Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives

Kunwu Zhang, *Member, IEEE*, Yang Shi, *Fellow, IEEE*, Stamatis Karnouskos, *Fellow, IEEE*,
Thilo Sauter, *Fellow, IEEE*, Huazhen Fang, *Member, IEEE*,
and Armando Walter Colombo, *Fellow, IEEE*

***Abstract*—Cyber-physical systems (CPSs) have attracted increasing attention in recent years due to their promise for substantial and long-term benefits to society, economy, environment, and citizens. In addition, the rapid advances in computing, communication, and storage technologies have resulted in a revolution in the information communication technology domain and domination in the industry context. The utilization of CPSs in industrial settings has led to industrial cyber-physical systems (ICPSs), which, in conjunction with the information-driven interactions, enables large-scale cooperation in industrial facilities and among all the stakeholders of the value chain. Hence, the research on ICPSs is essential, especially with respect to the engineering of such systems for industrial applications. This article presents an overview of recent developments in ICPSs. We first introduce the architecture of ICPSs. Then, we review the developments of ICPSs in relevant research domains. Finally, this article concludes by presenting some potential future research directions on ICPSs.**

***Index Terms*—Communication and networking, control, cyber security, industrial cyber-physical system (ICPS), information acquisition.**

I. Introduction

THE radical advances in the technologies of computing, communication, and storage have given rise to a revolution in several industries that are now heavily dependent on information communication technologies (ICT). The prevalence of ICT in all the aspects of modern life has drastically expanded the presence and power of cyberspace and changed the way of information collection and exploitation. The term *cyber-physical system (CPS)* was coined around 2006 to illustrate this increasingly important area integrating the computation with physical processes [1], [2]. CPSs refer to complex engineered systems that leverage embedded computing, sensing, and network communication to monitor, coordinate, control, and integrate physical devices or processes. By tightly coupling the cyber and physical domains, CPSs represent a promising framework to connect individual systems and different entities into a whole to provide sophisticated functions and meet significant needs for reliability, adaptability, resilience, and scalability. The past few years have witnessed the rapid development of CPSs across a broad range of areas, such as intelligent transportation, advanced industries, smart grid, and intelligent agriculture [1], [3], [4], [5]. The growing body of work indicates the substantial benefits of applying CPSs to address various societal imperatives while demonstrating their increasing impacts on industrial production.

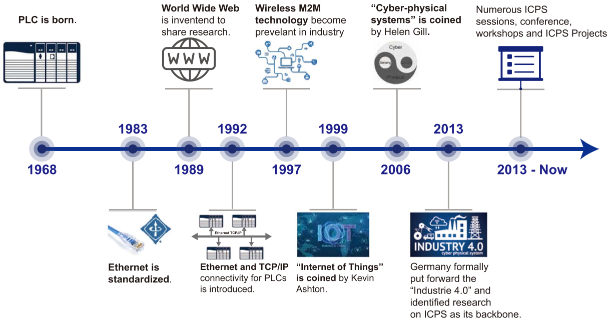

PLC is born.
World Wide Web is invented to share research.
Wireless M2M technology become prevelant in industry
"Cyber-physical systems" is coined by Helen Gill.
Cyber
Numerous ICPS sessions, conference, workshops and ICPS Projects
1968
1983
1989
1992
1997
1999
2006
2013
2013 - Now
Ethernet is standardized.
Ethernet TCP/IP
Ethernet and TCP/IP connectivity for PLCs is introduced.
IOT
"Internet of Things" is coined by Kevin Ashton.
INDUSTRY 4.0
cyber physical system
Germany formally put forward the "Industrie 4.0" and identified research on ICPS as its backbone.

Fig. 1. ICPS timeline [6].

With the increasing penetration of the ICT in industry, the use of computers and networks in physical devices is ubiquitous in manufacturing domains, enabling the transformation of the traditional industrial settings into an industrial environment on the basis of CPSs. This led to the development of industrial cyber-physical systems (ICPSs). Fig. 1 shows the timeline for the development of the ICPS. By digitizing the data and information in the product life cycle, the industrial infrastructures in ICPSs can have a cyber representation (digital twin). This digitalization enables the migration from current industrial infrastructures to digital, networked, adaptive, intelligent, and reliable infrastructures, thereby improving the competitive

Manuscript received 11 January 2022; revised 23 April 2022 and 21 July 2022; accepted 10 August 2022. Date of publication 17 August 2022; date of current version 8 November 2022. This work was supported by the Natural Sciences and Engineering Research Council of Canada. Paper no. TII-22-0169. *(Corresponding author: Yang Shi.)*

Kunwu Zhang and Yang Shi are with the Department of Mechanical Engineering, University of Victoria, Victoria, BC V8W 2Y2, Canada (e-mail: kunwu@uvic.ca; yshi@uvic.ca).

Stamatis Karnouskos is with the SAP, 69190 Walldorf, Germany (e-mail: karnouskos@ieee.org).

Thilo Sauter is with the Institute of Computer Technology, Vienna University of Technology, 1040 Vienna, Austria, and also with the Department for Integrated Sensor Systems, University for Continuing Education Krems, 2700 Wiener Neustadt, Austria (e-mail: sauter@iiss.at).

Huazhen Fang is with the Department of Mechanical Engineering, University of Kansas, Lawrence, KS 66045 USA (e-mail: fang@ku.edu).

Armando Walter Colombo is with the Institute for Industrial Informatics, Automation and Robotics, University of Applied Sciences Emden/Leer, 26723 Emden, Germany (e-mail: awcolombo@ieee.org).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3199481.

Digital Object Identifier 10.1109/TII.2022.3199481

performance of industrial sectors. The visions for the next generation of industrial applications and services (referred to as *Industry 4.0*) are, therefore, strongly linked to the developments in ICPSs [2].

Although the ICPS has some common features with current popular ICT-based systems, such as networked control systems (NCSs), the Internet of Things (IoT), and the Industrial Internet, there are several fundamental differences between ICPSs and these ICT systems. The ICPS is not only the networked and embedded control system but also the intelligent and software-intensive system capable of collaboration, adoption, and evolution [2]. As introduced in [7], the IoT interconnects the physical devices via wireless and Internet technology to achieve reliable information transmission and intelligent data processing. The Industrial Internet, also known as the Industrial IoT (IIoT), refers to the integration of intelligent machines, advanced analytics, the IoT, and the current industrial ecosystem. From the network perspective, the IoT and Industrial Internet enable the implementation of ICPSs. Even though the terms (ICPS, IoT, and Industrial Internet) are sometimes interchangeable on their technological basis, there are subtle differences: The IoT and Industrial Internet can be regarded as the extension of the Internet, concentrating on the openness and networks; ICPSs originate from engineering fields and focus on the applicability and modeling of physical systems, usually in a closed-loop manner. This difference may be hairsplitting but leads to significant differences in the design, modeling, and control of industrial systems [2], [7], [8], [9].

Although the ICPS is a specific CPS class of CPSs focusing on industrial applications, it has some distinctive features. First, according to Internet-based services, ICPSs allow information-driven interactions and open collaboration among multiple stakeholders, such as factories, business partners, and customers, from local or different geographical regions [9], [10], [11], [12]. In addition, the human factors, such as the human-to-machine and human-to-business interactions, are also fully considered in ICPSs. As an integral part of ICPSs, the workforce can interact with the ICPS ecosystem and offer its services to other machines in ICPSs, or even to other CPSs. Furthermore, there exist intelligent mechatronic systems and legacy systems in ICPSs at the same time. ICPSs are required to operate, coexist, and integrate legacy systems, leading to complicated migration processes from traditional infrastructures to new ICPS infrastructures.

The implementation of ICPSs brings new challenges. Several surveys have been published with comprehensive literature reviews and in-depth discussions on key technologies enabling the implementation of ICPS from different perspectives. For example, Serror et al. [13] focus on the IIoT security issue, discussing the applicability and security benefits of recent approaches. The paper [14] reviews research efforts on edge- or edge–cloud-computing-based strategies that optimize the quality of service (QoS) of CPS applications from the perspectives of service latency, energy consumption, security, privacy, and reliability. Mao et al. [15] summarize recent results on communication and computation mechanisms in the IIoT from the perspective of energy efficiency. Ahmad et al. [16] focus on the design of artificial intelligence (AI)-assisted concepts, tools, and algorithms in wireless networks for communication in the IoT. A generalized conceptual framework of the AI-based communication network infrastructure is also proposed in this paper. The work [17] reviews the research efforts on cloud–edge-computing-based ICPS assisted with AI techniques. A data-driven reasoning module is also proposed in this work to improve the intelligence and autonomy of the monitoring and control at the shop floor level.

This article aims to review and highlight the recent advances in the field of ICPSs that span a broad spectrum of application domains. Different from the survey papers [13], [14], [15], [16], [17], the focus of this article will be set on the key aspects in selected directions that are relevant to the operational usage of ICPSs in industry in the years to come. More specifically, we identify the critical challenges of implementing the ICPS from the perspectives of information acquisition, data analysis, communication, and control. Then, we review related research works in these selected directions to demonstrate the state-of-the-art approaches that address the identified challenges. Furthermore, this article provides readers with the current status of ICPS applications in smart manufacturing, smart agriculture, and smart city. Finally, we raise some challenging issues for future research.

The rest of this article is organized as follows. Section II introduces the system components and the reference architecture of ICPSs. Section III discusses the critical challenges of implementing ICPSs in selected directions, and Section IV reviews the recent advances in ICPSs addressing these challenges. Section V presents the applications of ICPSs in different fields. Finally, Section VI concludes this article by presenting some perspectives and an outlook on future research opportunities.

II. Architecture and Modeling of the ICPS

The profound coordination between the physical and cyber domains of the ICPS makes the involved entities interact in significantly complicated ways, thus presenting many challenges for the ICPS modeling and verification [8], [9]. Significant research efforts have been made to explore the architecture of ICPSs.

