Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges

Jian-Qiang Li, F. Richard Yu, *Senior Member, IEEE*, Genqiang Deng,
Chengwen Luo, Zhong Ming, and Qiao Yan

***Abstract*—This paper provides an overview of the Industrial Internet with the emphasis on the architecture, enabling technologies, applications, and existing challenges. The Industrial Internet is enabled by recent rising sensing, communication, cloud computing, and big data analytic technologies, and has been receiving much attention in the industrial section due to its potential for smarter and more efficient industrial productions. With the merge of intelligent devices, intelligent systems, and intelligent decisioning with the latest information technologies, the Industrial Internet will enhance the productivity, reduce cost and wastes through the entire industrial economy. This paper starts by investigating the brief history of the Industrial Internet. We then present the 5C architecture that is widely adopted to characterize the Industrial Internet systems. Then, we investigate the enabling technologies of each layer that cover from industrial networking, industrial intelligent sensing, cloud computing, big data, smart control, and security management. This provides the foundations for those who are interested in understanding the essence and key enablers of the Industrial Internet. Moreover, we discuss the application domains that are gradually transformed by the Industrial Internet technologies, including energy, health care, manufacturing, public section, and transportation. Finally, we present the current technological challenges in developing Industrial Internet systems to illustrate open research questions that need to be addressed to fully realize the potential of future Industrial Internet systems.**

***Index Terms*—Industrial Internet, 5C architecture, enabling technologies, application, challenge.**

I. Introduction

OVER the last two hundred years, the world has experienced four major waves of innovations [1]. The first wave of innovations, known as the Industrial Revolution, started in the mid-eighteenth century with the introduction of the steam engine into the industrial production process. The second wave started at the beginning of 20th century and accelerated the industrial evolution by the introduction of electricity. In the 1950s, the third wave started with the development of the modern computing technologies and the invention of the Internet that connects computers with one another. The in-depth merging of the Industrial Revolution and the Internet Revolution, results in a new wave of the *Industrial Internet* revolution [1], [2].

The Industrial Internet, or Industry 4.0, has attracted great interests from both industry and academia as the fourth industrial revolution due to the rise of recent exponentially growing technologies (e.g., big data [3], cloud computing [4], networking [5], 3D printing [6], artificial intelligence [7], etc.). For example, different sensor data will be collected and sent to cloud computing for smart decisioning using big data technologies. In manufacturing, 3D printing technology also produces customized products of almost any shape at a lower costs but within a very short duration [8]. The Industrial Internet is often understood as the application of the generic concept of Cyber Physical Systems (CPSs) [9], [10], within which the information from all industrial perspectives is closely collected, monitored from the physical space and synchronized with the cyber space. The demand of having information and services everywhere made CPS an inevitable trend in the highly networked world of today. And today there are many fields of applications for CPS in the industry, such as medical equipment, driving safety and driver assistance systems for automobiles, industrial process control and automation systems, etc. [11]. The melding of the physical industrial components, machines, fleets and factories with the advanced modern sensing and networking technologies, and big data analytics opens up tremendous opportunities to accelerate productivity, reduce inefficiency and waste, and enhance the working experience in the production process. The Industrial Internet has the potential to bring profound transformation to traditional industries, such as manufacturing, aviation, rail transportation, health care, power generation, oil and gas development, etc. [1].

The vision of the Industrial Internet heavily depends on the adoption of advanced information and communication technologies in traditional industries. Several streams of enabling technologies are involved in the Industrial Internet, including industrial networking, industrial sensing and control, big data, cloud computing, security, etc. These technologies cover different aspects of the industrial production process such as analytics, storage, sensing, connection, automation, Human-Machine Interaction (HMI), and manufacturing.

Manuscript received August 24, 2016; revised December 18, 2016 and February 21, 2017; accepted March 23, 2017. Date of publication April 5, 2017; date of current version August 21, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61300174, Grant 61572330, and Grant 61602319, in part by the Natural Science Foundation of SZU under Grant 2016048, and in part by the Technology Planning Project from Guangdong Province, China, under Grant 2014B010118005. *(Corresponding author: Chengwen Luo.)*

J.-Q. Li, G. Deng, C. Luo, Z. Ming, and Q. Yan are with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518000, China (e-mail: lijq@szu.edu.cn; 956271303@qq.com; chengwen@szu.edu.cn; mingz@szu.edu.cn; yanq@szu.edu.cn).

F. R. Yu is with the School of Information Technology, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: richard.yu@carleton.ca).

Digital Object Identifier 10.1109/COMST.2017.2691349

1553-877X © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

Despite the significant development of the Industrial Internet in both theory and practice, numerous challenges exist and need to be addressed to fully realize its potential. For example, industrial systems are designed to have strict performance and reliability requirements. When performing critical functionalities, industrial systems are designed to have strict performance requirements, such as stability, accuracy and resistance against extreme environments and long-term operation, etc. [12], owing to their critical functionalities. In addition, These systems often use highly-customized infrastructure programmed for specific tasks, with life-cycles of over 15−20 years [13]. Moreover, security vulnerability when exploited may result in huge lost in industrial systems. As a result, in the realization of the Industrial Internet, security becomes a huge challenge and is still under exploration. Furthermore, to ensure a safe, efficient, and productive industrial production environment, other challenges associated with the integration of the Information Communication Technologies (ICTs) with the industrial environment need to be carefully addressed, such as big data analytics, advanced sensing, networking, etc.

In this paper, we provide a brief survey on some of the works that have already been done on the Industrial Internet, and discuss some research issues and challenges. To the best of our knowledge, this paper is the first survey on the Industrial Internet that covers the architecture, enabling technologies, applications, and challenges. The contributions of this paper can be summarized as:

- We present the architecture of the Industrial Internet and discuss its key properties.
- We discuss the recent advances of the enabling technologies, including big data, cloud computing, networking, artificial intelligence, and augmented reality technologies, to enable researchers to quickly get up to speed with the key enablers of the Industrial Internet.
- We provide an overview of the key applications and their integration with the Industrial Internet technologies.
- We also discuss the current technical challenges and open research issues that need to be addressed to fully realize the potential of the Industrial Internet.

The roadmap of this paper is given in Fig. 1. Section II introduces the brief history of the Industrial Internet, and Section III presents the architecture of the Industrial Internet. In Section IV, we discuss the key enabling technologies of the Industrial Internet, and Section V presents the applications. Section VI summarizes the current technical challenges and open research issues. And finally, we conclude this work in Section VII.

II. Brief History

The recent rise of the Industrial Internet has been preceded by several industrial and technological revolutions in the history of mankind. Fig. 2 shows the brief history of the Industrial Internet development. The first industrial revolution was driven by the introduction of steam engines in the second half of the 18th century. The automation enabled by the steam engines reforms the industrial production from period of pure manual labor to the era of mechanization, which resulted in an extreme increase in the productivity. Since 1870s, the replacement of steam by electricity and the division of labor resulted in another industrial revolution with productivity explosion. The third industrial revolution, which is known as the "digitalization", was introduce around 1960s, when advanced electronics and programmable logic controllers developed further improved the production efficiency and led to automation systems.

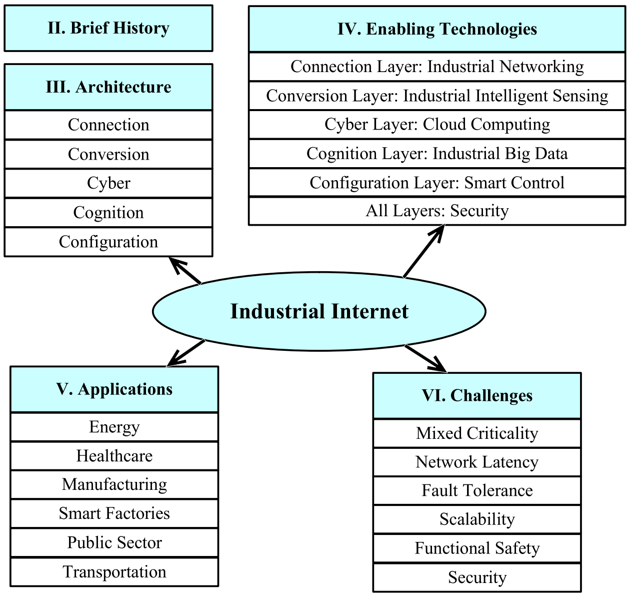


Fig. 1. Roadmap of this paper.

From the end of the 20th century to the beginning of the 21st century, the information and communication technologies grew exponentially, which resulted in a spectrum of new technologies such as Radio Frequency Identification (RFID) (1940s), Artificial Intelligence (AI) (1950s), Sensor Networks (1970s), 3D Printing (1980s), IoT (1990s), Cyber-Physical Systems (2005), Cloud Computing (2006), Big Data (2008), etc. These technologies significantly improve the industrial production by increasing the intelligence in the sensing (RFID and IoT), networking (Sensor Network and Cloud Computing), decisioning (Artificial Intelligence and Big Data), control (CPS), and manufacturing (3D printing). With the vision of combining the advanced information technologies with traditional industries, the Industrial Internet is currently prevalent in both academic and industrial communities. The term Industry 4.0 was first used at the Hanover Fair in 2011 that refers to the fourth industrial revolution, and has been attracting much attention in Europe. German federal government announced Industry 4.0 as one of the key initiatives of its national high-tech strategy [14], and numerous academic projects, research articles, and conferences have focused on this topic [2]. In 2012, General Electric (GE) Inc. brought up the similar vision, and coined it as the Industrial Internet. It is remarkable that the new industrial revolution is known a priori, and the idea of the Industrial Internet has the potential to be as formative as the previous three Industrial Revolutions [14]. In 2014, the Industrial Internet Consortium (IIC) [15] was founded by AT&T, Cisco, Genral Electric, IBM and Intel,

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

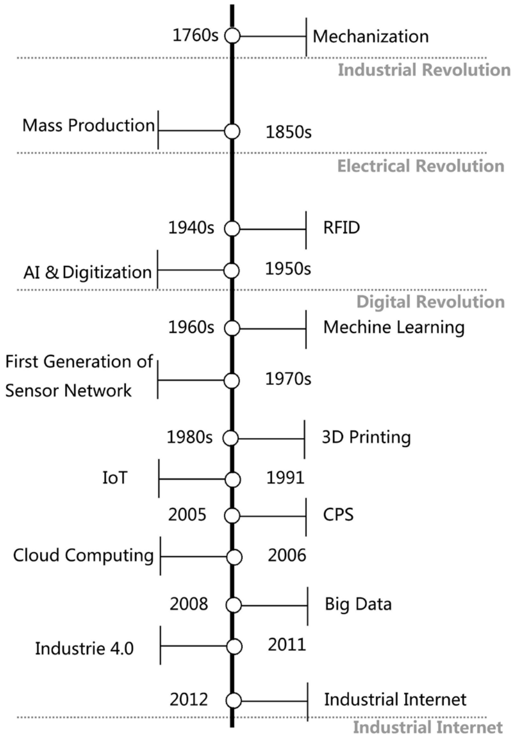


Fig. 2. Timeline of key milestones of the Industrial Internet.

which sets benchmark for the Industrial Internet and promotes the development of the Industrial Internet. To date, IIC is an open membership organization with 237 members. The IIC was formed to accelerate the development, adoption and widespread use of interconnected machines and devices, and intelligent analytics.

III. The Architecture of the Industrial Internet

The Industrial Internet is generally understood as the application of CPS [14]. Since the Industrial Internet is at its early development phase, understanding the architecture of typical Industrial Internet systems plays an important role in the system design. A generally adopted architecture is the unified 5-level architecture, namely the 5C architecture [16].

As shown in Fig. 3, the 5C architecture consists of five different layers: *smart connection level*, *data-to-information conversion level*, *cyber level*, *cognition level*, and *configuration level*. These layers support different functionalities and can be mainly divided into two functional components: (1) the smart and reliable bidirectional connectivity component that supports efficient real-time data acquisition from the physical space and feedback from the cyber space; (2) intelligent data fusion and analytics component that supports smart decisioning.

The properties of each 5C layer are shown in Fig. 4. In the connection layer, sensors collect the raw data using reliable communications provided by the industrial filed bus, and communication protocols such as NB-IOT, LoRa, and 5G. Then conversion layer extracts the useful information for each individual device using intelligent sensing technologies. The cyber layer connects distributed devices to form a network of machines and fuses individual information using cloud computing technologies. The cognition layer merges

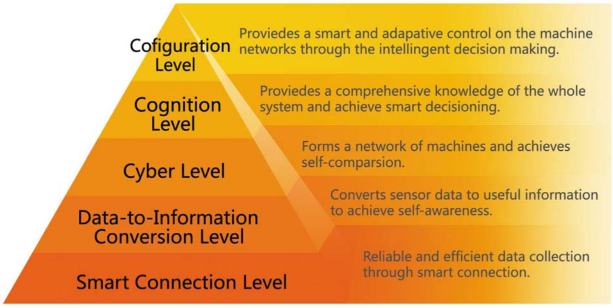

Cofiguration Level
Proviedes a smart and adapative control on the machine networks through the intellingent decision making.
Cognition Level
Proviedes a comprehensive knowledge of the whole system and achieve smart decisioning.
Cyber Level
Forms a network of machines and achieves self-comparsion.
Data-to-Information Conversion Level
Converts sensor data to useful information to achieve self-awareness.
Smart Connection Level
Reliable and efficient data collection through smart connection.

Fig. 3. 5C architecture of the Industrial Internet.

all information and generates comprehensive knowledge using big data analytics. And finally, intelligent decisions are made automatically in the configuration layer.

The detail of the 5C architecture is summarized as follows.

A. Connection

This layer handles the accurate data acquisition in the Industrial Internet. The data source of the Industrial Internet includes the direct sensor input and the data from controller or enterprise manufacturing systems, such as Enterprise Resource Planning (ERP), Manufacturing Execution System (MES), or Capability Maturity Model (CMM) for Software [16]. Since the physical devices in different Industrial Internet systems are usually produced by different manufacturers, the heterogeneity of hardware and software makes it especially challenging to inter-connect different physical components. Besides, selecting proper sensors as data sources is also one important concern at this layer. As a result, reliable, efficient, and general protocols that are able to handle the heterogeneity of different data sources are the key concern at this level.

B. Conversion

The collected raw data from sensors or other data sources needs to be processed and useful information needs to be inferred before moving to the next layer. In recent years, extensive research effort has been applied aiming to achieve the context-awareness from the sensor data. For example, based on the collected sensor data, machines provide health diagnosis to themselves, remaining useful life estimation, and other machine-related information. By converting the raw data to the useful information, the second layer brings *self-awareness* to physical components in Industrial Internet systems.

C. Cyber

The cyber layer in this architecture retrieves the information from all connected machines and serves as a central information hub for data processing in the Industrial Internet. Research on the cyber layer has been extensively studied in the area of cloud computing and has attracted great attentions recently. The collected machines in this layer forms a network of machines, and the data are fused in this layer to support functionalities of upper layers such as smart decisioning. By comparing with other machines, each machine achieves the *self-comparison* ability, thus the performance of each machine can be compared and rated among a network

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

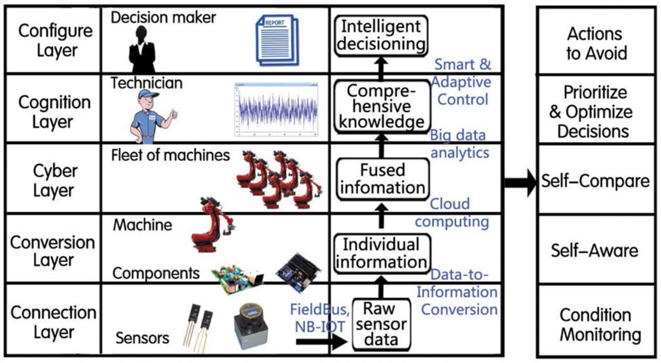


Fig. 4. Properties of each 5C layer.

of machines [16]. And by similarity measurement, future performance predictions can be achieved for each machine.

