manufacturing cyber-physical systems. *IEEE/ASME Trans. Mechatronics* **2018**, *23*, 2537–2546. [CrossRef]
132. Tao, F.; Qi, Q.; Wang, L.; Nee, A. Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering* **2019**, *5*, 653–661. [CrossRef]
133. Monostori, L.; Kadar, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihn, W.; Ueda, K. Cyber-physical systems in manufacturing. *Cirp Ann.* **2016**, *65*, 621–641. [CrossRef]
134. Yao, X.; Zhou, J.; Lin, Y.; Li, Y.; Yu, H.; Liu, Y. Smart manufacturing based on cyber-physical systems and beyond. *J. Intell. Manuf.* **2019**, *30*, 2805–2817. [CrossRef]
135. Qiao, F.; Liu, J.; Ma, Y. Industrial big-data-driven and CPS-based adaptive production scheduling for smart manufacturing. *Int. J. Prod. Res.* **2021**, *59*, 7139–7159. [CrossRef]
136. Han, M.; Duan, Z.; Li, Y. Privacy issues for transportation cyber physical systems. In *Secure and Trustworthy Transportation Cyber-Physical Systems*; Springer: Berlin, Germany, 2017; pp. 67–86.
137. Lin, J.; Yu, W.; Yang, X.; Yang, Q.; Fu, X.; Zhao, W. A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems. *IEEE Trans. Veh. Technol.* **2016**, *66*, 2551–2566. [CrossRef]
138. Zhou, Y.; Mo, Z.; Xiao, Q.; Chen, S.; Yin, Y. Privacy-preserving transportation traffic measurement in intelligent cyber-physical road systems. *IEEE Trans. Veh. Technol.* **2015**, *65*, 3749–3759. [CrossRef]

139. Kantarci, B. Cyber-physical alternate route recommendation system for paramedics in an urban area. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015.
140. Li, Y.; Zhang, L.; Zheng, H.; He, X.; Peeta, S.; Zheng, T.; Li, Y. Nonlane-discipline-based car-following model for electric vehicles in transportation-cyber-physical systems. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 38–47. [CrossRef]
141. Hussain, M.; Beg, M. Using vehicles as fog infrastructures for transportation cyber-physical systems (T-CPS): Fog computing for vehicular networks. *Int. J. Softw. Sci. Comput. Intell. (IJSSCI)* **2019**, *11*, 47–69. [CrossRef]
142. Ko, W.H.; Satchidanandan, B.; Kumar, P. Dynamic watermarking-based defense of transportation cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.* **2019**, *4*, 1–21. [CrossRef]
143. Lu, Y. Cyber physical system (CPS)-based industry 4.0: A survey. *J. Ind. Integr. Manag.* **2017**, *2*, 1750014. [CrossRef]
144. Chattopadhyay, A.; Lam, K. Security of autonomous vehicle as a cyber-physical system. In Proceedings of the 2017 7th International Symposium on Embedded Computing and System Design (ISED), Durgapur, India, 18–20 December 2017.
145. Lv, C.; Hu, X.; Sangiovanni-Vincentelli, A.; Li, Y.; Martinez, C.M.; Cao, D. Driving-style-based codesign optimization of an automated electric vehicle: A cyber-physical system approach. *IEEE Trans. Ind. Electron.* **2018**, *66*, 2965–2975. [CrossRef]
146. Zhao, H.; Sun, D.; Zhao, M.; Cheng, S.; Liu, W. A novel CPS-based vehicle safety state evaluation scheme. In *Proceedings of the Institution of Civil Engineers-Transport*; Thomas Telford Ltd.: London, UK, 2016; Volume 169, pp. 12–23.
147. Zhao, H.; Yue, H.; Gu, T.; Li, W. CPS-based reliability enhancement mechanism for vehicular emergency warning system. *Int. J. Intell. Transp. Syst. Res.* **2019**, *17*, 232–241. [CrossRef]
148. Mikusz, M.; Csiszar, A. CPS Platform Approach to Industrial Robots: State of the Practice, Potentials, Future Research Directions. In *Proceedings of the PACIS*; Pacific Asia Conference on Information Systems: Singapore, 2015. .
149. Michniewicz, J.; Reinhart, G. Cyber-Physical-Robotics–Modelling of modular robot cells for automated planning and execution of assembly tasks. *Mechatronics* **2016**, *34*, 170–180. [CrossRef]
150. Rahman, S.M. Cognitive cyber-physical system (C-CPS) for human-robot collaborative manufacturing. In Proceedings of the 2019 14th Annual Conference System of Systems Engineering (SoSE), Anchorage, AK, USA, 19–22 May 2019; pp. 125–130.
151. Genders, W.; Wang, J.; Razavi, S. Smartphone construction safety awareness system: A cyber-physical system approach. In Proceedings of the 16th International Conference on Computing in Civil and Building Engineering (ICCCBE2016), Osaka, Japan, 6–8 July 2016.
152. Guo, Y.; Hu, X.; Hu, B.; Cheng, J.; Zhou, M.; Kwok, R.Y. Mobile cyber physical systems: Current challenges and future networking applications. *IEEE Access* **2017**, *6*, 12360–12368. [CrossRef]
153. Syed, B.; Pal, A.; Srinivasarengan, K.; Balamuralidhar, P. A smart transport application of cyber-physical systems: Road surface monitoring with mobile devices. In Proceedings of the 2012 Sixth International Conference on Sensing Technology (ICST), Kolkata, India, 18–21 December 2012; pp. 8–12.
154. Raisin, S.N.; Jamaludin, J.; Rahalim, F.M.; Mohamad, F.A.J.; Naeem, B. Cyber-Physical System (CPS) Application-A REVIEW. *REKA ELKOMIKA J. Pengabdi. Kpd. Masy.* **2020**, *1*, 52–65. [CrossRef]
155. Raj, R.; Rai, N. Voice controlled cyber-physical system for smart home. In *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*; Association for Computing Machinery: New York, NY, USA, 2018.
156. Alhafidh, B.; Allen, W. High level design of a home autonomous system based on cyber physical system modeling. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 5–8 June 2017.
157. Ahmad, A.; Paul, A.; Rathore, M.M.; Chang, H. Smart cyber society: Integration of capillary devices with high usability based on Cyber–Physical System. *Future Gener. Comput. Syst.* **2016**, *56*, 493–503. [CrossRef]