A. System Components

Even though the definition of ICPSs has been widely accepted in industrial communities, there is no unanimous agreement on the essential components of ICPSs. The architecture of ICPSs is expected to accommodate the increasing complexity and emergent features of ICPS infrastructures. To meet these requirements, the use of the *service-oriented architecture (SOA)* and *multiagent systems (MAS)* in industrial automation environments is a promising solution, where the entities interact and collaborate based on the cloud computing and web service technologies. By configuring appropriate embedded units and using cloud-intrinsic capabilities, ICPSs can benefit from the needed agility and flexibility imposed by business needs in real time, without the need for reprogramming large monolithic systems [2], [8], [11], [18]. In the SOA paradigm, the discrete components of software functionalities can be decomposed as services such that different applications can use the common

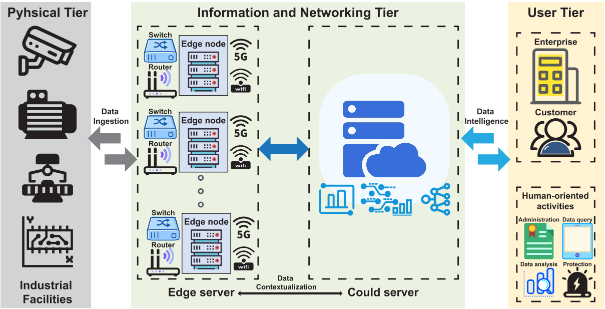


Fig. 2. Service-oriented interaction among ICPS tiers.

parts and enhance the reusability as well as the robustness of the infrastructure. Various auxiliary services can be hosted in the cloud, leading to the "service cloud," which simplifies the integration of complex monitoring and control systems and also simplifies the migration from current- to next-generation industrial systems [8], [12], [19]. The use of MAS can establish the distributed intelligence in ICPSs and promote system flexibility, adaptability, and reconfigurability. Such distributed systems can be designed based on the holonic principles, where the complex system can be considered as hierarchical systems with intermediate stable forms [20]. Integrating SOA principles to the network of distributed industrial agents can eliminate some limitations of MAS, for example, the limited interoperability among agents. Therefore, the SOA and MAS are considered as the critical enablers for the implementation of ICPSs [2], [8], [12], [21]. From the application point of view, the components of ICPSs featuring the SOA- and MAS-based collaborative automation can be briefly categorized into three main tiers.

1) The *physical tier* consists of numerous industrial facilities, including industrial machines, sensors, embedded systems, and other intelligent devices. This tier typically enables real-time data collection and processing and provides control capabilities to execute commands for physical processes.
2) The *communication and networking tier*, composed of the edge/cloud servers and communication and sensor networks, acts as an intermediary to facilitate information transmission, storage, and processing. It can also integrate high-level functions, such as manufacturing execution systems and enterprise resource planning.
3) The *user tier* empowers human-oriented activities, such as data query, decision making, and safety protection. It also includes cautions to limit human errors and prevent malicious actions.

A graphical view of these abstract tiers is shown in Fig. 2 [22].

B. Reference Architectures

For the implementation of ICPSs, the deployment of SOA, MAS, and cloud computing in the industrial automation environment plays an essential role [21]. Today's industrial infrastructures are typically structured into the five-level hierarchical enterprise reference architecture defined by the International Society of Automation (ISA)-95 paradigm [23] in Fig. 3, although many different models have been devised over time [24]. The information-driven interactions and collaboration among legacy systems and stakeholders of the value chain render the automation systems increasingly complex. Therefore, structured methods and standardization efforts are desired to simplify the interoperable interactions among different stakeholders and organizations. To align standards related to Industry 4.0, several organizations have developed reference ICPS architectures that still show the ISA-95 legacy [9].

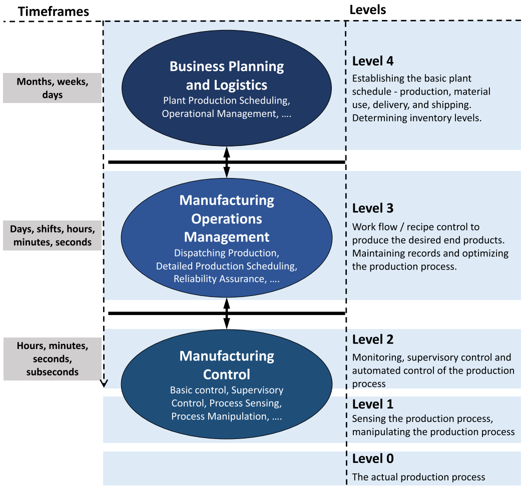

Timeframes
Levels
Months, weeks, days
Business Planning and Logistics
Plant Production Scheduling, Operational Management, ...
Level 4
Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.
Days, shifts, hours, minutes, seconds
Manufacturing Operations Management
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
Level 3
Work flow / recipe control to produce the desired end products. Maintaining records and optimizing the production process.
Hours, minutes, seconds, subseconds
Manufacturing Control
Basic control, Supervisory Control, Process Sensing, Process Manipulation, ...
Level 2
Monitoring, supervisory control and automated control of the production process
Level 1
Sensing the production process, manipulating the production process
Level 0
The actual production process

Fig. 3. Functional hierarchy of the ISA-95 standard [23].

1) Reference Architecture Model for Industry 4.0 (RAMI 4.0):

The German Electrical and Electronic Manufacturers' Association has developed *Reference Architecture Model for Industry 4.0 (RAMI 4.0)* to support Industry 4.0 initiatives [25], aiming to describe the fundamental aspects of Industry 4.0 with sufficient precision. As shown in Fig. 4, RAMI 4.0 is a 3-D layered hierarchical model showing connections between product life cycles, industrial infrastructures, stakeholders of the value chain, and information technology. These three dimensions include the following:

1) The "*Layers*" axis represents the characteristics of information technology components in Industry 4.0. This axis includes six layers, and each layer indicates a category of manageable parts of the system.
2) The "*Life Cycle Value Stream*" axis describes the life cycle of products based on the International Electrotechnical Commission (IEC) 62890 standard, describing the differentiation between the types and instants of the products.
3) The "*Hierarchy Levels*" axis indicates different functionalities within industrial sectors based on levels defined in IEC 62264 and IEC 61512 standards. By adding two labels, "Product" and "Connected World," this axis expands the functionalities defined by the layers of the ISA-95 automation pyramid to represent the Industry 4.0 environment.

Therefore, complex interrelationships among ICPS components can be decomposed into small and manageable sections within this 3-D space. By mapping existing standards and models to this space, RAMI 4.0 can provide a guideline to develop ICPS satisfying the sector requirements and various standards.

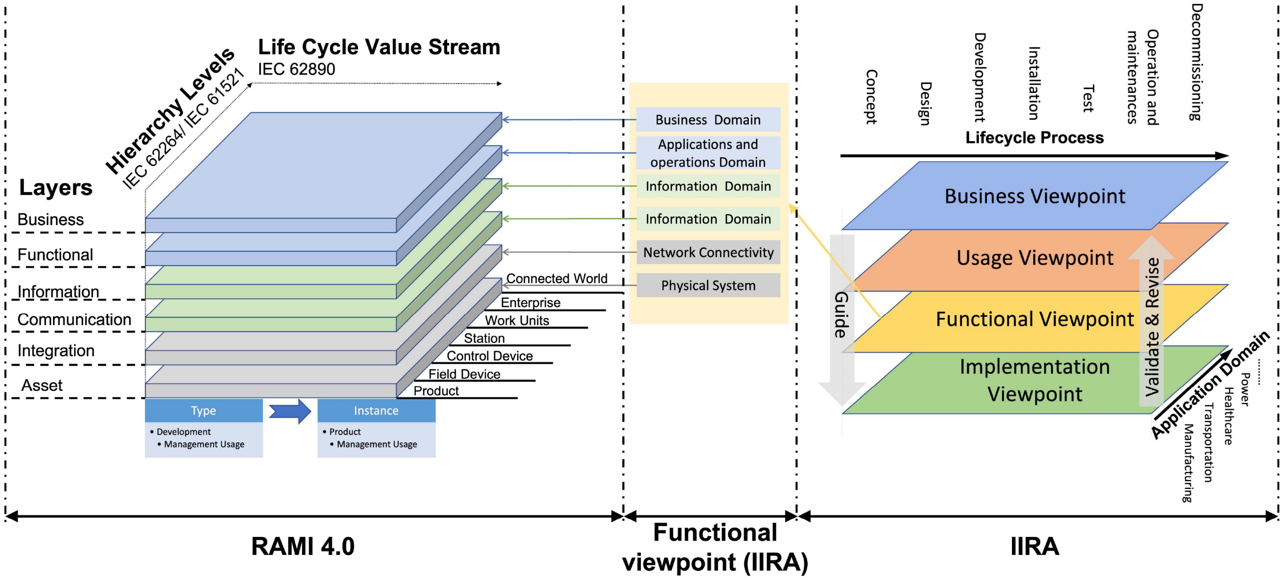


Fig. 4. Relations between RAMI 4.0 layers and IIRA functional viewpoint [29].

The main insight of RAMI 4.0 [25] is to ensure the Industry 4.0 compliance of components via the specifications of the *Asset Administration Shell* (AAS) [26], [27]. By deploying the AAS and standardizing its parts (submodels), the functionality of the asset can be represented to comply with Industry 4.0 such that the system components can interact via the interoperable SOA-based interfaces [28].

2) Industrial Internet Reference Architecture (IIRA): The Industrial Internet Reference Architecture (IIRA), developed by the Industry IoT Consortium, is standard-oriented and provides a common architecture framework for developing interoperable ICPSs [30]. This architecture is developed based on architecture description defined by the International Organization for Standardization/IEC/IEEE 42010 standard. As shown in Fig. 4, there are four viewpoints in the IIRA. Each viewpoint involves a specific class of system concerns [30].