D. Cognition

In the cognition layer, the system collects both the individual machinery information and the integrated information from the machine network. The gathered information provides the system a comprehensive knowledge of the whole monitored system. By using the technology such as big data analytics, smart decisioning on prioritize task scheduling or system optimizations can be done. Using a proper presentation to organize the knowledge of the system is also another key concern in this layer, and is used for system users to directly obtain the knowledge acquired.

E. Configuration

The configuration layer provides feedback from the user or the decisions made by the cognition layer to the physical machines. This layer provides a smart and adaptive control on the machine networks through the intelligent decision making. By closing the loop from the cyber space to the physical space, this layer acts as a smart control system to provide the monitored system the ability of *self-configuration* and *self-adaptiveness*.

IV. Enabling Technologies of the Industrial Internet

The realization of the potential of the Industrial Internet heavily relies on multiple enabling technologies, understanding which helps to gain insights on the functionalities of the Industrial Internet. In this section, we focus on the enabling technologies in each of the above mentioned five layers in the 5C architecture. In particular, we discuss the networking, sensing, cloud computing, big data, and smart control that constitute the key enablers of each layer.

A. Connection Layer: Industrial Networking

In complex industrial systems such as a modern smart factory, usually a distributed network of controllers is involved. The network involves multiple entities [17] and connects the sensors, actuators, machines, lights, switches, etc., in the factory with other factories, customers, and suppliers to form a connected industrial production system. A typical networking architecture of the Industrial Internet is shown in Fig. 5. When smart factories collect the demand from customers and generate customized order, the smart suppliers intelligently provide services based on the factories orders and feedbacks. In the production, the factory uses the industrial sensing technology to provide real-time monitoring to each stage of the production process. And the data of smart factory will be uploaded to the cloud server for big data analytics and smart decisioning. In this architecture, industrial networking plays a key role to provide reliable and efficient communications to connect different elements in the Industrial Internet system. The industrial networking technologies include the classical fieldbus technologies and rising communication standards, such as LoRa, NB-IoT, 5G, etc.

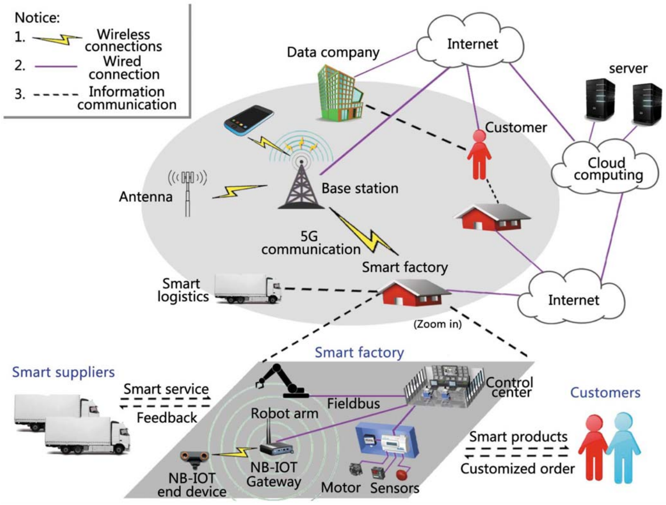


Fig. 5. A networking architecture of the Industrial Internet.

1) Foundation Fieldbus (FF): Developed by the Fieldbus Foundation, the FF serves as a base-level network in industrial systems such as a plant or a factory. FF adopts the simplified model of Open Systems Interconnection (OSI) architecture with physical layer, data link layer, and application layer. Two implementations of FF have been used in industrial environments, *FF H1* and *High-speed Ethernet (HSE)*. They use different physical media and have different data rates. H1 adopts the transmission rate of 31.25 Kbps, and the communication distance supports up to 1900 m. It uses the powered bus and can be used in intrinsically safe environments. HSE has a higher transmission rate of 1 Mbps and can reach up to 2.5 Mbps, with communication distance of 750m and 500m, respectively. HSE supports twisted pair, fiber optic but not the powered cables. In the physical layer, FF uses Manchester encoding [18]. The FF technology is mostly used in process industries. Recently, FF has also been implemented in power plants.

2) Controller Area Network (CAN): First introduced by the German BOSCH company in 1983 and made freely available, the CAN has been widely used in the field of discrete control in industrial systems. In 1993 the International Organization for Standardization released the CAN standard International Standards Organization (ISO) 11898. After that it has been

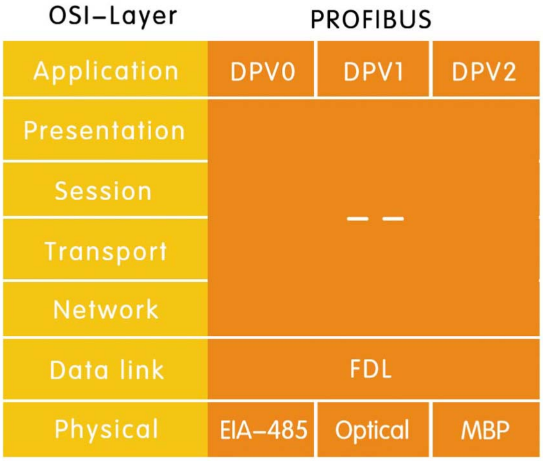
Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

used by Intel, Motorola, NEC and other companies. CAN protocol can be divided into two-layers: the physical layer and the data link layer. The data transmission of CAN uses short frame structure, as a result, the transmission time for each frame is short. CAN has an auto-off feature and has strong anti-jamming capability, which makes it a reliable industrial networking protocol. CAN supports multi-master tasks, and uses non-destructive bus arbitration technology by setting priorities to avoid transmission conflicts. The communication distances of CAN is up to 10km, and the communication rate is up to 40Mbp. CAN supports up to 110 number of nodes in the same system. Currently there are a number of companies developing CAN-enabled communications chips [19].

3) DeviceNet: DeviceNet is a low-cost communication protocol for the automation industry. It is an application-layer protocol that adapts the technology from the Common Industrial Protocol (CIP) [20] and is built on top of the CAN technologies to support a variety of field devices. DeviceNet has not only improved the direct communication between devices, but also provides a very important device-level positioning functionality. The transmission rate of DeviceNet ranges from 125 Kbps to 500 Kbps, and the maximum number of nodes in a network is 64. DeviceNet adopts a producer/customer communication model [21], and information is multicast by each data producer. Devices running DeviceNet can be freely connected or disconnected in the network without affecting other devices. As a result, wiring and installation costs of devices in the DeviceNet network is lower.

4) LonWorks: The LonWorks (local operating network) was launched by the US Echelon Corporation. It was designed specifically to support communications of devices in the control systems over media such as twisted pair, fiber optics, coaxial cable, and Radio Frequency (RF). The LonWorks adopts the full seven-layer architecture of the OSI model. The design of LonWorks uses the object-oriented design methods. The transmission rate of LonWorks ranges from 300 bps to 1.5 Mbps, and the direct communication distance is up to 2700m with 78Kbps, which is known as the universal control network. Lonworks technology uses the LonTalk protocol, which can be encapsulated into Neuron (neurons) chips. The neuron chip implementations of LonWorks are widely used in applications such as building automation, home automation, security systems, transportation, industrial process control and other industries [22].

5) Profibus: PROFIBUS is a fieldbus standard for process filed communications. First promoted in German, PROFIBUS became a standard and is then used by many companies such as Siemens. Several variations of PROFIBUS has been implemented, including *PROFITBUS FMS*, *PROFIBUS DP*, and *PROFIBUS PA*. Field bus Message Specification (FMS) was first specified to support demanding communication tasks. FMS has been applied to textiles, building automation, programmable controllers, and low-voltage switch industrials, etc. Decentralised Peripherals (DP) was then specified for high-speed data transfer between the decentralized peripherals for processing automation. Process Automation (PA) is process automation, and is subject to IEC1158-2 standard. PROFIBUS supports master-slave model, pure master model, multi-master multi-slave hybrid systems and other types of control models. PROFIBUS transmission rate ranges from 9.6Kbps to 12Mbps, and the maximum transmission distance 1200m with 9.6Kbps data rate. When the distance is 200 meters, the data rate remains as high as 12Mbps. The repeaters can be used to extend to communication distances up to 10km over the twisted pair or cable. As shown in Fig. 6, the PROFIBUS protocol implements three layers of the OSI model. In the application layer, various services have been defined, including DPV0 for data exchange and diagnosis, DPV1 for alarm handling, and DPV2 for broadcast.



OSI–Layer	PROFIBUS		
Application	DPV0	DPV1	DPV2
Presentation	– –		
Session			
Transport			
Network			
Data link	FDL		
Physical	EIA–485	Optical	MBP

Fig. 6. Comparison between the OSI model and the PROFIBUS protocol.

6) Highway Addressable Remote Transducer (HART): HART is an early implementation of the fieldbus protocol and is made an open protocol after the development by the Rosemount company. It supports the legacy analog wiring and currently is one of the most popular industrial communication protocols. HART operates in two different modes: the analog/digital mode and the multidrop mode. In point-to-point analog/digital mode, HART features digital signal communication in the existing analog signals, which brings the analog system to the digital system and makes it a good transitional protocol. In multidrop mode, it is possible to have more than one instruments on one signal cable. Each instrument needs to have a unique address. The HART protocol defines the physical layer, data link layer and the application layer to support the response mode and the multicast mode. The frame format is shown in Fig. 7. Since HART uses a mixture of analog and digital signals, it is difficult to develop a common communication chip interface. HART can use the bus power supply to meet the requirements of intrinsically safe applications.

7) Interbus: Phoenix INTERBUS was launched by a German company in February 2000 under the international standard IEC61158. INTERBUS has a simplified model of the OSI model with definitions on physical layer, data link layer, and application layer. INTERBUS has strong reliability guarantee and incurs lower cost in maintenance. The protocol strictly ensures the synchronization of the data transmission to achieve the real-time performance. INTERBUS is widely applied to in automobiles, tobacco, warehousing, paper production, packaging, food and other industries,

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

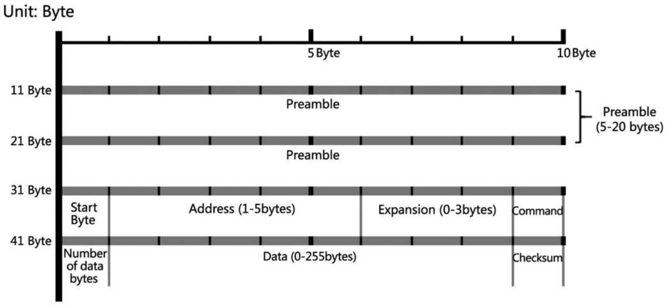


Fig. 7. The frame format specified in the HART protocol.

TABLE I
COMPARISONS OF INDUSTRIAL FILEDBUS TECHNOLOGIES

Field Bus	Bus Power	Data Rate	Max Device	Synchronization
Foundation Fieldbus H1	Yes	31.25 Kbps	240	Yes
Foundation Fieldbus HSE	No	2.5 Mbps	Almost Unlimited	Yes
CAN	No	40 Mbps	127	Yes
DeviceNet	Yes	500 Kbps	64	No
LonWorks	No	1.5 Mbps	32,000	No
PROFIBUS DP	No	12 Mbps	126	Yes
PROFIBUS PA	Yes	31.25 kbps	126	No
HART	No	1.2 Kbps	126	No
CC-Link	No	10 Mbps	64	No
INTERBUS	No	2Mbps	511	No

and has become an international leader in the fieldbus protocols.

8) Control and Communication Link (CC-Link): CC-Link was developed in 1996 by Mitsubishi Electric Inc. After that CC-Link has enjoyed a rapid growth and gained a large share in Asia. CC-Link is specified to be an open network protocol, so that different automation equipment manufacturers can incorporate CC-Link compatibility into their products. And as a result, CC-Link enables devices from numerous manufacturers to communicate, and is widely used in manufacturing and production industries. In CC-Link, the data can be transferred at 10 Mbps, which not only solves the complex problem of industrial field wiring, but also has excellent anti-noise performance and compatibility.

Different fieldbus protocols have different sets of features and performance. Table I summarizes the comparisons of the popular fieldbus protocols.

9) WirelessHART: Compared to the traditional wired systems, the wireless counterparts have the potential to save costs and make deployment and maintenance easier [23]–[26]. To achieve the benefits of wireless access to field devices, the HART Communication Foundation developed a wireless interface for the HART standard, referred to as the WirelessHART. The WirelessHART was defined in Version 7 of the HART protocol released in September 2007, as an open standard for process measurement and control applications which offered a wireless interface to field devices [27].

Before WirelessHART, several wireless communication standards on consumer industry and manufacturing automation, such as ZigBee [28] and Bluetooth [29], have been released. However, these protocols cannot meet the robustness and security requirements of critical industrial control applications. For example, neither ZigBee nor Bluetooth provides a guarantee on end-to-end wireless communication delay, especially in harsh industrial environments with severe wireless interferences. ZigBee has no built-in channel hopping capability [30] and Bluetooth assumes quasi-static star network, which make them not stable and scalable in process control systems. WirelessHART is specifically designed to tackle these problems in industrial systems that require real-time data communication between sensor and actuator devices [31]. WirelessHART adopts the IEEE 802.15.4-2006 [32] as its physical layer. In the MAC layer, WirelessHART defines its own time-synchronized MAC, which enables strict 10ms time slot, network wide time synchronization, channel hopping, and channel blacklisting [31]. In the network layer, WirelessHART supports self-organizing and self-healing mesh networking techniques, which guarantee the network performance.

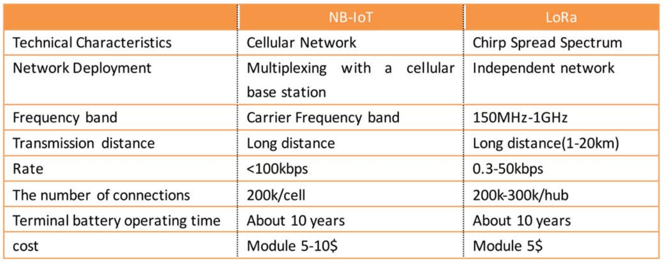
A WirelessHART network consists of field devices, gateways, and a network manager. Field devices can be sensors or actuators in industrial production systems. The gateway is responsible to connect the WirelessHART network to the plant automation system. The network manager is the central of the network and provides the scheduling and routing for the entire network. After the scheduling is performed, the network manager then distributes the schedules among the filed devices by providing the slots for which each device is able to transmit or receive [33].

10) ISA100.11a: Parallel to the development of WirelessHART, the International Society of Automation (ISA) started a family of standards on wireless communications for industrial networked systems at the end of 2008. The first standard ratified was ISA100.11a [34]. The goal of the ISA100.11a is to provide secure and reliable wireless communication for fixed, portable and mobile devices for non-critical industrial monitoring and control applications [35].

ISA100.11a defines the protocol stack, system management and security functions over low-power, low-rate IEEE 802.15.4 wireless networks. ISA100.11a specifies tools for constructing an interface, but does not specify a protocol application layer or an interface to an existing protocol [36]. The main difference between WirelessHART and ISA100.11a is that ISA100.11a is designed not just for handling the HART commands, but also Fieldbus Foundation, Profibus, and Modbus. In addition, ISA100.11 incorporates five different management functions that support management across the network and across different layers of the network architecture. The five management functions include accounting, configuration, fault, performance and security [35].

11) LoRa & NB-IoT: Recently, the Low Power Wide-Area network (LPWA) [37] starts to gain much attention in the communication community. The emergence of LPWA fills the gap in the existing technologies and lays the foundation for large-scale development of IoT. At present, there are mainly two types of LPWA communication technologies [38]. One is cellular network technologies in the authorized frequency band, such as NB-IoT and 5G. The other is LPWAN in the unlicensed band, and a representative one is LoRa.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.



	NB-IoT	LoRa
Technical Characteristics	Cellular Network	Chirp Spread Spectrum
Network Deployment	Multiplexing with a cellular base station	Independent network
Frequency band	Carrier Frequency band	150MHz-1GHz
Transmission distance	Long distance	Long distance(1-20km)
Rate	<100kbps	0.3-50kbps
The number of connections	200k/cell	200k-300k/hub
Terminal battery operating time	About 10 years	About 10 years
cost	Module 5-10$	Module 5$

Fig. 8. Detailed comparisons between LoRa and NB-IoT.

