


## Article

# Framework and Capability of Industrial IoT Infrastructure for Smart Manufacturing

Keng Li <sup>1,\*</sup>, Yu Zhang <sup>2</sup>, Yong Huang <sup>1</sup>, Zhiwei Tian <sup>1</sup> and Ziqin Sang <sup>3,\*</sup><sup>1</sup> FiberHome Telecommunication Technologies Co., Ltd., Wuhan 430205, China<sup>2</sup> Wuhan FiberHome Technical Services Co., Ltd., Wuhan 430205, China<sup>3</sup> China Information Communication Technologies Group, Wuhan 430074, China

\* Correspondence: kli@fiberhome.com (K.L.); zqsang@ycig.com (Z.S.)

**Abstract:** The Internet of Things (IoT) and smart manufacturing (SM) are mutually reinforcing. The establishment of IoT-based common facilities for SM is the premise of building SM system. Industrial IoT (IIoT) infrastructure for SM refers to common facilities based on IoT that support SM in industries or sectors, and plays a dominant role and faces severe challenges in the intelligence of SM. The infrastructure is independent of the products and production process in a specific factory. This paper develops conceptual and capability frameworks of IIoT infrastructure from a unified perspective of IIoT-related SM industries. These frameworks reflect relationships between IIoT and SM with in-depth relationships among basic facilities of IIoT infrastructure and lay the foundation of SM. In this paper the common characteristics and high-level requirements with respect to the different IoT layers of IIoT infrastructure are analyzed, and the capability framework and relevant capabilities of IIoT infrastructure are summarized according to the characteristics and requirements. In order to help service providers implement their systems to meet the needs of SM, the existing and newly developed IIoT infrastructure are integrated partially or in whole according to the intelligence level, so as to provide technical guidance for stakeholders to apply emerging ICTs to SM.

**Keywords:** capability; characteristic; framework; industrial Internet of Things; infrastructure; Internet of Things; requirement; smart manufacturing



**Citation:** Li, K.; Zhang, Y.; Huang, Y.; Tian, Z.; Sang, Z. Framework and Capability of Industrial IoT Infrastructure for Smart Manufacturing. *Standards* **2023**, *3*, 1–18. <https://doi.org/10.3390/standards3010001>

Academic Editor: Elzbieta Macioszek

Received: 16 November 2022

Revised: 3 December 2022

Accepted: 6 December 2022

Published: 3 January 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

As a new industrial ecosystem, key infrastructure and new application mode, the industrial Internet of Things (IIoT) realizes the comprehensive connection of all factors, all industrial chains and all value chains throughout the comprehensive interconnection of people, machines and things. The key value of IIoT lies in the transformation of traditional manufacturing mode, production mode and industrial form, in order to lay the foundation and inject kinetic energy for industrial transformation, upgrading and development of emerging industries.

The reference architectural model Industrie 4.0 (RAMI 4.0) [1] consists of a three-dimensional coordinate system that describes all crucial aspects of Industrie 4.0. This model provides the representation of the Industrie 4.0 environment in IEC 62264 [2], from workpieces of “Product” to “Connected World”, which focuses on the enterprise-control system integration. The Industrial Internet Reference Architecture (IIRA) [3] provides guidance to IIoT stakeholders at every level to optimize their endeavors in establishing IIoT systems, consummating the convergence of operational technology (OT) and information technology (IT) to achieve the tremendous economic benefits. The reference architecture for SM [4] published by National Institute of Standards and Technology (NIST) provides the integration of manufacturing software applications in the areas of fabrication and assembly of discrete electro-mechanical parts. It is limited to design engineering, manufacturing engineering, production systems engineering, and production activities. The white paper

for Architecture of Industrial Internet V2.0 [5] released by Alliance of Industrial Internet redefines the architecture according to RAMI 4.0, IIRA and other architectures, including the three major views of service, function and implementation, which intends to provide guidance and reference for all the stakeholders and facilitate the innovation development of Industrial Internet.

All of these reference models and architectures provide the high-level concepts and intend to address major aspects of Industrial Internet, IIoT and SM. However, neither IoT-based infrastructure nor presentation of IoT development of building SM system have been clearly presented. The capabilities of hardware and software technologies are described from different aspects of views with limited scopes, which are difficult to abstract the unified content of the basic infrastructure. Many SM stakeholders are still facing challenges and requiring common and customized solutions from different sectors of the manufacturing industry. Thus, it is necessary to establish the scope of IIoT infrastructure for SM from implementer's view, and provide the relationships among these basic facilities, in which the relationships between IoT and SM have not been systematically explored before. The common infrastructure is required to support agile and customized manufacturing from diverse manufacturing fields, which could be easily adopted, large-scale promoted, customized and optimized.