1) The *business viewpoint* includes the business-oriented concerns of identifying the stakeholders in ICPSs and the corresponding business visions, values, and objectives.
2) The *usage viewpoint* focuses on the concerns of expected system usage related to human factors. It usually represents the human-oriented activities in ICPSs, such as data queries and safety protection.
3) The *functional viewpoint* focuses on the functionalities of ICPSs and the system structure. It also attends to the interrelations and interactions among the system components and the relations and interactions with the environment.
4) The *implementation viewpoint* addresses the technologies needed for the implementation of ICPSs, the communication networks, and the life cycle procedures.

These four viewpoints forge the foundations of the IIRA, realizing the viewpoint-by-viewpoint analysis of ICPS concerns. This architecture can be further extended by adding additional viewpoints based on the specific system requirements [9].

As mentioned in [9], [29], and [31], the RAMI 4.0 and the IIRA share some conceptual similarities in modeling the distributed and heterogeneous industrial agents. For example, Fig. 4 shows the mapping between the information technology layers in the RAMI 4.0 and the functional viewpoint in the IIRA when addressing industrial interoperability. More details regarding the comparison between the RAMI 4.0 and the IIRA can be found in [29] and [31]. The introduction of other reference architectures, e.g., IBM Industry 4.0 architecture and NIST service-oriented smart manufacturing architecture, can be found in recent survey papers [32], [33].

III. ICPS Research Challenges

Challenges arising from implementing ICPSs have motivated large numbers of studies to assess and tackle the challenges, e.g., [2], [8], [9], [21], [34], [35]. In this section, we discuss these challenges in selected directions.

A. Challenges in Information Acquisition and Data Analytics

Typical information acquisition in ICPSs involves not only the collection of data from sensors but also data processing, which is realized based on various wired and wireless sensor and actuator networks. Sensors in these networks, especially in wireless sensor networks (WSNs) and wireless sensor–actuator networks, are attached to node systems to feature computing and collaboration capabilities [36], playing a pivotal role in supporting intelligent and autonomous decision making. However, the nodes in sensor and actuator networks usually have limited power and memory, and the communication networks in ICPSs have limited bandwidth. As a result, the network topology and information sensing strategy design should provide a tradeoff between energy efficiency, data reliability, and communication load.

The data analytics in ICPSs is also challenging due to the massive data generated from industrial infrastructures, enterprises, and humans with a wide variety of degrees, scales, densities, and modalities [2]. These data need to be processed online before being used for intelligent control. Owing to the modular system architecture, the issue of data interoperability and integration becomes increasingly crucial [31]. Furthermore, the hierarchical structure of the entire sensor network also brings a significant concern that the private or confidential information belonging to legitimate entities may be exposed to unauthorized entities [37]. Therefore, information privacy and security have become the primarily concerned issues.

B. Challenges in Communication Networks

Compared with the traditional industrial settings, the heterogeneity and hierarchical architecture of ICPSs gives rise to unique challenges in communication network design. The first challenge is how to satisfy the stringent latency requirements in the monitoring and control of ICPSs. As emphasized in [2], the capabilities of real-time monitoring, control, and management are one of the key enablers for the acceptance of CPSs in industrial facilities. Almost all the activities in ICPSs highly rely on data transmission among entities. If the data cannot reach their destination on time, they may become useless and work against effective subnetwork operation. The wide deployment of wireless technologies and the multihop communication over mesh networks inevitably induce the issue of communication delays. Advances in 5G and upcoming 6G communications also address such issues and are increasingly used in coupling edge- and cloud-based systems [34].

Reliability is another key factor of communication in ICPSs. Owing to the potentially harsh industrial environments, the conditions of the communication channels in ICPSs may change dynamically, which can lead to reliability issues, such as time-varying delays, packet dropouts, time jitter, and data rate limitation. The tight integration of cyber components and physical devices can further worsen the impacts of the transmission failure caused by packet dropouts, interfaces, and outages [4]. Furthermore, the issues of stability, efficiency, schedulability, and security also should be addressed in designing the communication strategy to guarantee the QoS for machine-to-machine (M2M) communications and cross-domain collaboration [38], [39].

C. Challenges in Advanced Control

In traditional industrial settings, most real-time monitoring and control solutions are model-based, in which system performance closely depends on the accuracy of the mathematical models of the processes and devices to be controlled. However, applying these model-based approaches to ICPSs is difficult since it is challenging to establish a precise mechanism model based on the physical laws. The human factors in the ICPS also render the modeling process more complicated [40]. In addition, there exist continuous-time dynamics and discrete-time events in ICPSs at the same time. The information is collected from the physical devices, which commonly operate in the continuous-time domain, transmitted to the information layer in a discrete-time manner, and finally processed and sent back to physical devices [41]. Owing to the need for bridging the gaps between the inherently discrete semantic and intrinsically concurrent physical world, the modeling and analysis of dynamic behaviors of ICPSs are challenging. In addition, the ICPS is a complex set of numerous heterogeneous and seamlessly connected systems with various power resources. Combining these systems results in a large-scale complex distributed system capable of performing complicated tasks that cannot be done by individual systems. Each subsystem should have operational and managerial independence and behave consistently, which renders the control system design much more complicated.

IV. ICPS Research Directions

In this section, we summarize some recent advances of ICPSs in selected directions, which address the research challenges mentioned in Section III.

A. Information Acquisition and Data Analytics

The performance of ICPSs highly depends on their capability to collect and analyze data and information from different sources and utilize them in their interactions with other systems and services. As aforementioned, one main challenge of information acquisition and data processing in ICPSs is how to achieve the tradeoff between energy efficiency, data reliability, and communication load under the consideration of privacy, security, and interoperability. In the following, we discuss the potential solutions to this issue from several perspectives.

1) Information Sensing and Data Processing: In ICPSs, the data are collected from heterogeneous sources with various power resources. Selecting a high sampling rate in ICPSs has potential utility in performance improvement, but it unavoidably leads to heavy communication load and possibly communication delays. Therefore, it is desired to select a proper sampling rate to balance the control performance and communication load [36]. A multiobjective optimization problem is formulated in [42] to maximize the sampling interval and minimize the energy consumption. Saifullah et al. [43] employ the schedulability analysis technology to optimize the sampling rate based on the communication deadlines. By applying the compressive sampling theory, Luo et al. [44] develop a compressive data gathering scheme for large-scale WSNs without introducing intensive computation or complicated transmission control. In [45], an adaptive trajectory compression algorithm called *SimpleTrack* is proposed based on compressive sensing. It is proved that the proposed SimpleTrack algorithm can improve computational efficiency with slightly affected performance.

Owing to massive data generated from industrial infrastructures, enterprises, and humans with a wide variety of degrees, scales, densities, and modalities, the traditional data fusion methods may not be applied to ICPSs [2]. In addition, the information collected from entities may be private or confidential. The issues of privacy and security need to be addressed when fusing data. Furthermore, in order to ensure accurate analysis after the data fusion, a certain degree of data availability is required.

Therefore, the tradeoff between data privacy and data availability should be considered when designing data fusion algorithms. To address these issues, Luo et al. [46] develop a secure data sensing and fusion scheme for CPSs based on the integration of the grey model, kernel recursive least squares, and Blowfish encryption algorithm. Qi et al. [47] present a privacy-aware data fusion and prediction algorithm for the cyber-physical social systems. It is shown that the proposed data fusion schemes can improve prediction performance. The overview of recent developments on data fusion for cyber-physical social systems can be found in [48].

2) Privacy and Security: In ICPSs, the wide deployment of sensing, processing, and communication devices in industrial environments has promoted corporate connectivity and interoperability between physical devices and cyber parts. However, this inevitably exposes the industrial infrastructures, which may be isolated in traditional industrial settings, to the outside world. Compared with the industrial infrastructures in traditional industrial environments, these infrastructures are more susceptible to cybersecurity vulnerabilities in ICPSs. Therefore, the privacy and security of information have become the primarily concerned issues at all the layers, including the resulting applications that are based on such data.

One immediate solution to this problem is data encryption, where the data are encrypted before the transmission stage and then decrypted to compute the control inputs. For example, a high-quality data collection scheme called *TrustData* is proposed in [49], where a data encryption technique is employed to maintain the security of collected data. Based on lightweight streaming authenticated data structures, Xu et al. [50] present a privacy-preserving data integrity verification model for healthcare CPSs to ensure secure data transmission. The survey paper [51] discusses the privacy-preserving problem in CPSs from a control perspective. But enabling the data encryption in ICPSs gives rise to quantization errors, which may degrade the control performance. Therefore, how to deal with these quantization errors needs to be further investigated in the control system design.

Designing industrial communication networks with secure architectures and network protocols is also a promising solution to guarantee the privacy and security of information. Because of heterogeneity, it is impossible to obtain the same security level for all the components in ICPSs. Alternatively, a practical solution is to meet the security requirements for individual groups of assets by categorizing the ICPS components into separate zones based on their properties, functionalities, and requirements [52]. Each zone connects to the public networks and can be further divided into subzones. But the security architecture and network protocols of the communication network for the zone can be designed independently based on the specific requirements. These zones are also referred to as security zones [53]. This is an extension of the classical and proven defense-in-depth approach [52]. However, especially with the growing popularity of WSNs and mobile networks leading to less hierarchically structured communication architectures, this approach becomes increasingly difficult to apply [39]. Utilizing the concept of the security zone can help designers modularize the ICPS communication networks, thereby simplifying the security policy design.