In August 2013, the Semtech company released a new type of ultra-long distance under 1GHz, low-power data transmission technology chip, which was referred to as LoRa [38]. The LoRa network mainly composes of the terminal, gateway, server and the cloud. The application data has two-way transmissions, and the receiver sensitivity can achieve up to -148dbm. Compared with other advanced sub-GHz chips with the highest receiving sensitivity, the improvement is more than 20db, which ensures the reliability of the network connection.

NB-IoT was proposed in July 2015, and standardized in June 2016. The difference between NB-IoT [39] and LoRa is listed in Fig. 8. NB-IoT is currently focused on the smart city and industrial applications. In the future, NB-IoT will continue to play a key role in the carrier-class network for IoT to cover wider range, enable more simultaneous connections, and lower network costs [39]. LoRa implements fast and flexible deployment in smart city, industry and enterprise applications.

12) 5G: In 2012, the International Telecommunication Union (ITU) decided to develop an International Mobile Telecommunication (IMT) system for 2020 and beyond (IMT-2020), the system has been defined as the fifth generation (5G) mobile network. The 5G has three main characteristics: massive machine-type communications, ultra-reliable, and low-latency communications [40]–[42].

Enabling technologies of 5G communications include massive MIMO, millimeter wave, extreme densification, and offloading. The massive MIMO technology can increase spectral efficiency to support more data in each node. The millimeter wave technology can increase bandwidth, and making better use of WiFi's unlicensed spectrum in the 5-GHz band. The densification and offloading technology can improve the area spectral efficiency. In other words, more active nodes per unit area and frequency [43]. The 5G technology aims to achieve 100 billion connections, 1 ms latency, and 10 Gbps throughput, which will significantly benefit the industrial applications that require extremely low latency. 5G will play an important role in the Industrial Internet.

B. Conversion Layer: Industrial Intelligent Sensing

To achieve industrial automation, advanced sensing technologies need to be applied to industrial systems to allow machines and products to interact with the environment and to automatically complete the production process. Physical sensors, such as motion sensors, ultrasound, cameras, microphones, etc. sense the environment in the form of raw sensor data, and the intelligent sensing layer collects the raw data and infers useful information through smart inference algorithms so that the machines and products achieve self-awareness. In addition, for many commonly used sensors in industry, such as camera, ultrasound and infrared sensors, the sensing abilities are directional, i.e., these sensors sense based on the directional sensing model [44]–[46]. In the following, we discuss identity sensing, health status sensing, location sensing, and environmental sensing.

1) Identity Sensing: The Industrial Internet combines the traditional industries with cutting-edge information and communication technologies. To enable efficient automation in industrial systems, identification is the first important step. By identifying machines, machines can talk to each other, and by identifying products, the traditional products turn into the "smart products", which have universally unique IDs and can interact with each other. As more and more field devices such as machines and even final products are equipped with RFID or intelligent sensors, identifying and connecting them becomes much easier [47].

In the conversion layer, the wireless-enabled smart devices equipped with tags or sensors are now able to automatically sense and communicate among different devices. The communication and sensing technologies significantly improve the capability of the Industrial Internet to sense and identify things in the production process. In some industry sectors, a Universal Unique Identifier (UUID) is assigned to each industrial service or filed device such that they can be easily identified and retrieved.

The identification and tracking technologies involved in the Industrial Internet include RFID, barcode, intelligent sensors, and wireless interfaces, such as Bluetooth Low Energy (BLE) and WiFi. A simple RFID system consists of an RFID reader and an RFID tag. Due to its powerful capability to identify, trace, and track devices in the production field, the RFID system is increasingly being used in a variety of industries, such as logistics, supply chain management, and healthcare monitoring [48]. Currently the research and development on industrial RFID systems mainly focus on the following aspects [48]–[50]: 1) large scale RFID systems with efficient identification, retrieval and cardinality estimation; and 2) technology of managing RFID applications [49], [50]. There is still a plenty of room for the development of the RFID-based applications in the Industrial Internet [51]. To further realize the potential of industrial RFID systems, RFID can be integrated with the latest wireless sensing technologies in developing industrial services and applications. By integrating the data collected from the intelligent sensors with RFID data, more powerful Industrial Internet applications can be developed.

2) Health Status Sensing: Estimating the health status and the Remaining Useful Life (RUL) of critical components and machines plays an important role in industrial prognostics activities. With the advanced sensing technologies using sensors, such as motion sensor, temperature sensor, etc., the states of machines can be directly monitored and the health status can be inferred. In industrial systems, prognostics activity estimates of the RUL of physical systems such as machines and

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

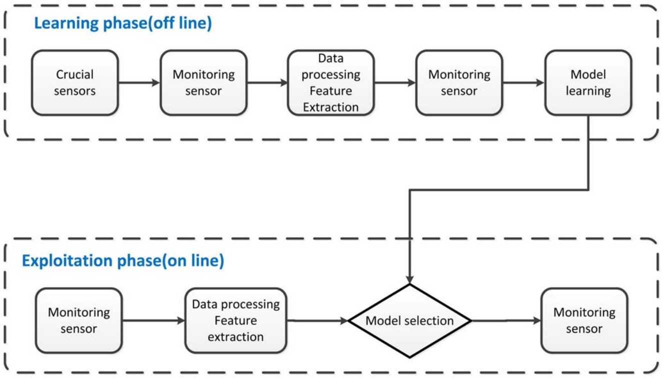


Fig. 9. Remaining useful life (RUL) estimation for critical components in industrial health status sensing.

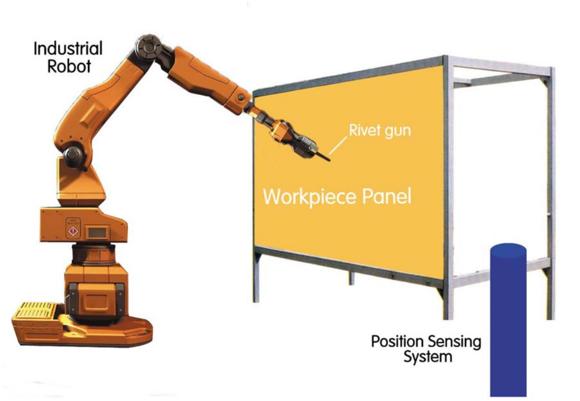


Fig. 10. Illustration of the location sensing in robotic riveting systems.

controlling devices based on their current health status and their future operating environment.

Understanding the health status of physical components is critical in maintaining the machines in good operational conditionals. To avoid non-desired situations due to system faults, one can implement the maintenance strategy based on the Condition Based Maintenance (CBM) [52]. In CBM, the failures are predicted and the RUL before failure are estimated, allowing the system admin to maintain the system before the failure occurs.

Numerous approaches have been studied to estimate the machines' RUL value. These methods can be generally classified into two categories: the *model-based prognostics* [53] and the *data-driven prognostics,BDKBF13*. In model-based prognostics, mathematical or physical models are built to model the degradation phenomenon (crack by fatigue, wear, corrosion, etc.). In data-driven approach, data collected from sensors attached to the physical components are transformed into relevant models of the degradation phenomenon. A lot of research works regarding failure prognostics have been proposed in the literature [52]–[54]. Medjaher *et al.* [55] proposed a data-driven prognostics method, where the RUL of the physical components is estimated based on its critical components. Once the critical component is identified, sensors such as accelerometer, temperature sensors, etc are installed to provide the direct measurement. And the data from the sensors are used to model the degradation's behavior. For this purpose, mixture of Gaussians Hidden Markov Models (MoG-HMMs), represented by Dynamic Bayesian Networks (DBNs), are used as a modeling tool [55]. As shown in Fig. 9, the prognostics process is then done in two stages: a learning stage to train the model based on the sensor input, and an online estimation stage to estimate the RUL of the machine. The intelligent health sensing technology provides the machines the self-awareness on its current status, and allows the users to significantly reduce the maintenance cost.

3) Location Sensing: In Industrial Internet systems, sensing the accurate locations is critical as location is one of the most important context information for industrial robots to complete automation tasks successfully. For example, accurate path tracking of industrial robots aims at accurate location tracking along the predefined paths in the workspace. Location sensing and path tracking has numerous industrial robot applications, such as riveting, welding, material handling, part assembly, etc. [56].

In industrial automation systems, accurate location and path tracking is becoming increasingly demanded [57]–[59]. For example, in aerospace assembly, riveting is the major joining methods and required to be done precisely [52], [56]. Fig. 10 shows the working scenario of a typical robotic riveting system, which consists of an industrial robot, a tooling with a rivet gun, and a location sensing system [53]. The location sensing system is the key component in such automation systems and the positioning accuracy requirement is usually very high (mm level in this case). Accurate location sensing is used to measure the coordinates of the feature points on the tooling to support automatic control during the riveting process. Over the past few years, numerous researches on path-tracking and control strategies for industrial robots have been proposed [15], [48], [60], [61]. Recently, Xi *et al*. [62] developed a novel automatic robotic riveting system. However, there always exists undesired errors in such systems, which in general can be classified into two groups: 1) intrinsic errors due to the manufacturing imperfection, assembly clearances, etc., and 2) extrinsic errors such as external disturbances [56]. In [63], the ultrasound localization sensors are used to measure the path offsets of the robot end-effector. The measured offsets are then provided as the path-correcting control input to the robot controller to improve the performance. Zhao *et al*. [56] recently proposed to correct a preplanned path through an Iterative Learning Control (ILC) method. Instead of seeking the conventional ILC strategy, the proposed calibration-based ILC, is developed to calibrate the robot kinematic parameters along the path during the riveting process. Since accurate location information is required in many other applications such as automatic delivery, navigation, etc., accurate multi-modal localization techniques need to be integrated with future Industrial Internet systems to support more sophisticated industrial applications.

C. Cyber Layer: Cloud Computing

The conversion layer extracts the useful information from the sensor data collected from the connected components,

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

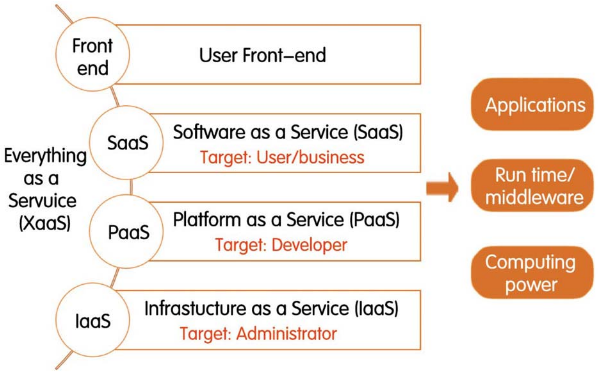


Fig. 11. Architecture of cloud computing from the service perspective.

machines, fleets, and factories, and the information is uploaded to the cyber layer for smart decisioning.

During the past few years, many advanced manufacturing models have been proposed in order to maximize the production efficiency, lower costs, and become environmental friendly for manufacturing enterprise [64]. The proposed manufacturing models include Computer-Integrated Manufacturing (CIM), Manufacturing Grid (MGrid) [15], [52], [61], [65], Networked Manufacturing (NM) [66], Virtual Manufacturing (VM) [60], [67], Agile Manufacturing (AM) [68], and Industrial ProductService System (IPS2) [68], etc. However, these models mainly focus on network and resource sharing. What is largely ignored in these types of models is the centralized operation management of services to turn the manufacturing industries from production-oriented to service-oriented [64].

In the cyber layer, cloud computing is emerging as a key enabler for revolutionizing manufacturing industries. In cloud computing [69], [70], resources are abstracted as services so that the ubiquitous services can be provided to users seamlessly such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), etc. Fig. 11 shows the architecture of cloud computing from the service perspective. The National Institute of Standards and Technology (NIST) defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [71].

Cloud computing is rapidly changing the way industries produce products and do their businesses. Resources are virtualized and can be accessible as services through the Internet. Combining the advanced networking, sensing, and cloud computing technologies, a new manufacturing model, named cloud manufacturing is proposed recently [72]. Cloud manufacturing is considered as a new multidisciplinary domain that reflects both the concept of "integration of distributed resources" and "distribution of integrated resources" [72]. In cloud manufacturing, distributed resources that are required in the industrial productions are encapsulated into cloud services and are managed in the cloud. The cloud users can request services in different stages of production such as product design, manufacturing, testing and management. The cloud manufacturing platform provides intelligent search, recommendation and execution of cloud services. The cloud manufacturing model aims at enhancing the resource utilization and reducing costs and wastes during industrial production, and has the potential to be widely adopted in the cyber layer to further promote the Industrial Internet applications.

D. Cognition Layer: Industrial Big Data

In the cognition layer, the knowledge behind the collected data needs to be extracted. The Big Data Analytics (BDA) fits well in this goal. Many signs have indicated that big data will become a significant field in the Industry Internet era. In the production process, sensors and controllers generate huge amount of data, which contains a lot of information and values that need to be uncovered. As the development of sensing and communication technology, it now becomes easier to obtain real-time data that cover all stages of industrial production. Besides, the technology of embedded systems and cloud computing have also developed rapidly recently, which enables industrial systems to process big data efficiently in a real-time manner [73].

Big data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process within a tolerable elapsed time [74]–[76]. Gartner's big data definition of the 3Vs is still widely being used, in agreement with a consensual definition that "Big Data represents the information assets characterized by such a high *Volume*, *Velocity* and *Variety* to require specific technology and analytical methods for its transformation into value [77]. Additionally, a new "V", i.e., the "Veracity" is added by some organizations later to describe the big data [78], as a result big data is generally considered to have the 4V characters: volume, velocity, variety, and veracity.

In the Industrial Internet, due to its own properties, the industrial big data has another 2Vs characters [79]: (1) *Visibility*: Through big data analysis, invisible information can be uncovered and data can be visualized; (2) *Value*: Information gained by the big data analysis should be valuable. The first 4 Vs indicate the appearance of the big data, and the last 2 Vs indicate the goal and significance that the big data pursues in industrial systems. The value of big data reflects in these aspects in industry [80]:

- The invisible problem can be visible with data mining so that invisible risks in the past can be avoid.
- Big data combining with advanced analytic technologies enables products to achieve intelligent update and provides user with an understanding of full product life cycle.

Different from traditional Internet big data, industrial big data should solve the "3B" problems [81]:

- *Below Surface:* Industrial big data technologies should be able to extract insightful meanings behind features.
- *Broken:* Avoid incoherence and emphasize timeliness.
- *Bad Quality:* Improve data quality and demand low fault rate.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

Traditional big data analytic technologies may not satisfy the demand of industrial big data. Industrial big data requires better knowledge representation [82], deeper domain knowledge, clear definitions of analytical system functions, and the right timing of delivering extracted insights to the right personnel to support wiser decision making [81], [83]. In the following, we discuss the major data processing steps in the industrial big data analytics.

1) Data Acquisition: Data acquisition (DAQ) is the process of converting physical parameters into digital signals that can be manipulated by a computer. In general, Industrial Internet systems use sensors to collect analog information, then Analog-to-Digital Converters (ADCs) are then used to convert analog information to digital data. The volume of industrial data is getting bigger and bigger due to the increasingly high data sampling rate and enlarging scale of sensor deployment.

2) Data Transmission: In the process of data transmission, data may be sniffed by third parties, so it is important to ensure the security and reliability of data transmission. There are many methods in different industry fields. For example, the encryption standards such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Escrowed Encryption Standard (EES) are widely used to solve the problem of communication over an insecure channel. In wireless networks, Kerberos [84] is a computer network authentication protocol that allows nodes to communicate over a non-secure network to prove their identity to one another in a secure manner.

3) Data Storage and Index: In many industrial fields, traditional database technologies have been used to store and index a large amount of data. However, fundamental differences exist compared with the industrial big data. The objectives of traditional database technologies deal with structured data, including different tables and views, while current big data technologies mostly handle unstructured data and aim to gain a variety of useful information from data stored in distributed file systems and distributed databases.