In the process of the industrial transformation, SM stakeholders use a large number of emerging ICTs for system integration to empower the traditional manufacturing industry. There are huge technical barriers for manufacturing practitioners and ICT practitioners: (1) for the edge IoT-based devices, there are diverse types of sensors and gateways that adopt diverse interfaces and protocols. It is difficult, or even impossible, to make them work together. This would create isolated silos in production fields; (2) for the network, the IT and OT networks are independent of each other. It will block the development of the IT and OT convergence; (3) for the service and application support, many emerging technologies are difficult to be used due to isolated systems and platforms with limited capabilities and application scopes. In order to better help relevant stakeholders to deploy and implement SM, this paper develops a conceptual framework of IIoT infrastructure. It is based on the common IoT reference model defined in the Recommendation ITU-T Y.4000 [6], and it is dedicated to the common IIoT-related industries. This paper collects and summarizes the general characteristics and requirements of IIoT infrastructure for SM, as well as analyzes and integrates the intelligent dimension in the SM reference model defined in the Recommendation ITU-T Y.4003 [7].

The IoT and SM reference models defined in those standards only provide common high-level architectures and frameworks, but are not dedicated to specific areas such as common IIoT facilities for SM. This paper provides integration and expansion of IoT and SM framework mainly based on those two widely influential reference models and enables the IIoT infrastructure with smart capabilities and their relationships in the intelligent dimension.

It is helpful to clarify the capabilities of various types of infrastructure in the process of ICT system integration and enablement, in order to facilitate relevant practitioners to carry out accurate positioning and output ICT enabled products and technologies in the process of SM transformation from R&D, production, manufacturing, integration and other nodes, and iteratively integrate these products and technologies into the manufacturing industries, in order to achieve the goal of SM. By integrating these new solutions, factories can develop their processes digitally, boost creativity and reduce the time from design to production [8].