Using secure communication technologies alone cannot meet the security requirements of ICPSs due to the wide range of cyberattacks. Security protection for industrial infrastructures is also desired to enhance the resiliency of the system. This demand can be satisfied by designing the attack–defense mechanism based on the attack detector in the decision-making unit. When detecting cyberattacks, the decision-making unit in the system can determine how to respond to these attacks, e.g., dropping unsafe data and switching to the resilient safety control unit [37]. Another solution to this problem is using resilient control frameworks to enhance the system's capabilities of absorbing, recovering, and adapting to adverse impacts caused by cyberattacks [54]. The survey paper [37] summarizes the recent developments on attack detection and resilient control for ICPSs.

The aforementioned strategies focus on security protection from the perspective of data transmission and processing. From the machine perspective, in traditional industrial settings, the safety risk assessment process is employed in industrial infrastructures to identify hazards and decide appropriate countermeasures to minimize the impact of hazards on the machine. As mentioned before, a modular system structure is desired for ICPSs to promote system flexibility, adaptability, and reconfigurability. However, the modularity of the ICPS changes the scope of the safety risk assessments for each machine, leading to new security issues in ICPSs. Therefore, a new industrial safety risk assessment approach addressing the ICPS adaptability and reconfigurability is desired. Different surveys summarize various threat assessment tools for the attack analysis [55], while others review the recent advances in the unified safety and security risk assessment framework for modular systems in industrial automation [56] and conclude that the joint approach for handling the issues of security and safety in the same steps can enhance cost-effectiveness. To address the safety and security issues in a unified framework, Hollerer et al. [57] present a new threat modeling approach considering various metrics, including common vulnerability scoring system, security level, and safety integrity level, for operational technology systems. Hosseini et al. [58] develop a safety and security AAS model based on RAMI 4.0 to address the Industry 4.0 safety and security issues.

3) Data Interoperability: As aforementioned, one main feature of the ICPS is the modular structured industrial environment. In order to optimize the industrial and business processes and enhance business values for enterprises, the modules need to consume not only the internal data from components among the ICPS but also the external data from other exogenous systems, such as the market trends, economic factors, current, and future demands. Therefore, integrating data from various sources plays an important role in implementing the ICPS, which, however, is complicated due to the wide variety and heterogeneity [59]. In addition, the data generated by each module are expected to be published and subscribed by other modules participating in the networked value chain based on the concept of the IoT. Therefore, all the modules should be widely interoperable throughout all the devices and components in the networked value chain, from the factory floor to the business and enterprise systems. A semantic description of data is desired for data producers and consumers in the ICPS [60].

In order to handle the increasing data heterogeneity problem, semantic interoperability, which aims at improving the information transmission efficiency in collaborative and heterogeneous environments, is a promising solution [61]. But this solution requires that the semantic definitions of the components provided by the common ontologies and information models are available for all the data providers and consumers in the networked value chain. A solution to this problem is to use the middleware standards, where the semantic information model in the middleware transforms the raw data into well-defined information with various semantics. In [62], by integrating the principles of Devices Profile for Web Services for Process Control Unified Architecture (OPC UA) into IEC 61850 applications, a novel middleware is developed to support semantic definitions for distributed energy resources in smart grid. The resulting framework is service-oriented and semantic enabled and can support the dynamic management of Smart Grid assets. In [60], an interoperability layer is developed for the CPSs with the SOA-based cross-layer structure. The interoperability layer acts as an intermediary between the physical and cyber layers, aiming at mapping the component information and data from the physical layer into a common information model readable for the cyber layer.

Beyond these examples, there is a coordinated effort in several fora to aim toward interoperability, for instance within Industry 4.0 and its architecture RAMI 4.0 [25] as well as in Industry IoT Consortium and their reference architecture [30]. Especially, RAMI 4.0 has evidenced the last years active specification development of the AAS [26], [27] and interoperability (including semantic interoperability) is pursued via it [28] and the standardization of its submodels in organizations, such as the Industrial Digital Twin.[1]

B. Communication Networks

The data and information exchange between the entities in ICPSs are realized via the communication networks. Therefore, communication networks play an important role in bridging the physical worlds and cyberspaces. In order to guarantee the QoS for M2M communications and cross-domain collaboration, there are several concerns, such as the real-time capability, reliability, stability, efficiency, schedulability, and security, which should be primarily considered in designing the communication strategy [34], [38], [39]. There are several promising results reported in the literature to address the aforementioned concerns. Some of them are reviewed and analyzed in the following:

1) Real-Time Capability: As emphasized in [2], the capabilities of real-time monitoring, control, and management are key enablers for the acceptance of CPSs in industrial facilities. Almost all the activities in ICPSs highly rely on data transmission among entities. If the data cannot reach their destination on time, they may become unless and harm the communication subnetworks. In addition, the heterogeneity and hierarchical architecture of ICPSs give rise to various issues in the communication network design, such as time-varying delays, packet dropouts, time jitter, and data rate limitation. Some results have been reported in the literature to address these issues. The survey paper [63] summarizes and compares three systematic methods for handling time delays and further shows that the Markov decision process approach method can perform better than the other two methods. In [64], a smart collaborative balancing strategy is developed for dynamically adjusting the orchestration of network functions and efficiently optimizing the workflow patterns.

Instead of enhancing real-time capability by optimizing workflow patterns, another immediate solution is to improve the computing efficiency of the entire system based on the cloud-based computing paradigms, such as edge computing, fog computing, and edge–cloud computing. An overview of recent advances in end–edge–cloud orchestrated network computing can be found in [65]. Unlike centralized cloud computing, edge computing and fog computing are distributed methods that aim to extend the services and functionalities offered by the cloud at the edges and fog nodes of the network. The term edge–cloud computing indicates the combination of edge computing and cloud computing. Compared with centralized cloud computing, these distributed computing paradigms have lower service latency while requiring significantly less bandwidth [14]. Therefore, it is promising to integrate ICPSs with edge computing, fog computing, or edge–cloud computing. In addition, since there are numerous heterogeneous systems with various computing power in ICPSs, how to effectively deploy cloud-based computing in ICPSs is challenging. The concerns of connectivity, latency, bandwidth, security, and privacy should be adequately addressed. Villalonga et al. [17] provide a solution to this problem based on data-driven techniques. They develop a cloud-to-edge-based ICPS architecture with reasoning modules, where the prediction model and data processing strategies in edge modules are updated by using these modules. A survey paper [14] overviews the recent results on the edge-computing- and edge–cloud-computing-based CPSs.

Recently, microservice architectures have attracted increasing interest in the manufacturing industry. Compared with the SOA, the microservice architecture decomposes the system's main functionalities into loosely coupled and independently deployable services to simplify the implementation [66]. Therefore, the microservice architecture is a promising alternative to implementing the service-enabled and distributed ICPSs. The edge–cloud computing techniques enable the execution of these deployable services or modules in the edge or the cloud to optimize resource allocation and accommodate the power constraint. Therefore, the real-time capability and scalability of the ICPS can be improved with the aid of microservice architecture and edge–cloud computing techniques. In addition, due to the increasing interest that microservices gained in industry, serverless computing is emerging as a new and compelling technique for deploying cloud computing applications [67]. Serverless computing is a programming model and architecture used for creating cloud computing applications. The cloud provider provides this programming model and takes charge of all the operational concerns, while the developer can use it

[1] [Online]. Available: https://industrialdigitaltwin.org/en/

as a platform for fast deployment. As a result, this paradigm can not only reduce the operational cost for the cloud provider by optimizing the cloud resource management developer but also reduce the deploying cost for the developer by avoiding the resource allocation process. By extending this serverless computing paradigm to IoT applications, a deviceless diagram is presented in [68], where the IoT infrastructures can be used by the developers in a serverless-like manner.

2) Reliability: In ICPSs, there are numerous embedded systems with integrated computing functionalities. Their computing performance closely relies on real-time and reliable data. Therefore, reliability is another key factor of communication in ICPSs. Reliable communication can ensure the success of data delivery to the destination without corruption. The tight integration of cyber components and physical devices makes the impacts of the transmission failure caused by packet dropouts, interfaces, and outages more serious. There are some methods reported in the literature for improving communication reliability in ICPSs. For example, by formulating a multiobjective optimization problem, Cao et al. [69] develop a communication and control codesign framework for CPSs, where the packet dropouts, communication delays, and energy capacities are considered as the constraints to the optimization problem. Peng et al. [70] investigate the power allocation problem for wireless CPSs, in which the packet dropout probabilities depend on the sensor transmission power. An optimal power allocation scheme is then derived by formulating the power allocation problem as the Markov decision processes. Since the ICPS can be abstractly considered as an NCS, some methods used for improving the communication reliability in NCSs can be potentially extended to ICPS. We refer the interested readers to a survey paper [71] for an overview of methods for handling transmission failure in NCSs.

C. Advanced Control for ICPS

The ICPS combines numerous multidisciplinary and heterogeneous systems and components from various vendors and platforms. The overall control and automation functionalities of the resultant combined system are greater than the sum of functionalities of its subsystems [40]. To improve ICPS capabilities, each constituent system should have operational and managerial independence and perform efficiently and collaboratively. However, reliable and real-time information acquisition and communication are not enough for building such systems; control plays an essential role in achieving cooperation among constituent systems as well as the self-autonomous operation of each constituent system. Depending on the applications and domains, there are many problems associated with the control, especially the closed-loop control, of ICPSs. We present some issues that need to be primarily considered in the following.