Mainly three massive storage solutions exist before big data storage; Direct Attached Storage (DAS) [85], Network Attached Storage (NAS) [86], and Storage Area Network (SAN) [87]. Distributed technologies rely on such storage solutions, and now distributed file systems are widely used to store big data in industrial environments, which enable industrial systems to gain higher performance, better optimization, and easier to scale.

4) Data Mining: In the era of big data, data processing always involves distributed computing platform, such as Hadoop [88]. Data mining is generally referred to the process of discovering interesting patterns and knowledge from large amounts of data [89]. To extract meaningful information from the industrial big data, data mining technologies play a key role in revealing insights from the data and achieve cognition in the Industrial Internet systems. Data mining is often treated as a synonym for another term "Knowledge Discovery from Data" (KDD) that highlights the goal of the mining process. For such goals, most professionals prefer to use Machine Learning techniques for modeling and prediction, data aggregation and clustering, and knowledge discovery. Machine Learning, as part of Data Mining, provides methods to treat and extract information from data automatically, where human operators and experts are not able to deal with because of the level of complexity or the volume to be treated per time unit [90].

E. Configuration Layer: Smart Control

To provide feedbacks to the physical components and enable smart control, the configuration layer closes the loop of the data flow in Industrial Internet systems. For example, smart control strategies are the key enablers for efficient unmanned vehicle navigations [91]. To monitor and control industrial machinery and processes, industrial control systems play an important role in the industrial production [92]. In the Industrial Internet, in which intelligent production systems are being developed and deployed to support more complex control operations [48], distributed rather than local control is preferred. Moreover, the new type of industrial control must be intelligent and resilient so that it can maintain acceptable level of operation or service within a dynamic and unpredictable environment where there are undesirable incidents, including unexpected and malicious attacks or disturbance. The goal of smart control in modern industrial systems therefore is to use a distributed, collaborative capability to sense, make sense of, and affect the world and to achieve the goals of the specific application [49].

The controllability over the Industrial Internet relies on the control over a field network, the Internal, software applications and networking protocols, which are involved with timeliness, reliability, and Quality of Service (QoS) [50]. An Industrial Control System (ICS) is one electronic device or a set of electronic devices to monitor, manage, control and regulate the behavior of other device or system, including Supervisory Control And Data Acquisition (SCADA) system [93], Distributed Control System (DCS) [94], Programmable Logic Controllers (PLC) [95], etc. In the following, we discuss the architecture of an ICS [12].

1) DCS Architecture: DCS takes centralized supervisory loops as an intermediate layer in a group of distributed controllers who share the same logic of controlling the process. DCS can modularize the process in order to reduce failures of single point within the functional units. As shown in Fig. 12, the DCS architecture has 4 layers, enterprise layer, operation layer, control layer and field layer [96]. The DCS server, which is connected to both operation and control network, is responsible for downloading the application to different PLCs. When the downloading process is completed, the controllers receive process variable values from the field devices through fieldbus network and then execute the embedded control logic. As for the distributed control case, the controllers interact with each other to operate a distributed logic execution. During the execution of control application in the controllers, the DCS server requests data from the distributed filed controllers and devices, which are then graphically showed to the system operators.

2) SCADA Architecture: The key element of a SCADA system is the control room. SCADA servers are connected to SCADA clients for displaying the process events from acquired data from the telemetry outstations. SCADA servers

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

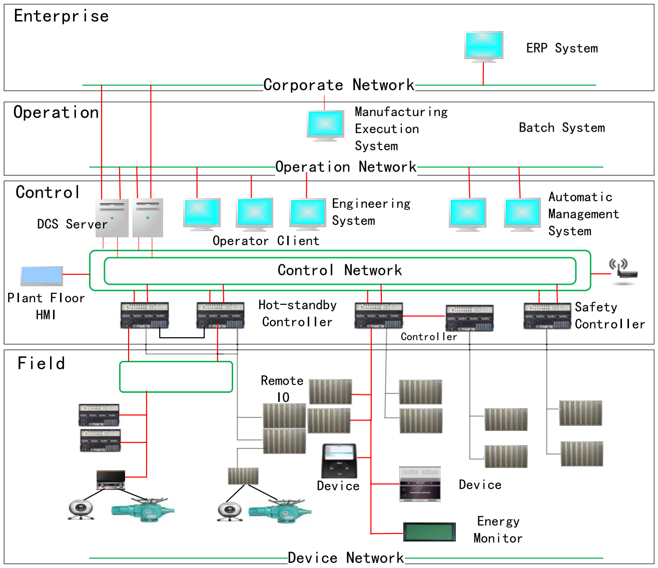


Fig. 12. The overview of the DCS architecture.

keep a list of tags to all the devices connected to the control and acquisition network. In telemetry implementations, SCADA systems are ensured through different kinds of connections, wired connections, wireless or radio connections and satellite connections, as shown in Fig. 13. While in the remote sites, a LAN is needed for Remote Terminal Units (RTUs) to connect to filed devices. A SCADA server provides the ability to SCADA client to perform control actions in case of untreated alarms. The Data Historian is responsible for storing all the information gathered from the field for data analytics purposes.

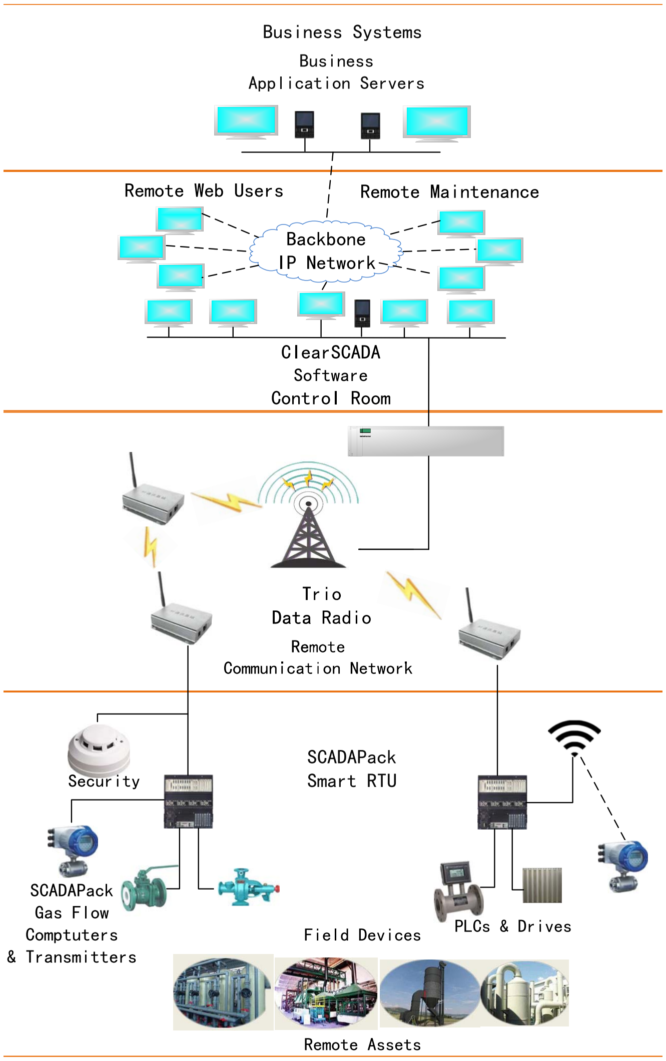


Fig. 13. The overview of the SCADA architecture.

F. All Layers: Security

The security guarantee is critical in implementing all layers of Industrial Internet systems. Nowadays, the security of industrial systems often relies on the proprietary communication protocols, isolated system and physical security [49]. Traditional security methods mostly rely on hardware, and do not have a complete solution for industrial systems. Therefore, the characteristics of traditional security systems may not suitable to the Industry Internet.

In the era of the Industrial Internet, industrial systems are connected and distributed. They are not isolated, on the contrary, the systems are open and data is frequently exchanged among systems. For example, the industrial systems are deeply integrated with enterprise systems. Once the system has evolved over their lifetimes, they can transit their data to another industrial system, or converging with other Industrial Internet systems [97].

With the above characteristics, compared to traditional industrial systems, the Industrial Internet is more vulnerable to malicious attacks. Therefore, how to ensure the security of the Industrial Internet is a key issue throughout their lifecycle. Security of the Industrial Internet cannot simply be functional components, instead it should be approached as a process.

To address the security concerns, the design of security module of Industrial Internet systems must take into account the terminal equipments, the communication system, the management of both the terminal and the communication mechanisms, and data processing and storage. As shown in Fig. 14, the security components of Industrial Internet systems are usually separated into four parts [16].

1) Industrial Terminal Security: Terminal, including but not limited to computers, mobile phones, servers, storage devices, production equipment, and embedded devices, is an indispensability part of the Industrial Internet. Therefore, the terminal security is vital to the Industrial Internet and directly affects their performance of operation.

Many factors affect the terminal security, including application sandboxing, endpoint identity, access control, peripheral devices management, etc [49]. In this section we provide a summary on these terminal security issues.

- *Application sandboxing:* Malware is one of the most significant security threats to automation systems. To prevent malware compromise and damage the system, application sandboxing [98] has emerged as one effective approach.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

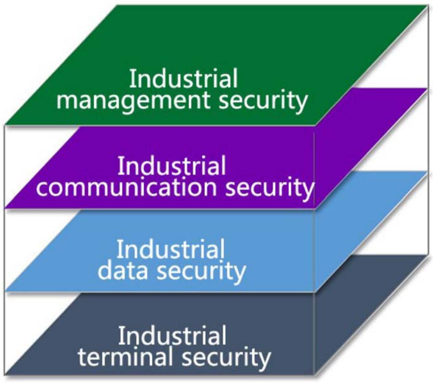

Industrial management security
Industrial communication security
Industrial data security
Industrial terminal security

Fig. 14. Security components of the Industrial Internet.

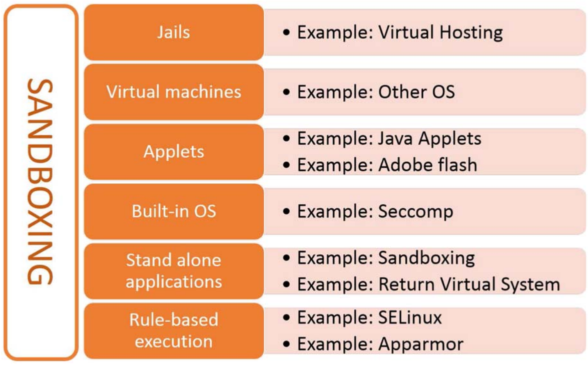


Fig. 15. Categories of Sandboxing techniques.

Application sandboxing is a current mainstream technique to test untrusted or untested programs, and can be run on various applications or operate systems. Malware detection is supervised, and the access that the program has is limited using sandboxing. If the program is detected to be malware or the program cannot run normally, the application sandboxing will report the errors, thus, avoiding the program to damage the system [99]. As shown in Fig. 15, the sandboxing can be categorized into six different categories. These 6 parts are jails, virtual machines, applets, built-in OS, standalone applications, and rule-based execution [98], [99].

- *Terminal identity:* Terminal identity represents the process of differentiating equipment to be either internal or external devices. In order to get managed and tracked easily, every terminal must have a unique identity in the Industrial Internet. Nowadays, the traditional identity, such as IP address, International Mobile Equipment Identity (IMEI) or host names are not secure and can be changed easily. So the ideal and feasible identity is hardware-embedded since it cannot be altered easily. Credentials, such as cryptographic keys, are used as one potential ideal identity in this system, as they cannot be changed easily [49].
- *Access control:* In industrial systems, access control [61] represents the process of managing the access permissions of user, peripherals device, or program when an object (such as an user or a program) request to access someplace. During access control, the system makes a decision to approve or refuse the access request according to what the object is authorized to access, it can ensure that resources not from unauthorized object access and resources can be protected against misuse [61]. In the process of access control, the security management system will record the unauthorized access attempts for analysis [49]. For the security of whole system, principle of minimum privilege should be followed. In other words, users should only possess minimum operation authorities that they have to accomplish their responsibilities, and the system should not endow users [61], [100]. In general, access control can be categorized into three main parts [100], [101] as shown in Fig. 16. The discretionary access control model (DAC), the mandatory access control model (MAC), and the role-based access control model (RBAC) [100]. DAC allows legitimate users to access regulated objects through the user or group of users, and some users are free to grant access to other users [102]. In order to achieve this function, the system should identify the user identity, and then based on the access control list permissions to control the user to use the object resources. Usually, DAC implementation mechanism includes access control matrix, access control list and access control capability lists (ACCLs). In MAC, each user and file is given a certain security class, and the user cannot change the security class of any object, only the system can determine whether the user can access the file. So the MAC is more stringent than the DAC access control strategy [103]. The security categories of the MAC generally include the top secret (TS), the secret (S), the confidential (C), the restricted (R) and the unrestricted (U), and the security level is $T > S > C > R > U$. RBAC [104] assigns access privileges to explicit roles. Users can gain the access authority possessed by the role through playing different roles, and confirm access control permissions in the branches through individual user roles. In practice, the emergence of RBAC greatly simplifies rights management over DAC and MAC, and it directly supports three security principles, namely, the minimum authority privilege, the responsibility separation principle and the data abstraction principle.

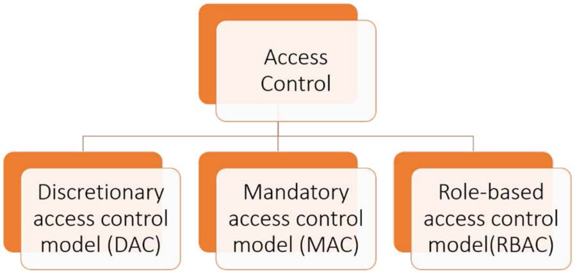

Access Control
Discretionary access control model (DAC)
Mandatory access control model (MAC)
Role-based access control model(RBAC)

Fig. 16. Main components of access control.

2) Industrial Data Security: Data security aims to protect data from misuse from unauthorized users. In traditional industrial systems, the system core is the industrial hardware,

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

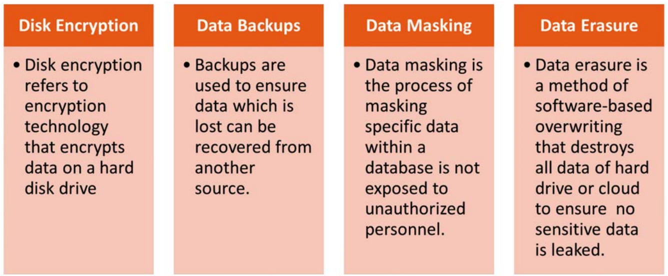

Disk Encryption
• Disk encryption refers to encryption technology that encrypts data on a hard disk drive
Data Backups
• Backups are used to ensure data which is lost can be recovered from another source.
Data Masking
• Data masking is the process of masking specific data within a database is not exposed to unauthorized personnel.
Data Erasure
• Data erasure is a method of software-based overwriting that destroys all data of hard drive or cloud to ensure no sensitive data is leaked.

Fig. 17. Main components of data security.

including manufacturing equipment, computers and servers. In the era of the Industrial Internet, however, management of the rising amount of industrial big data is becoming the center of the system. Data of the Industrial Internet can help improve the efficiency of production, produce on-demand, and automated diagnosis [61], [105]. Due to the importance of data protection, many technologies have been proposed as shown in Fig. 17. For example, disk encryption technology secures data on hard disk drives, data backup technology recovers lost data from backup sources, data masking prevents data from exposing to unauthorized personnel, and data erasure avoids data leaking by destroying all sensitive data in hard drives and clouds through a method of software-based overwriting.

3) Industrial Communication Security: Communication security addresses the threats during data communication and aims to prevent unauthorized parties from accessing the communication channel in an intelligible form while the data is being transferred.

The Industrial Internet requires a combination of technologies to provide an efficient communication protection [106], [107]. Traditional communication protection technologies mostly focus on the widespread communication protocols, such as TCP/IP suite and Ethernet [49]. The TCP/IP suite protocol is one of the most widespread protocols for reliable data communication in the Internet [108], [109]. Ethernet also is used for local area network and metropolitan area network [110]. In the Industrial Internet, the traditional security protocols can be integrated, however the following additional security concerns should also be addressed.