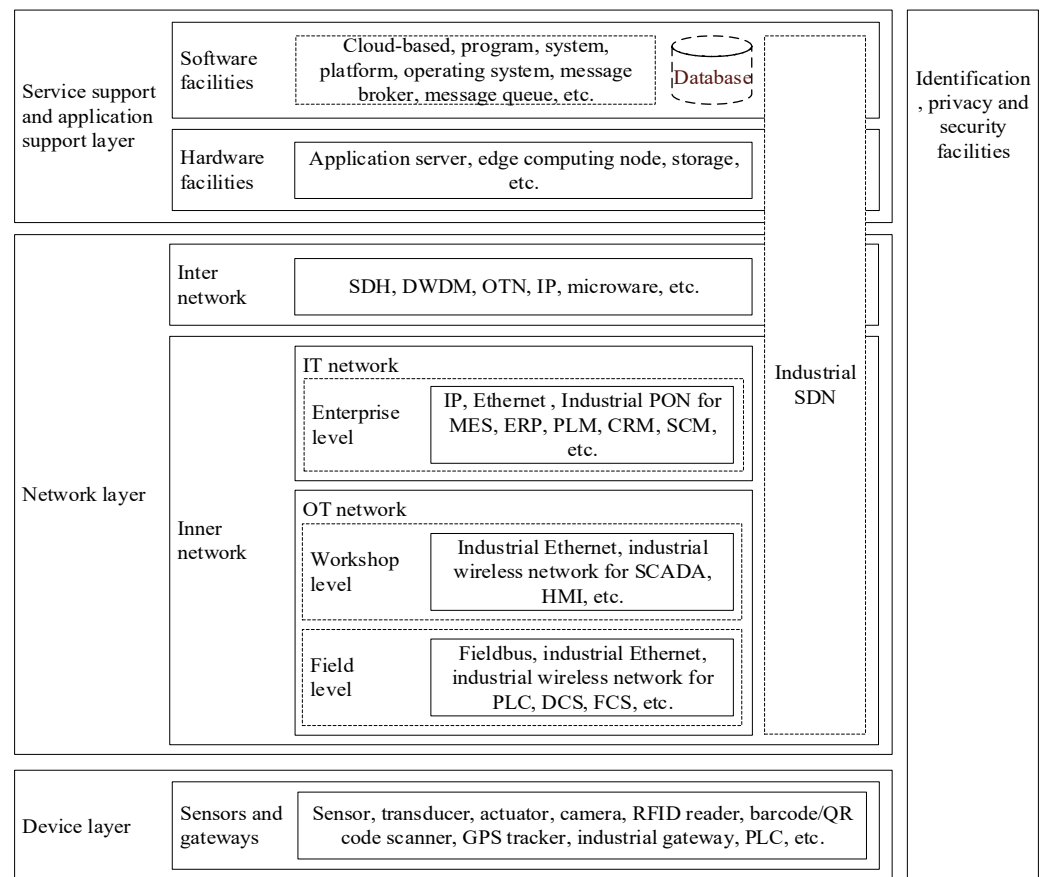
## 2. IIoT Infrastructure

SM provides an advanced production mode based on the deep integration of advanced manufacturing technologies and new generation information technologies. These technologies run through the whole product lifecycle of design, production, sales, logistics and services [9]. SM has the characteristics of self-perception, self-decision-making, self-

performing, self-adaptation and self-learning, and it aims to improve the quality, efficiency and flexibility of the manufacturing industry.

IIoT infrastructure plays a crucial role in SM. It provides supporting capabilities. With respect to SM, the IIoT can be assumed to constitute a critical foundation which may be built upon for the next steps [10]. The IIoT infrastructure is not specifically dedicated only to the support of SM, but also to other applications or industries. However, there is a strong crossover between “IIoT” and “SM” in terms of public recognition by global advanced manufacturing and IoT engaged standards developing organizations (SDOs), organizations and other interested groups [11].

We propose a conceptual framework of the IIoT infrastructure from the perspective of IoT and SM, as shown in Figure 1. It is mainly based on the IoT and SM reference model [6,7]. By exploring and developing common facilities at different layers, the model is enriched in unification of different views into one view for use by implementers and other stakeholders [1–5].



**Figure 1.** Conceptual framework of the IIoT infrastructure from the IoT and SM points of view.

### 2.1. Device Layer

Due to many communication technologies in the industrial network, the relevant communication media in physical layer of the IIoT infrastructure are very diverse [12]. The devices connected in the industrial network are not only ordinary networking and IT equipment (such as switches, routers, firewalls, PCs, printers and other equipment), but also industrial control and management equipment (such as industrial PCs, human machine interface (HMI), programmable logic controllers (PLCs), motion controllers, remote terminals and radio frequency identification (RFID) equipment).

These devices work at different layers or across multiple layers of the OSI reference model, provide data in standardized or non-standardized format, receive control and

adjustment signals from the upper layers, and perform comprehensive sensing and control of relevant hardware and processes in the industrial production environment [13].

The devices in this layer can be distinguished into sensors and gateways, which directly interact with machines, robotics, environment equipment and other field facilities for SM production, in order to improve productivity and results [14].

#### 2.1.1. Sensors

The sensors fall into different categories, such as sensors of resources, security, presence, lighting, movement, environment and position, which are installed on the physical facilities for SM. These devices make it possible to collect and track status of SM machines, robotics, operations, environment, etc., in order to help the facilities in the upper layers gather, process, analyze and eventually generate valuable information in SM services.

#### 2.1.2. Gateways

The manufacturing-specific gateways connect manufacturing facilities such as sensors, PLCs, machines and robotics [15] which have open data interfaces. This is in order to sense and identify data upward from different resources and help control and execute decision flows downward from the upper layer facilities. Gateways translate and transform information coming from devices and sensors into formats and structures suitable for applications and systems in the upper layer, and transport them using suitable network protocols, and vice versa.

In the advanced industrial environment, services are not only deployed in the cloud but are also likely to be deployed in both the industrial field and the cloud [16]. The industrial field equipment and machines will produce extensive data at the edge of the network, and the edge network equipment such as gateways at the industrial field will require interoperable data processing capability and flexible service carrying and forwarding capability.

### 2.2. Network Layer

The network provides comprehensive interconnection of people, machines and things, in order to transport data among them, this being a basic function to fulfil the requirements of industrial applications [17]. It promotes seamless flowing and integration of diverse industrial data.

The IIoT network connections involve different technical fields inside and outside the factory. Many networking technologies are used in the industrial field with related performance [18] advantages in specific scenarios. However, these technologies with specific capabilities (such as many kinds of industrial fieldbuses) are designed and applied only in specific scenarios and cannot meet the requirements of IIoT in terms of data interoperability and seamless integration.

The overall goal of the network connectivity is to promote the interconnection between systems, unlock data from isolated systems or networks, and make data playing a greater value for industry and cross industry applications.