1) Control System Requirements: In order to meet performance requirements, the following concerns should be considered when designing the control algorithms.

a) Stability and reliability: The ICPS is the integration of industrial facilities and CPSs that requires high process stability and reliability. Ensuring process stability and reliability is the primary objective of most ICPS applications.

b) Robustness: Owing to a large number of entities and in-depth coordination between the physical and cyber domains, perturbations, including process noises, transmission errors, and model mismatch, are inevitable in ICPS applications. In order to make control performance robust to perturbations from cyber parts, physical devices, and the interaction between physical and cyber worlds, how to enhance the control system robustness should be considered.

c) Power capacities: In ICPSs, there are numerous embedded systems with limited computing power. The communication networks are also subject to limited bandwidth. Therefore, the power constraints of embedded systems and the limitation of the network's bandwidth should be considered in control system designs.

d) Codesign: As aforementioned, in ICPSs, there exist continuous-time dynamics and discrete events at the same time. In addition, the information-driven interaction in ICPS connects industrial infrastructures with other CPSs and enterprise systems along the supply chain [8]. The collaboration among entities and interaction between physical and cyber worlds need to be designed in a cross-layer fashion.

e) Real-time operation: Similar to the design of communication networks, the real-time capability is also the prime concerning issue in the ICPS control system design, which is mainly determined by the controller's computational complexity. The designed control algorithms should meet the requirements of computational complexity from a wide variety of embedded systems and networks in ICPSs, especially when considering the requirements of robustness, power capacities, and codesign. The tradeoff between the computational complexity and reliability of the control algorithm is desired.

2) Recent Developments: The ICPS control problems have been widely studied in the literature. Some promising results addressing the problems mentioned above are reviewed in the following.

In order to clarify the robustness requirements for CPSs, Tabuada et al. [72] introduce a notion of robustness based on the definition of input–output stability in control theory. This article presents a mathematical definition of robustness for cyber parts that captures the effects of bounded and sporadic disturbances. By modeling the CPS as finite-state transducers, this article also proposes a scheme for verifying the robustness in pseudo-polynomial time. Based on the dissipativity approach, Gao et al. [73] propose the estimator-based time-driven scheme and the self-triggered method for CPSs to deal with external disturbances and attacks on the sensor and actuator channels. Distributed control is a promising solution to meet the requirements of real-time operation and power capacities in ICPSs. Huang and Dong [74] describe the CPS as a networked heterogeneous linear system and then develop a modularized distributed control scheme for the cooperation of subsystems. Spinelli et al. [75] presents a distributed control architecture for implementing industrial cyber-physical manufacturing systems. The survey paper [76] summarizes the recent development of distributed filtering and control for ICPSs.

The aforementioned results on the control system design mainly focus on fulfilling the performance requirements, including stability and robustness. There are many results on the codesign principle to fulfill multiple objectives. Lin et al. [77] develop an energy-aware scheduling strategy for CPSs to minimize the overall energy consumption while ensuring system reliability. In [69], the coordination between the control and communication is investigated by formulating the multiobjective optimization problem. Similarly, Shi et al. [78] proposed a multiobjective-optimization-based energy management strategy for cyber-physical energy systems.

Owing to the seamless integration of physical and cyber components, the system-wide optimization and integrated design strategies have a great potential to improve the system performance. The digital twin has attracted increasing attention from researchers and practitioners for designing integrated monitoring and control systems in ICPSs [79]. A *digital twin* represents a virtual replica of physical entities for simulating their behaviors in the real world based on the data from the physical objects, enabling the factories and enterprises to predict, detect, and eliminate physical errors and intentional malicious attacks and optimize manufacturing processes [80], [81].

With the aid of digital twin techniques, an integrated monitoring and control framework for ICPSs is presented in [40] to achieve a plant-wide performance supervised life cycle management. In this framework, the overall system is divided into four levels, including the plant-wide decision level, subsystem level, control level, and component level. The digital twin techniques are used to describe the key performance indicators and then formulate the multidimensional decision-making problems, thereby achieving the plant-wide optimization [40].

V. ICPS Applications

By enabling the cyber-representation of industrial infrastructures and digitalization of data and information in enterprises, supply chain, and process life cycle, ICPSs will revolutionize industrial sectors at great speeds with significantly improved efficiency. Several research and prototyping efforts have been made by academia, industry, and governments to realize ICPSs in many industrial application domains. In this section, we introduce several categories of industrial applications that gain great potential benefits from ICPSs.

A. Smart Manufacturing

Smart manufacturing receives a high priority in the development of the ICPS industrial ecosystem, in which the machines and products are duly equipped with sensors and embedded systems to communicate with each other cooperatively. Smart manufacturing can collect and harness massive data to help factory managers make better-informed decisions and optimize production processes [82]. To spur the development of smart manufacturing, several industries and government organizations have promoted new programs with significant research investments. In the United States, the Smart Manufacturing Leadership Coalition[2] focuses on developing an adaptive and resource-efficient smart manufacturing platform with a tight integration of customers and partners. The Industry IoT Consortium[3] aims to accelerate the development of Industrial IoT by developing open and interoperable reference architectures and frameworks and industry testbeds. In Europe, the Zero Defect Manufacturing Platform project[4] funded by the H2020 Framework Program of the European Commission focuses on developing an extendable platform for manufacturing processes with a high interoperability level to achieve the goal of zero defects based on the prediction and provision of faults and defects.

The ICPS applications in smart manufacturing have been widely studied in the literature. The integration of process and quality control using multiagent technology project [83] presents a framework to design distributed manufacturing control systems. This framework integrated the process and quality control with self-adaptation and self-optimization mechanisms to improve production efficiency and product quality. The Adaptive Production Management project [84] describes a smart manufacturing architecture capable of dealing with unexpected and drastic changes in production processes. Based on the service-oriented paradigms, this architecture has an integrated framework for agent-based planning and scheduling. The Architecture for Service-Oriented Process, Monitoring and Control project [12] focuses on the service-oriented paradigms for the development and implementation of next-generation industrial supervisory control and data acquisition and distributed control systems. Based on the OPC UA and MTConnect, a Cyber-Physical Machine Tools platform is developed in [85] to improve the efficiency of data transmission between machine tools and software applications, where the data interoperability issue can be addressed by designing an MTConnect to OPC UA interface. Beregi et al. [86] present a Fluid Manufacturing Architecture for cyber-physical production systems. A novel Dew computing layer is established in this architecture based on the cloud, fog, mist, and edge computing paradigms to reduce computational complexity and infrastructural requirements. A framework named Smart Information Platform and Ecosystem for manufacturing is presented in [87] to address the inconsistency of data models in the engineering life cycle of cyber-physical production systems. Instead of using digital twins in the design and deployment phases, this framework employs multiple digital twins consistent with the product life cycle phases to envision a connective structure. As shown by these examples, agent-based and cloud-based technologies and concepts are well-suited for realizing ICPS [8], and this is evident also from some of the open challenges in the specific areas such as those of cyber-physical production systems.

B. Smart Agriculture

The growth of the global population is one of the major challenges to today's society. The world's population is expected

[2] [Online]. Available: http://smlconsortium.org

[3] [Online]. Available: http://www.iiconsortium.org

[4] [Online]. Available: https://www.zdmp.eu/

to reach 9.7 billion in 2050. Accordingly, food production must be improved to feed the growing population, which, however, cannot be achieved by expanding cultivated land due to its limited availability. In addition, extreme weather conditions and rising climate change also threaten food productivity. Therefore, precision farming (PF) or precision agriculture (PA) of the existing cultivated land concerning local characteristics is desired for yield growth and sustainable cultivation.

The increasing application of ICT in agriculture motivates the development of the next generation of industrial agriculture, namely, Agriculture 4.0 [35], where ICPSs play an important role in the evolution. The massive data collected from agriculture sensors enable PF as well as the adaptation to changing needs. The increasing penetration of computing, communication, and control technologies in agriculture provides significant potential benefits for growers and farmers to enhance productivity and reduce waste. More details related to key technologies and challenges for ICPS-based PA can be found in [35].

In literature, some results have been reported to address the development of smart agriculture. The survey paper [88] summarizes recent results on agricultural applications of the IoT and data analytics. The authors conclude that deploying IoT and data analytics in agriculture has great potential to improve the operational efficiency and productivity of plants and livestock. Rad et al. [89] develop a precision agricultural management system for multispectral monitoring of potato crops, whose architecture consists of four layers: the physical layer, the network layer, the decision layer, and the application layer. Ruan et al. [90] present an agricultural CPS framework with four cyclic stages, including data acquisition, scenario reconstruction, and detection, rule training and monitoring, and rule-oriented and scenario-dependent control. In [91], a CPS-based framework, named monitoring, detecting, and responding CPS, is developed for the management of greenhouse stresses, where the collaborative control theory is employed to improve collaboration between sensors, robots, and human in agricultural CPSs. Kang et al. [92] develop a CPS-based agricultural production management strategy for the solar greenhouse. Based on the data collected from markets and greenhouse environments, the cropping plan can be optimized.

C. Smart Cities

As the world continues to urbanize, there is a need for the efficient management of environmental, social, and economic sustainability of resources. The digital transformation of cities is the key to sustainable urbanization, and the smart city has championed the role in global digital-era urbanization. A smart city indicates the integration of ICT with humans, which improves the quality of life, efficiency of urban operations and services, and competitiveness in a ubiquitous manner. Besides the data processing capabilities, these smart city functionalities highly rely on robust real-time and reliable communication features enabling data exchange and information sharing between heterogeneous components with various computing power. Therefore, utilizing ICPSs in the smart city can enable the optimal management of resources, operations, services, and users in a distributed manner.

Many research efforts have been made on the integration of ICPSs in the smart city. In [93], IoT and cloud-computing-powered infrastructure is developed for providing crowd-sourced applications in smart cities. This infrastructure is developed based on an IoT-oriented platform Stack4Things [94] and the cloud platform OpenStack such that new services and applications can be easily added. Chang et al. [95] present an agent-based middleware framework for CPS-based smart cities. By optimally balancing the storage and resource usage, this framework can handle the problems of request failure and response time, thereby improving communication reliability. Jawhar et al. [96] investigate the communication network for a class of smart cities, including the smart grid, water networks, and unmanned aircrafts, where the issues of home power management, aircraft safety operation, and smart power and water systems control are considered when designing communication networks. Specific agent-based smart-grid scenarios have demonstrated effective energy management [97].