- *Communication authorization:* Before two parties communicate the information, the first step is communication authorization. Authentication can recognize who issued the information and can confirm the identity of the person. The typical types of communication authorization is *static authorization*, *quasi-static authorization* and *dynamic authorization*. In static authorization, once authentication matches system's authorization rule, the authorized party could stay in the trusted zone until he/she logs off. Quasi-static authorization is similar to static authorization except the lease mechanism. Once the lease expires, the user should be asked to get authorized again. Dynamic authorization checks the authorized party frequently due to changed dynamic authorization information [111], [112].

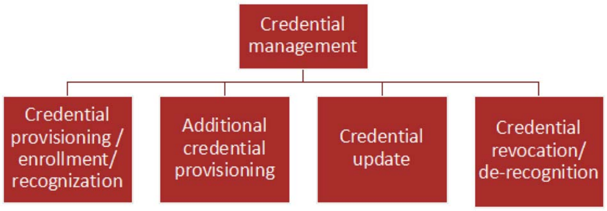

Credential management
Credential provisioning / enrollment/ recognization
Additional credential provisioning
Credential update
Credential revocation/ de-recognition

Fig. 18. The key elements of credential management.

- *Data Encryption:* In industrial security protection, encryption plays a key role and encodes the information in such a way that only authorized user can read it in a correct way [112]. In Industrial Internet systems, data exchange between terminals should be encrypted in order to keep confidentiality from unauthorized invader. Typical encryption schemes are symmetric key encryption and asymmetric key (public key) encryption. With symmetric key, both communication parties have agreed on the same encryption and decryption keys before they can achieve secure communication [113]. In public key encryption scheme, the encryption key is public while only the party who obtained decryption keys enable read messages in correct way [114]. Both schemes have been widely used in current industrial systems.

4) Industrial Management Security: Besides terminal security, data security and communication security, management security is also another important aspect of security protection in Industrial Internet systems [49]. In industrial management security, the following issues need to be addressed:

- *Credential management:* Credentials represent the qualification of users. Credential management is critical to the success of the system security [115]. The area of the credential management consists of credential provisioning, credential enrollment, credential recognition, additional credential generation (particularly for temporary credentials), credential update and credential revocation or de-recognition, as listed in Fig. 18.
- *Remote update:* In Industrial Internet systems, terminals are deployed in different physical locations. In order to maintain consistency, each terminal must securely, automatically, and remotely update software via a security agent [49].
- *Management and monitoring resiliency:* As the industrial system grows big, manual management of industrial systems becomes more and more difficult [116]. In Industrial Internet systems, the automation requires monitoring system's communication network at any time in order to prevent user's misuse and detect invaders. Whenever the system is under security threats, the monitoring system should alert the system and provide immediate responses [49], [117].

V. Applications of Industrial Internet Systems

As the rise of the Industrial Internet, different applications related to the industrial production process becomes more and more intelligent enabled by the advanced information technologies. The advent of the Industrial Internet also brings

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

industrial control systems online to form large end-to-end business and analytics solutions. These end-to-end systems are referred to Industrial Internet Systems (IISs), which cover the area of energy, healthcare, manufacturing, public sector, transportation and related industrial systems.

A. Energy

Several challenges exist in current energy industry. On the one hand, the world is facing many energy challenges due to factors such as increasing urban production, low energy efficiency, increasing population, etc. These challenges lead to more energy consumptions [53]. On the other hand, increasing ecological awareness, rising energy prices, and changing consumer behaviors are driving more efforts on green products, which are manufactured consuming as little energy as possible [52], [54], [118], [119]. The lack of understanding of the energy consumption behavior is the fundamental reason of the challenge in improving factory energy efficiency.

The technologies of the Industrial Internet is gradually transforming the traditional energy industries. In order to improve energy efficiency, significant efforts have to be made to obtain real-time monitoring data through sensor deployment so that the system administrators clearly understands the energy consumption of the factory [120], [121]. Industrial energy system is an indispensability part of the rising Industrial Internet systems. Compared with traditional energy systems, the new energy system transformed by the Industrial Internet has integrated many advanced information technologies to improve the efficiency of energy systems [53]. Such new energy systems not only save the cost, they also help improve the environment protection due to high utilization of energy [53].

Fig. 19 shows the energy management system in smart factories enabled by the Industrial Internet. Four stages needs to be followed in the production process [54]. The first stage requires the understanding of the details of the production processes and current energy management practices. The second stage collects the real-time sensor data through the ubiquitous sensing capability enabled by the industrial sensing and wireless communication technologies [122], [123]. After collecting the sensor data, the third stage processes the data and integrates them into the energy management systems such as energy decision support system to support decision makers detect the waste and come up with better energy saving strategies. Finally, the last stage integrates the energy data in production management practices to improve the energy efficiency. Compared with traditional energy systems, the energy system in the Industrial Internet has the following characteristics [48], [124]:

1) Advanced Control: Traditional energy systems usually require large amount of people to manage and control the system, while the Industrial Internet energy system significantly reduces the labor required [124]. The use of advanced technologies in connectivity and interoperability effectively improves the system operability [60], [124]. Advanced information and communication technologies such as software-defined machines, smart sensing, and big data analytics are applied to the Industrial Internet energy system. These new technologies are constantly improving the systems operational efficiencies [48], [60].

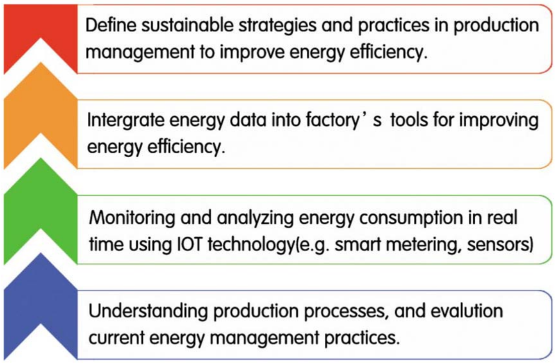

Define sustainable strategies and practices in production management to improve energy efficiency.
Intergrate energy data into factory' s tools for improving energy efficiency.
Monitoring and analyzing energy consumption in real time using IOT technology(e.g. smart metering, sensors)
Understanding production processes, and evalution current energy management practices.

Fig. 19. Energy management in the Industrial Internet [54].

2) Remote Monitoring: Traditional energy systems require huge amount of people in order to maintain the system working normally. Unfortunately, there are more than 337 million accidents happen each year according to the International Labor Organization (ILO) since many of them are exposed to hazard environment. In order to provide operators a safety working environment, the energy production systems should pay more attention to remote operations. The Industrial Internet energy system provides visualized operation to operators, and provides the real-time monitoring on the production environments through sensing and communication technologies. The analytic results will help operators optimize their operations. The remote monitoring techniques can improve product efficiency of the energy industries, and avoid the unnecessary hazard to employees [60].

3) Predictive Maintenance Technique: In energy production industry, equipments are exposed in water or air moisture for a long time. Maintaining the good conditions of equipments become a big challenge in energy industry. The Industrial Internet energy system utilizes big data and data analytics to make predictive analytics information, which can help system avoid unexpected shutdown and catastrophic failure, and minimize the unplanned downtime [60].

4) Improved Safety and Efficiency: Risk management strategies and system control security principles for Industrial Internet systems have unique requirements regarding the availability and security policies [125]. From the constant monitoring and real-time data analysis, the Industrial Internet energy system is able to detect problems before these problems occur and energy consumptions of different components [60]. Therefore, the system is able to prevent serious and dangerous incidents, avoid unnecessary losses, and improve the overall energy efficiency [52], [60].

B. Healthcare

Healthcare is another area that the technologies of the Industrial Internet will benefit. Through monitoring, modeling and controlling medical equipment remotely, the Industrial Internet drives down costs and provides home-bound patients with targeted care. Hospitals are already benefited from inteligent equipment that reduces patient's waiting time and

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

improves equipment efficiency. The Industrial Internet will provide a safer and more efficient health care environment with lower prices [15]. Several application domains of healthcare can be benefited as summarized below.

1) Patient-Centered Medical Home Care: The Patient-Centred Medical Home (PCMH) is a model of primary care that has become widely regarded as a potential solution to the problems of high medical cost, chronic disease management, patient satisfaction, accessibility, and over use of emergency rooms [65], [126]. The wearable devices can reduce the nurses' time in repetitive work, such as measurements for blood pressure and the time saved would be enormous and that's just the beginning of how the Industrial Internet of Things (IIoT) promises to change healthcare. Advanced technology is making it possible to deliver healthcare in new ways. By using IIoT devices to collect patient's information, upload it to the cloud and at the other end, doctor can make a timely decision with appropriate treatment [127]. One example is an IIoT home diagnostics concept called Flow Health Hub from Cambridge Consultants, a bedside unit that can take samples and quickly give measurements for cholesterol, diabetes, and blood pressure. It can automatically alert the patient's doctor if medical help is required [127].

2) Improved Equipment Efficiency: The rapid development of IIoT technology makes it possible for connecting medical equipment together and provide doctors more useful information [48]. It enables a concept called the Medical Device Plug-and-Play (MDPnP) [128]. An MDPnP system is a typical cyber physical system. On the one hand, it involves cyber world discrete computer logic of various embedded medical devices. On the other hand, it involves physical world patient-in-the-loop, which is a continuous complex biochemical system [120]. The collected real-time data from the CPS can be transformed to valuable information. If allocated with the proper work, medical equipment won't be idle and patient's waiting time will be reduced. Data from the sensors in the CPS can be transformed to information which will help doctors make right decisions for their patients.

3) Doctor Recommendation: Today, medical appointment platforms have been adopted in many hospitals. However, lots of patients are bothered by how to choose a right doctor online. Without professional knowledge and relevant experience, people have no idea about who are the appropriate doctors for their own health problems [129]. A doctor recommendation system, where patient can get the help from appropriate doctor, will solve the above problems. The recommendation systems are an active research topic in the data mining and machine learning fields. Learning from the sensor data and the previous recommendation system, the doctor recommendation system will transform the sensor data collected from patients, doctor appointment platforms, and patients' comments to the information that can be presented to patients for efficient doctor recommendation [130].

C. Manufacturing and Smart Factory

With the Industrial Internet technologies, smart sensors monitor the production environment and send the information about the status of the components, machines, fleets, and the factories regarding the production processes, surrounding environment, and maintenance schedules, etc. to the cyber space. The shortage of resources, increasing ecological sensitive, the consumer behaviors toward the products, etc. drive the decision makers to put green manufacturing and energy-efficient production processes to the first place. Fig. 20 shows the relationships between customers and smart factories in Industry Internet systems, and Fig. 21 shows the architecture of smart factories using the Industry Internet.

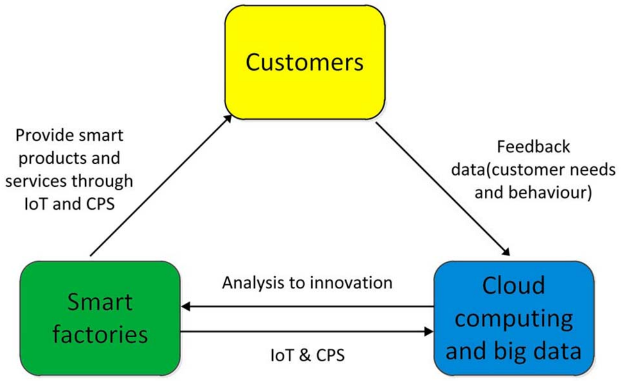

Customers
Provide smart products and services through IoT and CPS
Feedback data(customer needs and behaviour)
Smart factories
Analysis to innovation
IoT & CPS
Cloud computing and big data

Fig. 20. Customized productions in smart factories.

In smart factories, the smart devices include the controlling devices that are networked with the machines and people using the Industrial Internet technologies, such as the field devices, mobile devices, and other operating devices, etc. The goal of smart factories is to provide sustainable smart products and services to smart customers according to their behaviors, customized orders and feedback. Based on smart grid and smart suppliers, smart factories get organized their manufacturing processes, software and hardware with the help of cloud computing and big data. The key elements of smart manufacturing can be summarized as follows: smart machines, smart manufacturing processes, smart engineering, smart logistics, big data and cloud computing, smart suppliers, and smart grids [54].

1) Smart Machines: With the sensing, communication, and processing capabilities, smart machines can be intelligently networked and combined as an autonomous system. The self-awareness enables them to detect potential runtime risks and inform corresponding parties about the risk before error occurs. The smart machines are also connected with other filed devices and humans. The remote control capability also allows smart machines to operate or be repaired remotely. As a result, the smart machines achieve self-awareness, self-operability, and self-maintenance [131].

2) Smart Manufacturing Processes: The Industrial Internet provides significant potential value of manufacturers and other industrial organizations. The Industrial Internet affects the traditional manufacturing industry mainly through integrating with two streams of technologies: CPS and IIoT, with the goal of finally realizing the smart manufacturing, whose ultimate goal is to link the virtual world to the physical world in the manufacturing. The smart manufacturing process has

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

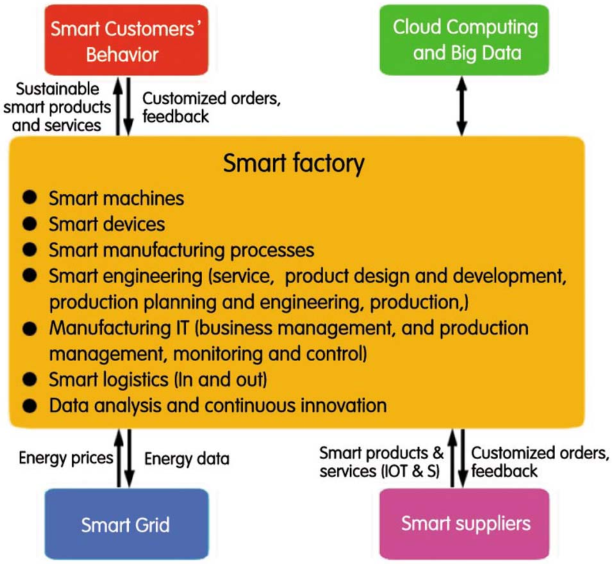

Smart Customers' Behavior
Cloud Computing and Big Data
Sustainable smart products and services
Customized orders, feedback
Smart factory
● Smart machines
● Smart devices
● Smart manufacturing processes
● Smart engineering (service, product design and development, production planning and engineering, production,)
● Manufacturing IT (business management, and production management, monitoring and control)
● Smart logistics (In and out)
● Data analysis and continuous innovation
Energy prices
Energy data
Smart products & services (IOT & S)
Customized orders, feedback
Smart Grid
Smart suppliers

Fig. 21. Architecture overview of the smart factories [54].

the characteristics of dynamic, automated, efficient and real-time [132]. The smart manufacturing processes require the production system to satisfy the dynamic requirements of consumers in real-time by utilizing the interconnectivity provided by the IIoT to achieve the personalized customization. A feedback system will also be created during the assembly-time and the consumers' feedback will be dynamically reflected in the manufacturing process through seamlessly integration of machines and customers [133]. The concept of smart manufacturing is based on the integration of both CPS and IIoT concepts [134]. IIoT's target is to inter-connect different types of devices with each other and with company's enterprise systems. Virtual objects and self-organized intelligent entities will become interoperable to form a united system enabled by the IIoT.

3) Smart Engineering: In smart factories, the engineering covers from the product design, product development, product engineering, production, to the final after sales services [54]. To achieve a more efficient engineering process, big data analytics can be used as an efficient mechanism of feedback to optimize the engineering processes and to increase productivity.

4) Manufacturing IT: The manufacturing IT represents the IT infrastructure that is required in smart factories. The manufacturing IT includes the algorithms and softwares that are used by the production system, and also the hardware infrastructure such as the sensors and actuators that provide the smart monitoring and control over the physical machines. It also includes the production management systems that incorporate different technologies and manage all data generated in the whole manufacturing process.