The intelligent transportation system (ITS), a complex system of transportation management, monitoring, and evaluation, is becoming an essential part of the smart city. It aims to improve transportation safety and efficiency based on various technologies, from basic management systems, including car navigation and traffic signal control systems, to new and emerging technologies, such as AI and IoT. The automotive IoT is a key enabler of the ITS, which also collects and generates massive data used for making decisions in smart cities. The ICPS provides a promising solution to design such ITSs and further integrate with the smart city. For example, Xu et al. [98] present a three-layer architecture, including the physical layer, the communication layer, and the service layer; for smart transportation systems in [99], a CPS-based architecture for smart transportation security systems is developed. Instead of considering the cybersecurity issue only, this article aims at addressing the comprehensive smart transportation security issue from both the perspectives of CPS and geospatial and public infrastructural configurations.

VI. Conclusion

The ICPS framework holds vast potential to drive the development of next-generation industrial systems. In this article, we presented an overview of recent and emerging research studies in this budding field. The overview covers three key dimensions: the typical service-oriented hierarchical ICPS architecture, critical challenges of implementing, and recent developments on ICPS in relevant research domains, from information acquisition to the control system design.

Although ICPSs potentially provide significant benefits and bring transformative opportunities to industry, society, and economy, gaps still exist between the ICPS theory and applications [8]. Some promising and practically demanding research thrusts need to be investigated to realize the benefits envisioned in industrial applications in the direction of the following:

1) *Integrated frameworks for the real-time ICPS monitoring, communication, and control:* The ICPS is composed of numerous embedded systems and communication networks. Therefore, it can benefit from the integrated

monitoring, communication, and control design approaches. The future development of theoretical foundations is expected to support the modeling of ICPS in an integrated fashion with the guarantee of dependability and reconfigurability. As mentioned in Section IV, most existing results on the ICPS focus on one perspective of monitoring, communication, and control. There is an urgent need to develop a unified framework for the codesign of monitoring, communication, computing, and control, where the integrated optimization of the plant-wide performance should be considered.

2) *Efficient management of heterogeneity and complexity for data and networks in ICPS migration solutions:* For the implementation and operation of ICPSs, how to migrate the legacy systems into the service-based collaborative ICPS ecosystems has a high priority [2]. Since ICPS should be able to operate, coexist, and integrate legacy systems during the migration to new infrastructures, the heterogeneity and complexity of data and communication networks are inevitably increased, resulting in significant obstacles to interoperability among physical and cyber components. How to efficiently manage the heterogeneity and complexity of data and networks and balance the interoperability and efficiency during the migration process should be primarily considered. Furthermore, how to design the metrics for evaluating the heterogeneity of data and networks during migration progress should be investigated.

3) *AI-assisted integrated safety and security protection for ICPSs:* The use of cloud platforms in ICPSs enables the storage of numerous data collected from sensors and the implementation of advanced intelligence data processing algorithms, offering an alternative way to design safety and security protection strategies for ICPSs based on AI technologies without requiring the sufficient knowledge of the physical models. From the communication perspective, based on AI paradigms, it is promising to design autonomous and intelligent communication networks capable of differentiating cyberattacks from legitimate traffic [16]. Leveraging AI in industrial agents can also enhance the process safety and security of the entire system. Owing to the convergence of safety and security threats in ICPSs, one challenge for AI-assisted safety and security protection solutions is to design a unique framework for simultaneous machine safety assessment and threat analysis. Another challenge lies in the limited bandwidth and latency constraints in the existing communication networks. How to efficiently deploy the AI mechanisms in ICPSs needs to be further investigated.

Finally, ICPS should not be seen as a stand-alone approach or technology and instead must be investigated in the wider context they operate and in conjunction with other satellite approaches [8]. For instance, the industrial acceptance of software agents is linked to design, technology, intelligence/algorithms, standardization, hardware, challenges, application, and cost [100], which also overlap with what ICPSs need to address in order to find widespread industrial applicability.

References

[1] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.

[2] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, Mar. 2017.

[3] S. Karnouskos, "Cyber-physical systems in the smartgrid," in *Proc. 9th IEEE Int. Conf. Ind. Informat.*, 2011, pp. 20–23.

[4] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[5] X. Guan, B. Yang, C. Chen, W. Dai, and Y. Wang, "A comprehensive overview of cyber-physical systems: From perspective of feedback system," *IEEE/CAA J. Autom. Sinica*, vol. 3, no. 1, pp. 1–14, Jan. 2016.

[6] C. Dufty, "The industrial IoT: A timeline of revolutionary technology," 2017. [Online]. Available: https://www.kepware.com/en-us/blog/2017/the-industrial-iot-a-timeline-of-revolutionary-te/

[7] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert, "Industrial Internet of Things and cyber manufacturing systems," in *Industrial Internet of Things*. New York, NY, USA: Springer, 2017, pp. 3–19.

[8] S. Karnouskos, P. Leitao, L. Ribeiro, and A. W. Colombo, "Industrial agents as a key enabler for realizing industrial cyber-physical systems: Multiagent systems entering Industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 14, no. 3, pp. 18–32, Sep. 2020.

[9] J. Jasperneite, T. Sauter, and M. Wollschlaeger, "Why we need automation models: Handling complexity in Industry 4.0 and the Internet of Things," *IEEE Ind. Electron. Mag.*, vol. 14, no. 1, pp. 29–40, Mar. 2020.

[10] S. Karnouskos, "Realising next-generation web service-driven industrial systems," *Int. J. Adv. Manuf. Technol.*, vol. 60, nos. 1–4, pp. 409–419, Sep. 2011.

[11] S. Karnouskos et al., "Towards the real-time enterprise: Service-based integration of heterogeneous SOA-ready industrial devices with enterprise applications," *IFAC Proc. Vol.*, vol. 42, no. 4, pp. 2131–2136, 2009.

[12] A. W. Colombo et al., *Industrial Cloud-Based Cyber-Physical Systems*. New York, NY, USA: Springer, 2014.

[13] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[14] K. Cao, S. Hu, Y. Shi, A. Colombo, S. Karnouskos, and X. Li, "A survey on edge and edge-cloud computing assisted cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7806–7819, Nov. 2021.

[15] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy efficient industrial Internet of Things: Overview and open issues," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7225–7237, Nov. 2021.

[16] I. Ahmad et al., "The challenges of artificial intelligence in wireless networks for the Internet of Things: Exploring opportunities for growth," *IEEE Ind. Electron. Mag.*, vol. 15, no. 1, pp. 16–29, Mar. 2021.

[17] A. Villalonga, G. Beruvides, F. Castano, and R. E. Haber, "Cloud-based industrial cyber–physical system for data-driven reasoning: A review and use case on an Industry 4.0 pilot line," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5975–5984, Sep. 2020.

[18] L. Ribeiro, J. Barata, A. Colombo, and F. Jammes, "A generic communication interface for DPWS-based web services," in *Proc. 6th IEEE Int. Conf. Ind. Informat.*, 2008, pp. 762–767.

[19] J. Delsing et al., "A migration approach towards a SOA-based next generation process control and monitoring," in *Proc. 37th Annu. Conf. IEEE Ind. Electron. Soc.*, 2011, pp. 4472–4477.

[20] A. W. Colombo, R. Neubert, and R. Schoop, "A solution to holonic control systems," in *Proc. 8th Int. Conf. Emerg. Technol. Factory Autom.*, 2001, pp. 489–498.

[21] P. Leitão, A. W. Colombo, and S. Karnouskos, "Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges," *Comput. Ind.*, vol. 81, pp. 11–25, Sep. 2016.

[22] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIOT),," in *Advances in Computers*, vol. 117. Amsterdam, The Netherlands: Elsevier, 2020, no. 1, pp. 129–164.

[23] *Enterprise-Control System Integration Part 1: Models and Terminology*, ISA Standard ANSI/ISA-95.00.01-2000 (IEC 62264-1 Mod), 2010.

[24] T. Sauter, "Integration aspects in automation—A technology survey," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, 2005, pp. 255–263.

[25] *Reference Architecture Model Industrie 4.0 (RAMI4.0)*, DIN Standard DIN SPEC 91345, 2016. [Online]. Available: https://www.din.de/en/wdc-beuth:din21:250940128

[26] *Details of the Asset Administration Shell—Part 1*, Platform Industrie 4.0 Standard, May 2022. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part1_V3.html

[27] *Details of the Asset Administration Shell—Part 2*, Platform Industrie 4.0 Standard, Nov. 2021. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part_2_V1.html

[28] J. Fuchs, J. Schmidt, J. Franke, K. Rehman, M. Sauer, and S. Karnouskos, "I4.0-compliant integration of assets utilizing the Asset Administration Shell," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom.*, 2019, pp. 1243–1247.

[29] S.-W. Lin et al., "Architecture alignment and interoperability," Industrial Internet Consortium, Boston, MA, USA, Tech. Rep. IIC:WHT:IN3: V1.0:PB:20171205, 2017. [Online]. Available: https://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf

[30] S.-W. Lin et al., "Industrial internet reference architecture," 2015. [Online]. Available: https://www.iiconsortium.org/IIRA.htm

[31] G. Pedone and I. Mezgár, "Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 technologies," *Comput. Ind.*, vol. 100, pp. 278–286, 2018.

[32] M. Moghaddam, M. N. Cadavid, C. R. Kenley, and A. V. Deshmukh, "Reference architectures for smart manufacturing: A critical review," *J. Manuf. Syst.*, vol. 49, pp. 215–225, 2018.