5) Smart Logistics: Intelligent warehousing systems have the properties of cost savings, management efficiency improvement and other advantages, and also can reduce the ultimate cost of current logistics solutions. Logistics industry will achieve more efficiency and level of automation through Industrial Internet technologies including RFID, vision computing, robotics, etc. Industrial sensing technologies will be widely used in the Industrial Internet logistics systems. Self-organized logistics [61] is one example of smart logistics that provides timely response to unexpected situations in the production process, such as materials shortages.

6) Big Data and Cloud Computing: With cloud computing and big data analytics, data processing will become one cloud service and bring profound opportunities for improving the productivity of factories and providing better products in smart factories.

7) Smart Suppliers: The industrial sensing technologies in smart manufacturing not only collect the production data and provide real-time monitoring on the machines through intelligent sensors and smart devices, they also collect the data from supply and consumers to get real-time feedback. The data helps the manufacturers to predict future demands, increase flexibility by selecting the best supplier based on factory needs according to the historical consumption and logistics data.

8) Smart Grid: The smart grid includes the smart infrastructures of smart factory in field of energy supply [54]. Smart grid is essential to react to changes in energy prices, and achieve a better energy saving in the production.

D. Public Sector

In the era of the Industrial Internet, the public sectors face the opportunities to integrate with the advanced information and communication technologies to reduce costs, reduce waste, improve public safety and service qualities for citizens. Citizens can use their mobile devices to request different public services [135]. Through information and communication technologies, the public sector can provide more convenient services to citizens to link the public areas with virtual world to achieve a better management, education and maintenance [136]. The sensor-embedded public facilities enable intelligent public services such as smart traffic management and monitoring, improving public education, public administration, public safety, crime prevention and emergency response [137]. Following we provide a summary on the typical services in the public sector enabled by the Industrial Internet technologies.

1) E-Government: E-government is a new form of public management model and administrative mechanism of public affairs, where the public sectors achieve digitalization to efficiently handle the requests of citizens and government affairs by means of advanced technologies. At the same time artificial intelligence has been utilized to improve the service qualities provided by the government [51]. From the citizens' perspective, the citizens are mainly concerned with how they can rapidly learn about the policies and regulations, understand government services and other information, and to directly express their wills and requests of public services through the Internet [138]. On the other hand, the government mainly concerns about the efficiency in announcement of information, obtaining the feedback from citizens, and administration of the public affairs [138]. This is often regarded as a revolutionary way of collecting, organizing

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

and sharing information on many public issues to increase the interaction, participation and transparency [139]. The service categories of e-government enabled by the Industrial Internet mainly include G2G (Government to Government), G2B (Government to Business), G2C (Government to Citizen), and G2E (Government to Employee).

2) Environmental Services: With the rapid development of advanced sensing technology, different environmental aspects of the city can be monitored in real-time. The biological sensors detect the water and air qualities and sense parameters of other environmental aspects. Environmental pollutions such as phenol, NO3, organic phosphorus salt and red tide, residual toxic pests, and persistent organic pollutants (pops), etc. can be detected efficiently through real-time monitoring, testing, implementation of environmental protection and pollution mechanisms [140].

3) Education Services: The new education services enabled can be divided into three parts, e-Learning applications, interactive learning environment, social and professional online educations [141]. Through advanced technologies, the e-Learning services establish a platform for education in poverty-stricken areas. Education services enable users to use ICT tools to communicate, learn, and access international educational content [141]. E-Learning can be used to improve the effectiveness of education services, improve the utilization efficiency of educational resources, and optimize the allocation of educational resources [142].

4) Public Safety: In public environments, the smart sensing technologies are applied to detect crimes and emergencies. With the passive monitoring capability, public safety events such as large crowd gathering events can be detected in real-time and reported to the corresponding management parties. Video sensor networks [143] are used to collect the visual information of target areas and process it in-network. In applications of intrusion detection, vibration sensor networks are deployed to guarantee the intruder can be detected quickly even following the minimal exposure path [144], [145]. In applications where individual safety parameters need to be collected, wearable sensors are used to locate the users and monitor their health status. Such large-scale monitoring also provides predictive safety warnings and prevents emergency events from happening when public environment becomes unsafe [146].

E. Transportation

Intelligent Transportation System (ITS) refers to integrating applications of communication, control and information processing technologies with the transportation infrastructure and vehicles [147] With the help of the Industrial Internet in which cloud computing and CPS technologies have been well-developed and wildly applied, ITS will become more intelligent and of better help for us. ITS under the Industrial Internet will be able to save time, money, energy, and reduce negative impact on our environment. ITS is based on a set of information handling techniques such as information collecting, information processing, information integration and information dissemination. That information is obtained from different sources such sensors on the vehicles, on the roadways to monitor weather conditions, traffic information, and so on.

The Industrial Internet sensing and communication technologies provide powerful data acquisition functions which provide sufficient traffic data ITS needs. ITS relies on the collection of the real-time traffic-related data, to provide smart scheduling over the road network. The information of traffic participants, such as pedestrians or vehicles, even the road relevant facilities will quickly be gathered to the Industrial Internet [148].

Drivers who want to make certain traveling decisions based on factors like traffic conditions, road maintenance, construction work, and weather conditions, will get the needed and timely help from ITS. Policy makers and road or highway operators will also find ITS helpful to manage the road networks [149]. The Industrial Internet will also help to lower costs and minimize system failures, while supplying a vast number of data for operators, drivers, and facilities that result in huge operational improvements. The transportation system will be able to sense and respond to what is happening in real-time, with operational efficiency and public safety increased, fleet down time reduced [150]. For example, vehicles will be able to sense each other's existence, and know who are around them, which can significantly improve the driving safety. Another example, if one wants to go to some place as fast as possible, ITS will tell you the best route to the destination without being trapped in the traffic. And traffic jams and accidents can be substantially reduced and timely handled. That is how ITS under the Industrial Internet helps to save time, energy, and improve transportation safety.

VI. Challenges

Despite the potential vision of the Industrial Internet, many significant research challenges remain to be addressed before widespread deployment of the Industrial Internet, including the mixed criticality, fault tolerance, scalability, scalable collaboration, functional safety, security challenges, and legacy long-lived industrial systems [151]. In this section we summarize these challenges that need to be addressed to fully realize the potential of the Industrial Internet.

A. Mixed Criticality

In Industrial Internet systems, different components or even separate systems are integrated through ubiquitous network connections, this results in more intelligent control and collaborative production. However it also results in a mixed criticality challenge when different functions with different criticalities are integrated into the same industrial system. To guarantee the reliability and availability in the industrial productions, these functions of different criticalities need to be isolated so the ones with lower criticality will not affect those with higher criticalities. Therefore it is essential to achieve software partitioning on such mixed criticality systems. For example, the authors of [34] pointed out that it is desirable to run real-time applications of different criticalities through

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

temporal partitioning. To enable functions with different criticalities to co-exist in the same system, virtualization is a technology that is gaining increasing popularity in industrial systems [151].

Through virtualization, the hypervisor, or the virtual machine monitor manages all the physical resources such as CPU, RAW, storage, etc., and share the resources among a set of virtual machines. Virtualization allows different operating systems running simultaneously on different virtual machines. As a result, it becomes feasible to efficiently separate resources and achieve isolation within the same system. The ability to achieve system partitioning provides opportunities for industrial systems to become compatible with legacy systems of different criticalities while allowing the systems featured by new industrial Internet of things technologies to run separately. Virtualization technologies have been used extensively to manage resources on the cloud, and have been gaining popularity for embedded real-time systems. The partitioning capability enabled by the virtualization preserves the criticality of different systems while seamlessly integrating them in the same platform through scheduling the execution automatically.

B. Network Latency

In Industrial Internet systems, the distributed sensors, actuators, machines, and other computing devices need to collaborate together to achieve real-time monitoring or complete the production tasks. Ensuring the reliable and low-latency data transfer is important to achieve the reliability and efficiency of industrial systems. As the number of distributed devices increase, the network latency challenge becomes more severe in Industrial Internet systems. Since the Internet Round Trip Time (RTT) ranges from tens of milliseconds to hundreds of milliseconds [152], the latency-sensitive industrial applications require the new distributed networked industrial systems to dynamically deploy computing tasks at different levels from the network edge to the cloud to achieve reliable services.

To reduce the latency in industrial IoT systems, fog computing or edge computing [152] has been proposed in the literature. In fog computing or edge computing, applications or services that have the real-time performance requirements are pushed to the network edge, or the end devices to reduce the latency and response time. The edge computing paradigm extends the cloud computing paradigm and relocates the services that are not suitable to be executed on the cloud to the end devices. The paradigm shift reduces the total network latency and improves the quality of service (QoS). Fog computing has been shown to be suitable for industrial IoT systems that require low and predictable latencies and real-time performance. Another paradigm is the cloud offloading [153] that uploads computation-extensive tasks to the cloud for fast and predictable execution. Suzuki and Inoue [154] proposed to utilize a router instead of a central gateway for applications that require different real-time performances. Latency-sensitive applications are run in local networks utilizing machine-to-machine communications, while non-real-time applications are deployed in the cloud [151].

C. Fault Tolerance

With hundreds or even thousands of nodes coordinating simultaneously in industrial production process, fault tolerance becomes a key issue in the management of Industrial Internet systems. The faults due to the local machine failure, communication unreliability, other software faults in the cloud, or malicious attacks will significantly affect the reliability and availability of the system and degrade the system performance, therefore it is crucial to design a fault-tolerant system and fault recovery mechanisms to adapt to unforeseen failures that may lead to service degradation or unavailability [151].

To improve the system reliability facing various potential faults, many works has been proposed in the literature. For example, Hegazy and Hefeeda [152] proposed a redundancy-based mechanism to achieve reliable operation under failure through distributed redundancy controllers. The redundancy scheme reduces the risk of single-point-of-failure by distributing the computing resources or content to physically separated sub-systems so that even parts of the system are down the redundant servers can maintain the running of services. The performance of industrial systems is sensitive to the connection unreliability due to the real-time requirements. To reduce uncertainty in the data transfer in industrial systems, edge computing [155] which deploys the computing tasks on the end devices efficiently controls and improves the predictability of the network latency. The computation shifting therefore complements cloud computing and minimizes the dependency on the cloud. To handle the hardware faults, the health monitoring mechanisms and remaining useful life predictions [55] can be made to achieve a predictive maintenance and reduces the chance of system failure. Based on the multilayer aggregation architecture, Sun *et al.* [156] designed a trust-based framework for data aggregation with fault tolerance with a goal to reduce the impact of erroneous data and provide measurable trustworthiness for aggregated results.

D. Scalability

As the number of connected components, machines, and factories becomes big, the scalability of Industrial Internet systems rises as a significantly challenge. The scalability issue of Industrial Internet systems comes from three aspects: (1) *Data scalability.* The growing number of sensors in Industrial Internet systems generate large amount of sensing data continuously. And for industrial control applications such as the motion-control application, the cycle-time requirement is usually very high and can reach 100 μs [151]. The high frequency data also places significant challenges to the scalability of the system. (2) *Scalable collaboration.* In traditional industrial systems, the control systems are usually independently engineered and do not scale. Therefore, improving the interoperability becomes a challenge here to enable heterogeneous devices and systems to communicate and collaborate. (3) *Scalable management*. The horizontal and vertical integration of various industrial components and systems places non-trivial management and maintenance challenge to the system administrators. In order to achieve scalability, modern

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

management technologies need to be integrated in the system management process.

To address the data scalability issue, the high frequency data needs to be preprocessed at the end devices before uploading. For example, Aazam and Huh [157] proposed to trim high-frequency data generated from small cycle-time systems before uploading to the cloud. This will reduce the bandwidth requirement and improve the scalability in high-frequency data systems. The collaboration scalability requires to reduce the manual effort in configuration when different systems integrate and collaborative. Different communication protocols have been proposed to achieve auto-configuration in connecting heterogeneous devices, such as Advanced Message Queueing Protocol (AMQP) [158], Message Queue Telemetry Transport (MQTT) [159], and Data Distribution Service (DDS) [160]. Cirani *et al.* [161] proposed a self-configuring architecture for large scale IoT systems by enabling resource discovery and auto-configuration.

E. Functional Safety

The industrial systems usually involve different critical production functionalities. Ensuring the functional safety is essential for the overall production safety. The industrial systems require the integration of safety and control applications such as the emergency shutdown systems [151]. The functional safety standards require to achieve traceability from the design, implementation, verification, and validation. However, it becomes challenging to certify the industrial systems lacking documentations from the development process [151]. It becomes especially challenging to ensure the functional safety when different systems are interconnected in Industrial Internet systems. In the development of the Industrial Internet, standardization is required for the functional safety to provide a reliable and safe industrial environment.

F. Security Challenge

Security guarantee is essential to industrial systems. With distributed sensor nodes, actuators, and machines connected to form the production system, it becomes non-trivial to ensure the authenticity and data confidentiality of the system. The ability for self-configuration and automation also leaves potential vulnerability for attackers to exploit and take control of the system. Besides, the industrial production-related data stored in the clouds also poses challenges to the system designers for data privacy and security protection. Therefore, the Industrial Internet software needs to protect the interconnected devices and the generated data from various malicious attacks. To protect the automation processes continuously, the security updates cannot interfere with the control processes and should be seamlessly integrate with the normal control cycle.

Most existing security techniques are signature based, which maintain the syntactic representation of the attack [162]. It is easy for an attacker to launch an attack with slight modification of this syntactical representation of the signature. One major challenge is how to design a system that represents the attack with a balanced abstraction to cater for similar variations of any particular attack. And most existing solutions use primitive (but fairly effective) static/signature based attack detection mechanisms. No practical system has been implemented that uses semantic analysis to data/protocols to mitigate this problem yet. This gives birth to a challenge to apply techniques from the field of semantic Web to the area of Web application security. Learning based security systems generate a high level of false positives and learning process has to be repeated after every change in the application logic, which is a time-consuming task. Moreover, owing to ubiquitous connections and high performance of the Industrial Internet, there could be more types of vulnerabilities and hence more attacks [163]. Those attacks may become more frequent, harmful and harder to be detected [164].

VII. Conclusion

Recent advances of sensing, networking, cloud computing, and big data technologies have started to revolutionize traditional industries and prosper the idea of the Industrial Internet. Overall, the Industrial Internet allows the interconnection and collaboration among devices and people in the industrial environment, reduces cost, and improves the productivity. In this paper, we have presented a brief history of the Industrial Internet, its architecture, and enabling technologies. This can provide a good foundation for those who are interested to gain insights into the concept of Industrial Internet and the key enablers of this emerging industrial revolution. Moreover, we have presented different application domains of the Industrial Internet, to illustrate how the integration of the Industrial Internet technologies will transform traditional industries such as energy, health care, manufacturing, public section, and transportation. We finally presented the research challenges and open issues to achieve secure, reliable, scalable, safe, and inter-operable industrial systems. These challenges need to be addressed to fully realize the potential of future Industrial Internet systems.

References

[1] P. C. Evans and M. Annunziata, "Industrial Internet: Pushing the boundaries of minds and machines," *Gen. Elect.*, vol. 26, nos. 1–2, pp. 1–23, Nov. 2012.

[2] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, Jan. 2016, pp. 3928–3937.

[3] X. D. Wu, X. Q. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 97–107, Jun. 2014.

[4] M. Armbrust *et al.*, "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California at Berkeley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[5] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[6] J. C. Chen and V. S. Gabriel, "Revolution of 3D printing technology and application of six sigma methodologies to optimize the output quality characteristics," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Taipei, Taiwan, 2016, pp. 904–909.

[7] S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Upper Saddle River, NJ, USA: Pearson Educ., Dec. 2009.

[8] J. J. Wu, Y. G. Tan, and G. F. Ma, "3D printing monitoring platform based on the Internet of Things," in *Proc. 5th Asia Int. Symp. Mechatronics (AISM)*, Guilin, China, 2015, pp. 1–5.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

[9] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," *Strasbourg*, vol. 14, no. 6, pp. 731–736, Jun. 2010.

[10] F.-J. Wu, Y.-F. Kao, and Y.-C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive Mobile Comput.*, vol. 7, no. 4, pp. 397–413, Aug. 2011.

[11] R. H. Rawung and A. G. Putrada, "Cyber physical system: Paper survey," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Bandung, Indonesia, 2014, pp. 273–278.

[12] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *Proc. Int. Conf. Cyber Security Smart Cities Ind. Control Syst. Commun.*, Shanghai, China, 2015, pp. 1–8.

[13] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial Internet of Things," in *Proc. IEEE World Forum Internet Things*, Milan, Italy, Dec. 2015, pp. 795–800.

[14] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [Industry forum]," *IEEE Ind. Electron. Mag.*, vol. 8, no. 2, pp. 56–58, Jun. 2014.

[15] *Industrial Internet Consortium*. Accessed on Feb. 20, 2017. [Online]. Available: http://www.iiconsortium.org/

[16] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.

[17] J.-Q. Li, S.-Q. He, Z. Ming, and S. Cai, "An intelligent wireless sensor networks system with multiple servers communication," *Int. J. Distrib. Sensor Netw.*, vol. 2015, pp. 1–8, Jul. 2015.

[18] I. Verhappen and A. Pereira, *Foundation Fieldbus*. Research Triangle Park, NC, USA: Int. Soc. Autom., Feb. 2012.

[19] G. Cena and A. Valenzano, "An improved CAN fieldbus for industrial applications," *IEEE Trans. Ind. Electron.*, vol. 44, no. 4, pp. 553–564, Aug. 1997.

[20] S. Viktor, D. J. Vangompel, and R. Voss, *The Common Industrial Protocol (CIP) and the Family of CIP Networks*, ODVA, Milwaukee, WI, USA, Feb. 2016.

[21] F.-L. Lian, J. R. Moyne, and D. M. Tilbury, "Performance evaluation of control networks: Ethernet, controlNet, and deviceNet," *IEEE Control Syst.*, vol. 21, no. 1, pp. 66–83, Feb. 2001.

[22] D. G. Gao, A. B. Jiang, F. X. Sheng, and J. J. Xu, "The summary of the LonWorks fieldbus technology," *Comput. Study*, vol. 5, p. 1, May 2006.

[23] D. Chen, M. Nixon, and A. Mok, "Why wirelessHART," in *WirelessHART*. New York, NY, USA: Springer, Mar. 2010, pp. 195–199.

[24] L. Ma, F. Yu, V. C. M. Leung, and T. Randhawa, "A new method to support UMTS/WLAN vertical handover using SCTP," *IEEE Wireless Commun.*, vol. 11, no. 4, pp. 44–51, Aug. 2004.

[25] F. Yu and V. C. M. Leung, "Mobility-based predictive call admission control and bandwidth reservation in wireless cellular networks," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, Apr. 2001, pp. 518–526.

[26] F. Yu and V. Krishnamurthy, "Optimal joint session admission control in integrated WLAN and CDMA cellular networks with vertical handoff," *IEEE Trans. Mobile Comput.*, vol. 6, no. 1, pp. 126–139, Jan. 2007.

[27] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the wirelesshart standard," in *Proc. IEEE Int. Conf. Emerg. Technol. Factory Autom.*, Hamburg, Germany, Sep. 2008, pp. 899–907.

[28] P. Baronti *et al.*, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, no. 7, pp. 1655–1695, May 2007.

[29] C. Bisdikian, "An overview of the Bluetooth wireless technology," *IEEE Commun. Mag.*, vol. 39, no. 12, pp. 86–94, Dec. 2001.

[30] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of wirelessHART and ZigBee for industrial applications," in *Proc. IEEE Int. Workshop Factory Commun. Syst.*, Dresden, Germany, 2008, pp. 85–88.

[31] J. Song *et al.*, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proc. IEEE Real-Time Embedded Technol. Appl. Symp. (RTAS)*, St. Louis, MO, USA, Apr. 2008, pp. 377–386.

[32] *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. Accessed on Feb. 20, 2017. [Online]. Available: http://profsite.um.ac.ir/~hyaghmae/ACN/WSNMAC1.pdf

[33] A. Saifullah, Y. Xu, C. Lu, and Y. Chen, "Real-time scheduling for wirelessHART networks," in *Proc. IEEE Real-Time Syst. Symp. (RTSS)*, San Diego, CA, USA, Dec. 2010, pp. 150–159.

[34] *Wireless Systems for Industrial Automation: Process Control and Related Applications*, ISA Standard 100.11 a-2009, 2009.

[35] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, no. 4, pp. 23–34, Dec. 2011.

[36] M. Nixon and T. R. Rock, "A comparison of wirelessHART and ISA100. 11a," Emerson Process Manag., Whitepaper, pp. 1–36, Sep. 2012.

[37] K. Mikhaylov, J. Petaejaejaervi, and T. Haenninen, "Analysis of capacity and scalability of the LoRA low power wide area network technology," in *Proc. Eur. Wireless Conf.*, Oulu, Finland, May 2016, pp. 1–6.

[38] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation model for LoRa technology," in *Proc. 14th Int. Conf. ITS Telecommun. (ITST)*, Copenhagen, Denmark, Dec. 2015, pp. 55–59.

[39] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops*, Doha, Qatar, Apr. 2016, pp. 1–5.

[40] J.-C. Guey *et al.*, "On 5G radio access architecture and technology [industry perspectives]," *IEEE Wireless Commun.*, vol. 22, no. 5, pp. 2–5, Oct. 2015.

[41] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 90–96, Feb. 2014.

[42] C. Liang, F. R. Yu, and X. Zhang, "Information-centric network function virtualization over 5G mobile wireless networks," *IEEE Netw.*, vol. 29, no. 3, pp. 68–74, May/Jun. 2015.

[43] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[44] H. Ma and Y. Liu, "On coverage problems of directional sensor networks," in *Proc. Int. Conf. Mobile Ad-hoc Sensor Netw.*, Wuhan, China, Dec. 2005, pp. 721–731.

[45] H. Ma, X. Zhang, and A. Ming, "A coverage-enhancing method for 3D directional sensor networks," in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 2791–2795.

[46] H. Ma and Y. Liu, "Some problems of directional sensor networks," *Int. J. Sensor Netw.*, vol. 2, nos. 1–2, pp. 44–52, Apr. 2007.

[47] R. Schmidt *et al.*, "Industry 4.0–potentials for creating smart products: Empirical research results," in *Proc. Int. Conf. Bus. Inf. Syst. Lecture Notes Bus. Inf. Process. (Bis)*, Poznań, Poland, Jun. 2015, pp. 16–27.

[48] P. Robison, M. Sengupta, and D. Rauch, "Intelligent energy industrial systems 4.0," *IT Prof.*, vol. 17, no. 3, pp. 17–24, May/Jun. 2015.

[49] *Industrial Internet Reference Architecture*. Accessed on Aug. 23, 2016. [Online]. Available: http://www.iiconsortium.org/

[50] P. Hu, "A system architecture for software-defined industrial Internet of Things," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband*, Montreal, QC, Canada, Oct. 2015, pp. 1–5.

[51] D. Valle-Cruz and R. Sandoval-Almaz, "E-gov 4.0: A literature review towards the new government," in *Proc. Int. Conf. Digit. Govt. Res.*, Aguascalientes, Mexico, Jun. 2014, pp. 333–334.

[52] M. Garetti and M. Taisch, "Sustainable manufacturing: Trends and research challenges," *Prod. Plan. Control*, vol. 23, nos. 2–3, pp. 83–104, Aug. 2012.

[53] M. Bornschlegl, M. Drechsel, S. Kreitlein, M. Bregulla, and J. Franke, "A new approach to increasing energy efficiency by utilizing cyber-physical energy systems," in *Proc. Intell. Solutions Embedded Syst.*, Pilsen, Czech Republic, Sep. 2013, pp. 1–6.

[54] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. Ind. Eng. Eng. Manag.*, Bandar Sunway, Malaysia, Dec. 2014, pp. 697–701.

[55] K. Medjaher, D. A. Tobon-Mejia, and N. Zerhouni, "Remaining useful life estimation of critical components with application to bearings," *IEEE Trans. Rel.*, vol. 61, no. 2, pp. 292–302, Jun. 2012.

[56] Y. M. Zhao, Y. Lin, F. F. Xi, and S. Guo, "Calibration-based iterative learning control for path tracking of industrial robots," *IEEE Trans. Ind. Electron.*, vol. 62, no. 5, pp. 2921–2929, May 2015.

[57] J.-Q. Li *et al.*, "Accurate RFID localization algorithm with particle swarm optimization based on reference tags," *J. Intell. Fuzzy Syst.*, vol. 31, no. 5, pp. 2697–2706, Oct. 2016.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

[58] C. Luo *et al.*, "Accuracy-aware wireless indoor localization: Feasibility and applications," *J. Netw. Comput. Appl.*, vol. 62, pp. 128–136, Feb. 2016.

[59] C. Luo *et al.*, "Pallas: Self-bootstrapping fine-grained passive indoor localization using WiFi monitors," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 466–481, Feb. 2017.

[60] *Productivity and the Industrial Internet*. Accessed on Feb. 20, 2017. [Online]. Available: http://www.iiconsortium.org/vertical-markets/energy-utility.htm

[61] *Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative Industrie 4.0*. Accessed on Feb. 20, 2017. [Online]. Available: http://tinyurl.com/m4f9nx3/

[62] F.-F. Xi, L. Yu, and X.-W. Tu, "Framework on robotic percussive riveting for aircraft assembly automation," *Adv. Manuf.*, vol. 1, no. 2, pp. 112–122, Jun. 2013.

[63] J. L. Joseph and M. R. Philip, "Method and system for robot localization and confinement," U.S. Patent 6 690 134, Feb. 2004.

[64] F. Tao, L. Zhang, V. C. Venkatesh, Y. Luo, and Y. Cheng, "Cloud manufacturing: A computing and service-oriented manufacturing model," *Proc. Inst. Mech. Eng. B J. Eng. Manuf.*, vol. 225, no. 10, pp. 1969–1976, Sep. 2011.

[65] D. L. Driscoll, "Process and outcomes of patient-centered medical care with Alaska native people at Southcentral foundation," *Ann. Family Med.*, vol. 11, pp. S41–S49, Jun. 2013.

[66] M. Mitsuishi and T. Nagao, "Networked manufacturing with reality sensation for technology transfer," *CIRP Ann. Manuf. Technol.*, vol. 48, no. 1, pp. 409–412, Jul. 2007.

[67] L. J. Chen, P. Bender, P. Renton, and T. El-Wardany, "Integrated virtual manufacturing systems for process optimisation and monitoring," *CIRP Ann. Manuf. Technol.*, vol. 51, no. 1, pp. 409–412, Jul. 2007.

[68] H. Sharifi, G. Colquhoun, I. Barclay, and Z. Dann, "Agile manufacturing: A management and operational framework," *Proc. Inst. Mech. Eng. B J. Eng. Manuf.*, vol. 215, no. 6, pp. 857–869, Jun. 2001.

[69] J. Li, L. Huang, Y. Zhou, S. He, and Z. Ming, "Computation partitioning for mobile cloud computing in big data environment," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 1–10, Mar. 2017.

[70] M. Qiu, Z. Ming, J. Li, K. Gai, and Z. Zong, "Phase-change memory optimization for green cloud with genetic algorithm," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3528–3540, Dec. 2015.

[71] P. Mell and T. Grance. *The NIST Definition of Cloud Computing*. Accessed on Feb. 20, 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[72] X. Xu, "From cloud computing to cloud manufacturing," *Robot. Comput. Integr. Manuf.*, vol. 28, no. 1, pp. 75–86, Feb. 2012.

[73] J. Lee, H.-A. Kao, and S. H. Yang, "Service innovation and smart analytics for industry 4.0 and big data environment," *Proc. CIRP*, vol. 16, pp. 3–8, May 2014.

[74] C. Snijders, U. Matzat, and U. D. Reips, "'Big data': Big gaps of knowledge in the field of Internet science," *Int. J. Internet Sci.*, vol. 7, no. 1, pp. 1–5, Jul. 2012.

[75] Y. He *et al.*, "Big data analytics in mobile cellular networks," *IEEE Access*, vol. 4, pp. 1985–1996, Mar. 2016.

[76] L. Cui, F. R. Yu, and Q. Yan, "When big data meets software-defined networking: SDN for big data and big data for SDN," *IEEE Netw.*, vol. 30, no. 1, pp. 58–65, Jan./Feb. 2016.

[77] M. A. Beyer and D. Laney, "The importance of 'big data': A definition," *Gartner*, vol. 2012, Jun. 2012, pp. 2014–2018.

[78] *What Is Big Data?* Accessed on Aug. 23, 2016. [Online]. Available: http://www.villanovau.com/

[79] J. Lee, E. Lapira, B. Bagheri, and H.-A. Kao, "Recent advances and trends in predictive manufacturing systems in big data environment," *Manuf. Lett.*, vol. 1, no. 1, pp. 38–41, Oct. 2013.

[80] *Bringing the Industrial Internet to the Marine Industry and Ships Into the Cloud*. Accessed on Aug. 23, 2016. [Online]. Available: https://www.webwiki.com/ esrgtech.com

[81] J. Lee, *Industrial Big Data*. Beijing, China: Mech. Ind. Press, Sep. 2015.

[82] J. Li, J. Li, X. Fu, M. A. Masud, and J. Z. Huang, "Learning distributed word representation with multi-contextual mixed embedding," *Knowl. Based Syst.*, vol. 106, pp. 220–230, Aug. 2016.

[83] M. Obitko, V. Jirkovský, and J. Bezdíček, *Big Data Challenges in Industrial Automation*. Heidelberg, Germany: Springer, Aug. 2013.

[84] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Kerberos authentication and authorization system," in *Proc. Project Athena Tech. Plan*, Feb. 1987, pp. 1–36.

[85] G. Kazuo, "Direct attached storage," in *Encyclopedia of Database Systems*. New York, NY, USA: Springer, 2009, p. 847.

[86] G. A. Garth and V. M. Rodney, "Network attached storage architecture," *Commun. ACM*, vol. 43, no. 11, pp. 37–45, Nov. 2000.

[87] O. A. Michael, "Method of enabling heterogeneous platforms to utilize a universal file system in a storage area network," U.S. Patent 6 564 228, May 2003.

[88] K. Shvachko, H. Kuang, S. Radia, and R. Chansler, "The hadoop distributed file system," in *Proc. IEEE 26th Symp. Mass Stor. Syst. Technol. (MSST)*, Incline Village, NV, USA, May 2010, pp. 1–10.

[89] S. Agarwal, "Data mining: Data mining concepts and techniques," in *Proc. Int. Conf. Mach. Intell. Res. Adv. (ICMIRA)*. Katra, India, Dec. 2013, pp. 203–207.

[90] J. L. Berral-García, "A quick view on current techniques and machine learning algorithms for big data analytics," in *Proc. IEEE 18th Int. Conf. Transparent Opt. Netw. (ICTON)*, Trento, Italy, 2016, pp. 1–4.

[91] J. Li *et al.*, "A hybrid path planning method in unmanned air/ground vehicle (UAV/UGV) cooperative systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9585–9596, Dec. 2016.

[92] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," in *Proc. 3rd Int. Symp. Resilient Control Syst. (ISRCS)*, Idaho Falls, ID, USA, Aug. 2010, pp. 15–22.

[93] D. J. Gaushell and H. T. Darlington, "Supervisory control and data acquisition," *Proc. IEEE*, vol. 75, no. 12, pp. 1645–1658, Dec. 1987.

[94] F. E. George, "Distributed control system," U.S. Patent 4 173 754, Nov. 1979.

[95] B. William, *Programmable Logic Controllers*. Waltham, MA, USA: Newnes, Mar. 2015.

[96] D. Paul, "Reference architectures for industrial automation and control systems," in *Proc. 15th Annu. Meeting ODVA Ind. Conf.*, Stone Mountain, GA, USA, Oct. 2012, pp. 1–17.

[97] J. Posada *et al.*, "Visual computing as a key enabling technology for industrie 4.0 and industrial Internet," *IEEE Comput. Graph. Appl.*, vol. 35, no. 2, pp. 26–40, Mar./Apr. 2015.