[33] D. G. Pivoto, L. F. de Almeida, R. da Rosa Righi, J. J. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial Internet of Things applications in Industry 4.0: A literature review," *J. Manuf. Syst.*, vol. 58, pp. 176–192, 2021.

[34] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[35] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From Industry 4.0 to Agriculture 4.0: Current status, enabling technologies, and research challenges," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4322–4334, Jun. 2021.

[36] C. Lu et al., "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1013–1024, May 2016.

[37] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA Trans.*, vol. 116, pp. 1–16, Jan. 2021.

[38] S. Soucek, T. Sauter, and T. Rauscher, "A scheme to determine QoS requirements for control network data over IP," in *Proc. 27th Annu. Conf. IEEE Ind. Electron. Soc.*, 2001, pp. 153–158.

[39] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and Industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[40] S. Yin, J. J. Rodriguez-Andina, and Y. Jiang, "Real-time monitoring and control of industrial cyberphysical systems: With integrated plant-wide monitoring and control framework," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 38–47, Dec. 2019.

[41] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[42] A. Termehchi and M. Rasti, "Joint sampling time and resource allocation for power efficiency in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2600–2610, Apr. 2021.

[43] A. Saifullah et al., "Near optimal rate selection for wireless control systems," *ACM Trans. Embedded Comput. Syst.*, vol. 13, no. 4s, pp. 1–25, 2014.

[44] C. Luo, F. Wu, J. Sun, and C. W. Chen, "Compressive data gathering for large-scale wireless sensor networks," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, 2009, pp. 145–156.

[45] R. Rana, M. Yang, T. Wark, C. T. Chou, and W. Hu, "SimpleTrack: Adaptive trajectory compression with deterministic projection matrix for mobile sensor networks," *IEEE Sens. J.*, vol. 15, no. 1, pp. 365–373, Jan. 2015.

[46] X. Luo, D. Zhang, L. T. Yang, J. Liu, X. Chang, and H. Ning, "A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems," *Cyber-Enabled Intell.*, pp. 37–66, Aug. 2019.

[47] L. Qi et al., "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4159–4167, Jun. 2021.

[48] P. Wang, L. T. Yang, J. Li, J. Chen, and S. Hu, "Data fusion in cyber-physical-social systems: State-of-the-art and perspectives," *Inf. Fusion*, vol. 51, pp. 42–57, Nov. 2019.

[49] H. Tao et al., "TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3311–3321, May 2020.

[50] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system," *Future Gener. Comput. Syst.*, vol. 108, pp. 1287–1296, Jul. 2020.

[51] Y. Lu and M. Zhu, "A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems," *Annu. Rev. Control*, vol. 47, pp. 423–440, 2019.

[52] A. Treytl, T. Sauter, and C. Schwaiger, "Security measures in automation systems—A practice-oriented approach," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, 2005, pp. 847–855.

[53] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proc. IEEE*, vol. 109, no. 4, pp. 517–541, Apr. 2021.

[54] I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," in *Cyber Resilience of Systems and Networks*. New York, NY, USA: Springer, May 2018, pp. 1–25.

[55] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annu. Rev. Control*, vol. 47, pp. 394–411, 2019.

[56] M. Ehrlich et al., "Alignment of safety and security risk assessments for modular production systems," *Elektrotechnik und Informationstechnik*, vol. 138, no. 7, pp. 454–461, Sep. 2021.

[57] S. Hollerer, W. Kastner, and T. Sauter, "Towards a threat modeling approach addressing security and safety in OT environments," in *Proc. 17th IEEE Int. Conf. Factory Commun. Syst.*, 2021, pp. 37–40.

[58] A. M. Hosseini, T. Sauter, and W. Kastner, "Towards adding safety and security properties to the Industry 4.0 asset administration shell," in *Proc. 17th IEEE Int. Conf. Factory Commun. Syst.*, 2021, pp. 41–44.

[59] V. Jirkovskỳ, M. Obitko, and V. Mařík, "Understanding data heterogeneity in the context of cyber-physical systems integration," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 660–667, Apr. 2017.

[60] O. Givehchi, K. Landsdorf, P. Simoens, and A. W. Colombo, "Interoperability for industrial cyber-physical systems: An approach for legacy systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3370–3378, Dec. 2017.

[61] A. L. Szejka, O. Canciglieri Jr, H. Panetto, E. R. Loures, and A. Aubry, "Semantic interoperability for an integrated product development process: A systematic literature review," *Int. J. Prod. Res.*, vol. 55, no. 22, pp. 6691–6709, 2017.

[62] S. Sučić, J. G. Havelka, and T. Dragičević, "A device-level service-oriented middleware platform for self-manageable DC microgrid applications utilizing semantic-enabled distributed energy resources," *Int. J. Elect. Power Energy Syst.*, vol. 54, pp. 576–588, 2014.

[63] Y. Cui, V. K. N. Lau, R. Wang, H. Huang, and S. Zhang, "A survey on delay-aware resource control for wireless systems—Large deviation theory, stochastic Lyapunov drift, and distributed stochastic learning," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1677–1701, Mar. 2012.

[64] F. Song, Z. Ai, H. Zhang, I. You, and S. Li, "Smart collaborative balancing for dependable network components in cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6916–6924, Oct. 2021.

[65] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A survey on end-edge-cloud orchestrated network computing paradigms," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–36, Nov. 2020.

[66] K. Thramboulidis, D. C. Vachtsevanou, and I. Kontou, "CPuS-IoT: A cyber-physical microservice and IoT-based framework for manufacturing assembly systems," *Annu. Rev. Control*, vol. 47, pp. 237–248, 2019.

[67] I. Baldini et al., "Serverless computing: Current trends and open problems," in *Research Advances in Cloud Computing*. New York, NY, USA: Springer, 2017, pp. 1–20.

[68] Z. Benomar, F. Longo, G. Merlino, and A. Puliafito, "Deviceless: A serverless approach for the Internet of Things," in *Proc. ITU Kaleidoscope, Connecting Phys. Virtual Worlds*, 2021, pp. 1–8.

[69] X. Cao, P. Cheng, J. Chen, and Y. Sun, "An online optimization approach for control and communication codesign in networked cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 439–450, Feb. 2013.

[70] L. Peng, X. Cao, and C. Sun, "Optimal transmit power allocation for an energy-harvesting sensor in wireless cyber-physical systems," *IEEE Trans. Cybern.*, vol. 51, no. 2, pp. 779–788, Feb. 2021.

[71] X.-M. Zhang et al., “Networked control systems: A survey of trends and techniques,” *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.

[72] P. Tabuada, S. Y. Caliskan, M. Rungger, and R. Majumdar, “Towards robustness for cyber-physical systems,” *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3151–3163, Dec. 2014.

[73] Y. Gao, G. Sun, J. Liu, Y. Shi, and L. Wu, “State estimation and self-triggered control of CPSs against joint sensor and actuator attacks,” *Automatica*, vol. 113, Mar. 2020, Art. no. 108687.

[74] X. Huang and J. Dong, “Modularized design for cooperative control of cyber-physical systems with disturbances and general cooperative targets,” *J. Franklin Inst.*, vol. 357, no. 15, pp. 10799–10809, Oct. 2020.

[75] S. Spinelli, A. Cataldo, G. Pallucca, and A. Brusaferri, “A distributed control architecture for a reconfigurable manufacturing plant,” in *Proc. IEEE Ind. Cyber-Phys. Syst.*, May 2018, pp. 673–678.

[76] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2483–2499, May 2019.

[77] M. Lin, Y. Pan, L. T. Yang, M. Guo, and N. Zheng, “Scheduling co-design for reliability and energy in cyber-physical systems,” *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 353–365, Dec. 2013.

[78] M. Shi, H. He, J. Li, M. Han, and C. Jia, “Multi-objective tradeoff optimization of predictive adaptive cruising control for autonomous electric buses: A cyber-physical-energy system approach,” *Appl. Energy*, vol. 300, Oct. 2021, Art. no. 117385.

[79] F. Tao, Q. Qi, L. Wang, and A. Nee, “Digital twins and cyber–physical systems toward smart manufacturing and Industry 4.0: Correlation and comparison,” *Engineering*, vol. 5, no. 4, pp. 653–661, 2019.

[80] Y. Jiang, S. Yin, K. Li, H. Luo, and O. Kaynak, “Industrial applications of digital twins,” *Philos. Trans. Roy. Soc. A*, vol. 379, no. 2207, 2021, Art. no. 20200360.

[81] Y. Jiang, S. Yin, and O. Kaynak, “Performance supervised plant-wide process monitoring in Industry 4.0: A roadmap,” *IEEE Open J. Ind. Electron. Soc.*, vol. 2, pp. 21–35, 2020.

[82] A. Wendt, S. Kollmann, A. Bratukhin, A. Estaji, T. Sauter, and A. Jantsch, “Cognitive architectures for process monitoring—An analysis,” in *Proc. 2020 IEEE 18th Int. Conf. Ind. Informat.*, 2020, pp. 167–173.

[83] C. Cristalli et al., “Integration of process and quality control using multi-agent technology,” in *Proc. IEEE Int. Symp. Ind. Electron.*, 2013, pp. 1–6.

[84] C. A. Marin et al., “A conceptual architecture based on intelligent services for manufacturing support systems,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, 2013, pp. 4749–4754.

[85] C. Liu, H. Vengayil, Y. Lu, and X. Xu, “A cyber-physical machine tools platform using OPC UA and MTConnect,” *J. Manuf. Syst.*, vol. 51, pp. 61–74, 2019.

[86] R. Beregi, G. Pedone, and I. Mezgár, “A novel fluid architecture for cyber-physical production systems,” *Int. J. Comput. Integr. Manuf.*, vol. 32, nos. 4/5, pp. 340–351, 2019.