[98] C. Greamo and A. Ghosh, "Sandboxing and virtualization: Modern tools for combating malware," *IEEE Security Privacy*, vol. 9, no. 2, pp. 79–82, Mar./Apr. 2011.

[99] F. A. Ameiri and K. Salah, "Evaluation of popular application sandboxing," in *Proc. Internet Technol. Secured Trans.*, Abu Dhabi, UAE, Dec. 2011, pp. 358–362.

[100] Q. H. Bai and Y. Zheng, "Study on the access control model in information security," in *Proc. Cross Strait Quad Reg. Radio Sci. Wireless Technol. Conf.*, Heilongjiang, China, Jul. 2011, pp. 830–834.

[101] A. Almehmadi and K. El-Khatib, "On the possibility of insider threat prevention using intent-based access control (IBAC)," *IEEE Syst. J.*, to be published.

[102] D. D. Downs, J. R. Rub, K. C. Kung, and C. S. Jordan, "Issues in discretionary access control," in *Proc. IEEE Security Privacy Mag.*, Oakland, CA, USA, Apr. 1985, pp. 208–218.

[103] T. Y. Win, H. Tianfield, and Q. Mair, "Virtualization security combining mandatory access control and virtual machine introspection," in *Proc. IEEE/ACM Int. Conf. Utility Cloud Comput.*, London, U.K., Dec. 2014, pp. 1004–1009.

[104] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," in *Proc. Conf. Inf. Assurance Cyber Security*, Rawalpindi, Pakistan, Dec. 2015, pp. 83–89.

[105] N. Jazdi, "Cyber physical systems in the context of industry 4.0," in *Proc. IEEE Int. Conf. Autom. Qual. Test. Robot.*, Cluj-Napoca, Romania, May 2014, pp. 1–4.

[106] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks," *IEEE Trans. Smart Grid*, to be published.

[107] A. Varghese and D. Tandur, "Wireless requirements and challenges in industry 4.0," in *Proc. Int. Conf. Contemporary Comput. Inf.*, Bengaluru, India, Nov. 2014, pp. 634–638.

[108] T. Sauter, "The three generations of field-level networks—Evolution and compatibility issues," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3585–3595, Nov. 2010.

[109] A. B. Lugli, M. M. D. Santos, and L. R. H. R. Franco, "A computer tool to support in design of industrial Ethernet," *ISA Trans.*, vol. 48, no. 2, pp. 228–236, Apr. 2009.

[110] *IEEE 802.3 [TM] ŚStandard for EthernetŠ Marks 30 Years of Innovation and Global Market Growth*. Accessed on Feb. 20, 2017. [Online]. Available: https://standards.ieee.org/email/2013_06_802.3_ethernet_anniversary_web.html

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

[111] V. Hourdin, J.-Y. Tigli, S. Lavirotte, G. Rey, and M. Riveill, "Context-sensitive authorization for asynchronous communications," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, London, U.K., Nov. 2009, pp. 1–7.

[112] O. Goldreich, *Foundations of Cryptography*. Cambridge, MA, USA: Cambridge Univ. Press, Dec. 2004.

[113] M. Iwamoto and J. Shikata, "Constructions of symmetric-key encryption with guessing secrecy," in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, Jun. 2015, pp. 725–729.

[114] P. Yanguo, C. Jiangtao, P. Changgen, and Y. Zuobin, "Certificateless public key encryption with keyword search," *Commun. China*, vol. 11, no. 11, pp. 100–113, Nov. 2014.

[115] J. H. Abawajy, "An online credential management service for intergrid computing," in *Proc. IEEE Int. Conf. Asia–Pac. Services Comput.*, Yilan, Taiwan, Dec. 2008, pp. 101–106.

[116] D. Xikun, W. Huiqiang, and L. Hongwu, "A comprehensive monitor model for self-healing systems," in *Proc. Int. Conf. Multimedia Inf. Netw. Security*, Wuhan, China, Nov. 2010, pp. 751–756.

[117] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Topic Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.

[118] R. Xie, F. R. Yu, H. Ji, and Y. Li, "Energy-efficient resource allocation for heterogeneous cognitive radio networks with femtocells," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3910–3920, Nov. 2012.

[119] S. Bu, F. R. Yu, Y. Cai, and P. Liu, "When the smart grid meets energy-efficient communications: Green wireless cellular networks powered by the smart grid," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 3014–3024, Aug. 2012.

[120] T. Li *et al.*, "From offline toward real-time: A hybrid systems model checking and CPS co-design approach for medical device plug-and-play collaborations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 1–16, Apr. 2013.

[121] F. R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication systems for grid integration of renewable energy resources," *IEEE Netw.*, vol. 25, no. 5, pp. 22–29, Sep./Oct. 2011.

[122] H. Luo, J. Luo, Y. Liu, and S. K. Das, "Adaptive data fusion for energy efficient routing in wireless sensor networks," *IEEE Trans. comput.*, vol. 55, no. 10, pp. 1286–1299, Oct. 2006.

[123] H. Luo, Y. Liu, and S. K. Das, "Routing correlated data with fusion cost in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 11, pp. 1620–1632, Nov. 2006.

[124] Z. Zbunjak and I. Kuzle, "Advanced control and system integrity protection schemes of Croatian power transmission network with integrated renewable energy sources," in *Proc. Eurocon*, Zagreb, Croatia, Jul. 2013, pp. 706–711.

[125] R. L. Krutz, *Industrial Automation and Control System Security Principles*. Research Triangle Park, NC, USA: Int. Soc. Autom., May 2013.

[126] B. F. Crabtree *et al.*, "Primary care practice transformation is hard work: Insights from a 15-year developmental program of research," *Med. Care*, vol. 49, no. 12, pp. S28–S35, Dec. 2011.

[127] *How the Internet of Things Will Revolutionise Medicine*. Accessed on Aug. 23, 2016. [Online]. Available: http://www.techradar.com

[128] L. Sha, S. Gopalakrishnan, X. Liu, and Q. X. Wang, "Cyber-physical systems: A new Frontier," in *Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput.*, Taichung, Taiwan, Jun. 2008, pp. 1–9.

[129] Y.-F. Huang, P. Liu, Q. Pan, and J.-S. Lin, "A doctor recommendation algorithm based on doctor performances and patient preferences," in *Proc. Int. Conf. Wavelet Active Media Technol. Inf. Process.*, Chengdu, China, Dec. 2012, pp. 92–95.

[130] H. Jiang and W. Xu, "How to find your appropriate doctor: An integrated recommendation framework in big data context," in *Proc. IEEE Comput. Intell. Healthcare e-health (CICARE)*, Orlando, FL, USA, Dec. 2014, pp. 154–158.

[131] B. Vogel-Heuser, J. J. Weber, and J. Folmer, "Evaluating reconfiguration abilities of automated production systems in industrie 4.0 with metrics," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Luxembourg City, Luxembourg, Sep. 2015, pp. 1–6.

[132] C. Scheuermann, S. Verclas, and B. Bruegge, "Agile factory—An example of an industry 4.0 manufacturing process," in *Proc. IEEE Int. Conf. Cyber-Phys. Syst. Netw. Appl.*, Hong Kong, Aug. 2015, pp. 43–47.

[133] X. H. Guo and D. Lin, "Research on new industrial Ethernet network management and Internet remote control system," in *Proc. Int. Conf. Comput. Sci. Inf. Technol.*, Singapore, Sep. 2008.

[134] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on Internet of Things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, Jan. 2015.

[135] *Public Sector*. Accessed on Aug. 23, 2016. [Online]. Available: http://www.iiconsortium.org/vertical-markets/public-sector.htm

[136] A. Lohmeier, "eGovernment—A driving force for public sector innovation?" in *Proc. Int. Conf. Innov. Comput. Technol.*, London, U.K., Aug. 2013, pp. 149–154.

[137] J. M. Cheon *et al.*, "A single-chip CMOS smoke and temperature sensor for an intelligent fire detector," *IEEE Sensors J.*, vol. 9, no. 8, pp. 914–921, Aug. 2009.

[138] H. Zhang and L. Wang, "Research on Internet-based e-government on construction industry," in *Proc. Int. Conf. Manag. Service Sci. (MASS)*, Wuhan, China, Aug. 2010, pp. 1–3.

[139] H.-D. Tsui, C.-Y. Lee, and C.-B. Yao, "Creating a Web 2.0 government: Views and perspectives," in *Proc. Int. Conf. Netw. Digit. Soc. (ICNDS)*, Wenzhou, China, May 2010, pp. 648–651.

[140] Y. K. Gong and H. L. Zheng, "Bio sensing technology for environmental monitoring," *Spectrosc. Spectral Anal.*, vol. 23, no. 2, pp. 411–414, Apr. 2010.

[141] M. Kiesel and M. Wolpers, "Educational challenges for employees in project-based industry 4.0 scenarios," in *Proc. Int. Conf. Knowl. Technol. Data-Driven Bus.*, Graz, Austria, Oct. 2015, pp. 1–4.

[142] M. G. Fugini, P. Maggiolini, C. Raibulet, and L. Ubezio, "Risk management through real-time wearable services," in *Proc. 4th Int. Conf. Softw. Eng. Adv.*, Porto, Portugal, Sep. 2009, pp. 163–168.

[143] H. Ma and Y. Liu, "Correlation based video processing in video sensor networks," in *Proc. Int. Conf. Wireless Netw. Commun. Mobile Comput.*, vol. 2. Jun. 2005, pp. 987–992.

[144] Y. Song, L. Liu, H. Ma, and A. V. Vasilakos, "A biology-based algorithm to minimal exposure problem of wireless sensor networks," *IEEE Trans. Netw. Service Manag.*, vol. 11, no. 3, pp. 417–430, Sep. 2014.

[145] L. Liu, Y. Song, H. Zhang, H. Ma, and A. V. Vasilakos, "Physarum optimization: A biology-inspired algorithm for the Steiner tree problem in networks," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 818–831, Mar. 2015.

[146] H. S. Wasisto *et al.*, "Low-cost wearable cantilever-based nanoparticle sensor microsystem for personal health and safety monitoring," in *Proc. Transducers Int. Conf. Solid-State Sensors Actuators Microsyst.*, Anchorage, AK, USA, Jun. 2015, pp. 428–431.

[147] *Its Handbook*. Accessed on Aug. 23, 2016. [Online]. Available: http://roadnetworkoperations.piarc.org/index.php?option=com_content&task=view&id=38&Itemid=71&lang=en

[148] L. Chunli, "Intelligent transportation based on the Internet of Things," in *Proc. Int. Conf. Consum. Electron. Commun. Netw.*, Yichang, China, Apr. 2012, pp. 360–362.

[149] G. S. Tewolde, "Sensor and network technology for intelligent transportation systems," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, Indianapolis, IN, USA, May 2012, pp. 1–7.

[150] *Transportation*. Accessed on Feb. 20, 2017. [Online]. Available: http://www.iiconsortium.org/vertical-markets/transportation.htm

[151] H. P. Breivold and K. Sandström, "Internet of Things for industrial automation—Challenges and technical solutions," in *Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst.*, Sydney, NSW, Australia, Dec. 2015, pp. 532–539.

[152] T. Hegazy and M. Hefeeda, "Industrial automation as a cloud service," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 10, pp. 2750–2763, Oct. 2015.

[153] K. Sandstrom, A. Vulgarakis, M. Lindgren, and T. Nolte, "Virtualization technologies in embedded real-time systems," *Diabetes Care*, vol. 30, no. 2, pp. 1–8, Sep. 2007.

[154] K. Suzuki and M. Inoue, "Home network system with cloud computing and distributed autonomous control," in *Proc. IEEE 16th Int. Symp. Consum. Electron. (ISCE)*, Harrisburg, PA, USA, Jun. 2012, pp. 1–6.

[155] H. H. Pang and K.-L. Tan, "Authenticating query results in edge computing," in *Proc. IEEE Int. Conf. Data Eng.*, Boston, MA, USA, Apr. 2004, pp. 560–571.

[156] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 6, pp. 785–797, Nov./Dec. 2012.

[157] M. Aazam and E. N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. Int. Conf. Future Internet Things Cloud (FiCloud)*, Barcelona, Spain, Aug. 2014, pp. 464–470.

[158] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Comput.*, vol. 10, no. 6, pp. 87–89, Nov./Dec. 2006.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.

[159] U. Hunkeler, H. L. Truong, and A. S. Clark, "MQTT-S-A publish/subscribe protocol for wireless sensor networks," in *Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware (Comsware)*, Bengaluru, India, Jan. 2008, pp. 791–798.

[160] G. Pardo-Castellote, "OMG data-distribution service: Architectural overview," in *Proc. 23rd Int. Conf. Distrib. Comput. Syst. Workshops*, Providence, RI, USA, Oct. 2003, pp. 200–206.

[161] S. Cirani *et al.*, "A scalable and self-configuring architecture for service discovery in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 508–521, Oct. 2014.

[162] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[163] P. Verma, A. Makwana, and S. Khan, "Cyber security: A survey on issues and solutions," *J. Impact Factor*, vol. 6, no. 4, pp. 51–59, 2015.

[164] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in *Proc. IEEE 11th Int. Symp. Auton. Decentralized Syst. (ISADS)*, Mexico City, Mexico, 2013, pp. 1–6.

Jian-Qiang Li received the B.S. and Ph.D. degrees from the South China University of Technology in 2003 and 2008, respectively. He is an Associate Professor with the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China. He is leading two projects funded by the National Natural Science Foundation of China and two projects funded by the Natural Science Foundation of Guangdong, China. His major research interests include Internet of Things, robotic, hybrid systems, and embedded systems.

F. Richard Yu (S'00–M'04–SM'08) received the Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2006, he was with Ericsson, Lund, Sweden, and a start-up in CA, USA. He joined Carleton University in 2007, where he is currently a Professor. His research interests include cross-layer/cross-system design, connected vehicles, security, and green ICT. He was a recipient of the IEEE Outstanding Service Award in 2016, the IEEE Outstanding Leadership Award in 2013, the Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly, Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and International Conference on Networking 2005.

He serves on the editorial boards of several journals, including the Co-Editor-in-Chief for *Ad Hoc & Sensor Wireless Networks*, and a Lead Series Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE COMMUNICATIONS SURVEYS & TUTORIALS. He has served as the Technical Program Committee Co-Chair of numerous conferences. He is a registered Professional Engineer in the province of Ontario, Canada. He is a fellow of the Institution of Engineering and Technology. He serves as a member of Board of Governors of the IEEE Vehicular Technology Society

Genqiang Deng is currently pursuing the master's degree with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. His research focuses on Internet of Things.

Chengwen Luo received the Ph.D. degree from the School of Computing, National University of Singapore, Singapore. He was a Post-Doctoral Researcher in CSE with the University of New South Wales, Australia. He is currently an Assistant Professor with the College of Computer Science and Software Engineering, Shenzhen University, China. He has authored and co-authored of several research papers in top venues of mobile computing and wireless sensor networks, such as ACM SenSys, ACM/IEEE IPSN, IEEE TMC, IEEE/ACM ToN, and ACM TOSN. His research interests include mobile and pervasive computing, indoor localization, wireless sensor networks, and security aspects of Internet of Things.

Zhong Ming is a Professor with the College of Computer and Software Engineering, Shenzhen University. He led three projects of the National Natural Science Foundation, and two projects of the Natural Science Foundation of Guangdong Province, China. His major research interests include home networks, Internet of Things, and cloud computing. He is a Senior Member of the Chinese Computer Federation.

Qiao Yan received the Ph.D. degree in information and communication engineering from Xidian University, Xi'an, China, in 2003. She is a Professor with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. From 2004 to 2005, she was with Tsinghua University, Beijing, China, as a Post-Doctoral Fellow. From 2013 to 2014, she was with Carleton University, Ottawa, Canada, as a Visiting Scholar. Her research interests are in network security, cloud computing, and software-defined networking. Her current focus is research and development of security of software defined networking.

Authorized licensed use limited to: University of Winchester. Downloaded on October 18,2022 at 10:39:29 UTC from IEEE Xplore. Restrictions apply.