[87] R. Harrison, D. A. Vera, and B. Ahmad, “A connective framework to support the lifecycle of cyber-physical production systems,” *Proc. IEEE*, vol. 109, no. 4, pp. 568–581, Apr. 2021.

[88] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, “An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges,” *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018.

[89] C.-R. Rad, O. Hancu, I.-A. Takacs, and G. Olteanu, “Smart monitoring of potato crop: A cyber-physical system architecture model in the field of precision agriculture,” *Agriculture Agricultural Sci. Procedia*, vol. 6, pp. 73–79, 2015.

[90] J. Ruan, H. Jiang, X. Li, Y. Shi, F. T. S. Chan, and W. Rao, “A granular GA-SVM predictor for big data in agricultural cyber-physical systems,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6510–6521, Dec. 2019.

[91] P. Guo, P. O. Dusadeerungsikul, and S. Y. Nof, “Agricultural cyber physical system collaboration for greenhouse stress management,” *Comput. Electron. Agriculture*, vol. 150, pp. 439–454, 2018.

[92] M. Kang, X.-R. Fan, J. Hua, H. Wang, X. Wang, and F.-Y. Wang, “Managing traditional solar greenhouse with CPSS: A just-for-fit philosophy,” *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3371–3380, Dec. 2018.

[93] L. D’Agati, Z. Benomar, F. Longo, G. Merlino, A. Puliafito, and G. Tricomi, “IoT/cloud-powered crowdsourced mobility services for green smart cities,” in *Proc. IEEE 20th Int. Symp. Netw. Comput. Appl.*, 2021, pp. 1–8.

[94] F. Longo, D. Bruneo, S. Distefano, G. Merlino, and A. Puliafito, “Stack4Things: A sensing-and-actuation-as-a-service framework for IoT and cloud integration,” *Ann. Telecommun.*, vol. 72, no. 1, pp. 53–70, 2017.

[95] K.-C. Chang, K.-C. Chu, H.-C. Wang, Y.-C. Lin, and J.-S. Pan, “Agent-based middleware framework using distributed CPS for improving resource utilization in smart city,” *Future Gener. Comput. Syst.*, vol. 108, pp. 445–453, Jul. 2020.

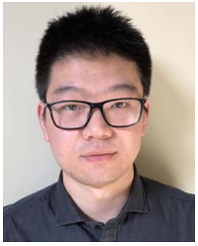
[96] I. Jawhar, N. Mohamed, and J. Al-Jaroodi, “Networking architectures and protocols for smart city systems,” *J. Internet Serv. Appl.*, vol. 9, no. 1, 2018, Art. no. 26.

[97] A. Dimeas et al., “Smart houses in the smart grid: Developing an interactive network,” *IEEE Electrific. Mag.*, vol. 2, no. 1, pp. 81–93, Mar. 2014.

[98] H. Xu, J. Lin, and W. Yu, “Smart transportation systems: Architecture, enabling technologies, and open issues,” in *Secure and Trustworthy Transportation Cyber-Physical Systems*. New York, NY, USA: Springer, 2017, pp. 23–49.

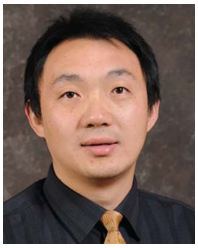
[99] J. Zhang, Y. Wang, S. Li, and S. Shi, “An architecture for IoT-enabled smart transportation security system: A geospatial approach,” *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6205–6213, Apr. 2021.

[100] S. Karnouskos and P. Leitao, “Key contributing factors to the acceptance of agents in industrial environments,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 696–703, Apr. 2017.



Kunwu Zhang (Member, IEEE) received the M.A.Sc. and Ph.D. degrees in mechanical engineering from the University of Victoria, Victoria, BC, Canada, in 2016 and 2021, respectively.

Since January 2022, he has been a Postdoctoral Researcher with the Department of Mechanical Engineering, University of Victoria. His current research interests include adaptive control, model-predictive control, optimization, and robotic systems.



Yang Shi (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2005.

From 2005 to 2009, he was an Assistant Professor and an Associate Professor with the Department of Mechanical Engineering, University of Saskatchewan, Saskatoon, SK, Canada. In 2009, he joined the University of Victoria (UVic), Victoria, BC, Canada, where he is currently a Professor with the Department of Mechanical Engineering. His current research interests include networked and distributed systems, model-predictive control, cyber-physical systems, robotics and mechatronics, navigation and control of autonomous systems (autonomous underwater vehicle and unmanned aerial vehicle), and energy system applications.

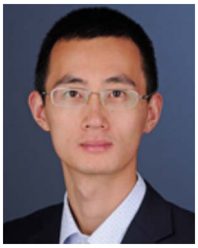
Dr. Shi received the University of Saskatchewan Student Union Teaching Excellence Award in 2007, and the Faculty of Engineering Teaching Excellence Award in 2012 at UVic. He is the recipient of the JSPS Invitation Fellowship (short-term) in 2013, the UVic Craigdarroch Silver Medal for Excellence in Research in 2015, the 2016 IEEE TRANSACTIONS ON FUZZY SYSTEMS Outstanding Paper Award, and the Humboldt Research Fellowship for Experienced Researchers in 2018. He is the Vice-President for Conference Activities of the IEEE Industrial Electronics Society (IES) for the period 2022–2023. He was a Member of the IES Fellow Evaluation Committee from 2017 to 2019. He is the Chair of IEEE IES Technical Committee on Industrial Cyber-Physical Systems. He is Co-Editor-in-Chief for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. He is an Associate Editor for *Automatica* and IEEE TRANSACTIONS ON AUTOMATIC CONTROL. He is a General Chair of 2019 International Symposium on Industrial Electronics and 2021 International Conference on Industrial Cyber-Physical Systems. He is a Fellow of the American Society of Mechanical Engineers, the Engineering Institute of Canada, and the Canadian Society for Mechanical Engineering. He is a registered Professional Engineer in British Columbia, Canada.

Stamatis Karnouskos (Fellow, IEEE) is with SAP, Walldorf, Germany, dealing with technology foresight, especially in the scope of industrial technologies and enterprise systems. For more than 25 years, he has led efforts in several European Commission and industry-funded projects related to cyber-physical systems, the Internet of Things, industrial automation, smart grids, cloud-based services and architectures, software agents, security, and mobility. He has extensive experience in research and technology management within the industry, as well as with the European Commission and several national research funding bodies. He is an Associate Editor for several IEEE journals and has coauthored/edited several books relevant to the Industrial Internet of Things and industrial cyber-physical systems.

Thilo Sauter (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the Vienna University of Technology, Vienna, Austria, in 1999.

He was the founding Director of the Department for Integrated Sensor Systems, University for Continuing Education Krems, Wiener Neustadt, Austria. He is currently a Professor of Automation Technology with the Vienna University of Technology. He is the author of more than 350 scientific publications and has held leading positions in renowned IEEE conferences. Moreover, he has been involved in the standardization of industrial communications for more than 25 years. His expertise and research interests include embedded systems and integrated circuit design, smart sensors, and automation and sensor networks with a focus on real-time, security, interconnection, and integration issues relevant to cyber-physical systems and the Internet of Things in various application domains, such as industrial and building automation, smart manufacturing, or smart grids.

Dr. Sauter is a Senior Administrative Committee Member of the IEEE Industrial Electronics Society.



Huazhen Fang (Member, IEEE) received the B.Eng. degree in computer science and technology from Northwestern Polytechnic University, Xi'an, China, in 2006, the M.Sc. degree from the University of Saskatchewan, Saskatoon, SK, Canada, in 2009, and the Ph.D. degree from the University of California, San Diego, CA, USA, in 2014, both in mechanical engineering.

He is currently an Associate Professor of Mechanical Engineering with the University of Kansas, Lawrence, KS, USA. His research interests include control and estimation theory with application to energy management and cooperative robotics.

Dr. Fang was a recipient of the 2019 National Science Foundation CAREER Award. He is an Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE CONTROL SYSTEMS LETTERS, and *Information Sciences*.

Armando Walter Colombo (Fellow, IEEE) received the B.Sc. degree in electronics engineering from the National Technological University of Mendoza, Mendoza, Argentina, in 1990, the M.Sc. degree in control system engineering from the National University of San Juan, San Juan, Argentina, in 1994, and the Ph.D. degree in engineering (manufacturing automation and systematization) from the University of Erlangen-Nuremberg, Erlangen, Germany, in 1998.

He is currently with the Department of Electrotechnical and Computer Sciences, University of Applied Sciences Emden/Leer, Emden, Germany, where he became a Full Professor in August 2010 and the Director of the Institute for Industrial Informatics, Automation and Robotics (I2AR) in 2012. From 2001 to 2018, he was a Manager for Collaborative Innovation Programs and as Edison Level 2 Group Senior Expert with Schneider Electric Corp. He has more than 30 industrial patents and more than 300 peer-reviewed publications. With his contributions, he has performed scientific and technical seminal contributions that are nowadays being used as one of the bases of what is recognized as "The 4th Industrial Revolution." His research interests include industrial cyber-physical systems, industrial digitalization, engineering of Industry 4.0-compliant solutions, system-of-systems engineering, industrial Internet of Things, and intelligent production automation systems.

Dr. Colombo is a Co-Editor-in-Chief for IEEE OPEN ACCESS JOURNAL of the IEEE Industrial Electronics Society, a Distinguished Lecturer of the IEEE Systems Council, a Senior AdCom Member of the IEEE Industrial Electronics Society, and a Member of the IEEE European Public Policy Committee. He is an Expert in the KDT-JU ECSEL as well as in the REA of the European Union and EUREKA programs. He is listed in Who's Who in the World/Engineering 99-00/01 and in Outstanding People of the XX Century (Bibliographic Centre Cambridge, U.K.).