The network layer consists of two sub-layers: inner network and inter network, as well as the industrial software-defined networking (SDN) [19] which crosses both network layer and service support and application support layer.

#### 2.2.1. Inner Network

The inner network is the network inside the factory or the enclosed area for production, which is used to connect personnel (such as production personnel, designers and external personnel), machines (such as equipment and office devices), materials (such as raw materials, work in progress and finished products), environment (such as instruments and monitoring equipment), etc. Through the inner network, they are interconnected with the enterprise data center and application servers to support the business applications in the factory [20].

From the SM points of view, the inner network encompasses OT network and IT network [21]. They are interconnected via industrial gateways (such as firewalls, data-diodes and invasion protection systems (IPSs)) to realize interconnection and physical network isolation. The OT network can be divided into field level and workshop level, while the IT network belongs to the enterprise level.

#### 1. Field level of the OT network;

In the field level of the OT network, the commonly used communication technologies in the field of industrial control are: industrial fieldbus, industrial Ethernet and industrial wireless network.

- Industrial fieldbus;

The industrial fieldbus technologies [22] (such as Profibus, Modbus, HART, CANopen, LonWorks, DeviceNet, ControlNet, CC-Link and RS232/RS485) are widely used to connect field detection sensors, actuators and industrial controllers. Industrial fieldbus mainly provides data communication support from field sensor to controller; controller to actuator; or between controller and each I/O control substation (such as PLC and DCS/FCS).

Compare with other communication technologies, the industrial fieldbus technology faces some weaknesses, such as low communication ability, short distance, poor anti-interference ability and so on [23]. Its vulnerability to strong current interference, low reliability, obsolete maintenance mode, limitation of bandwidth and distance, and high cost of cable laying cause strong limitation of usage. However, the industrial optical bus can be adopted under PLC, which is based on optical communication technology, combined with capabilities of optical splitting and multiple terminals accessing via the optical distribution network. The industrial optical bus provides competitive performance indicators for fieldbus, and, further, it provides higher bandwidth and reduces transmission delay.

- Industrial Ethernet;

The industrial Ethernet technologies (such as EtherNet/IP, PROFINET, Modbus TCP, Powerlink and EtherCAT) are the customized and optimized communication technologies based on Ethernet, which are introduced into the field of industrial control. Many industrial Ethernet protocols have gradually entered the control and communication applications in various industrial control systems [24]. Their low-cost, efficient communication ability and flexibility in network topology expansion have laid a foundation for the improvement of industrial field control level.

- Industrial wireless network.

The industrial wireless network is mainly used in some non-critical industrial applications, such as scenarios of material transport, inventory management, patrol inspection, maintenance, and other occasions [25]. Industrial wireless technologies [26] (such as Wi-Fi, Bluetooth, WirelessHART, WPAN, WIA-PA, WIA-FA, RFID, NB-IoT, ZigBee, ISA100.11a, 4G/5G and MulteFire) connect mobile equipment in the factory where cable connection is difficult or impossible.

With the development of 5G, the performance indicators such as delay, reliability and connectivity may require to be guaranteed for extreme industrial control applications [27]. With these improved capabilities, the 5G network can enlarge the scale of industrial wireless network applications for much flexible industrial application scenarios, and the industrial wireless network can work together with industrial fixed network to achieve comprehensive interconnection.

#### 2. Workshop level of the OT network;

In the workshop level of the OT network, it mainly provides connections between controllers; between controllers and local or remote monitoring systems; and between controllers and operation level systems (such as Supervisory Control and Data Acquisition (SCADA) and Human Machine Interface (HMI)). This level mainly adopts industrial

Ethernet and industrial wireless network, while some manufacturers use their own communication protocols to communicate between the industrial controllers and systems.

### 3. Enterprise level of the IT network.

In the enterprise level of the IT network, the commonly used communication technologies for network interconnection among enterprise level systems are high speed Ethernet, TCP/IP, industrial PON [28], etc. The enterprise level systems are Manufacturing Execution Systems (MES), Enterprise Resource Planning (ERP), Product Lifecycle Management (PLM), Customer Relationship Management (CRM), Supply Chain Management (SCM), etc.

The network devices in this layer help connect industrial users, systems, application servers and storage with high speed and high reliability performances, including switches, routers and other networking devices. These devices can be part of the industrial SDN, to help building the virtualized network architecture, in order to further providing networking services with the help of advanced networking technologies (such as SDN and network function virtualization (NFV)), which can have different service-level agreements (SLAs) in different logical slides of the network. These networking services can be rapidly deployed, adjusted and recycled with high quality of service (QoS) guarantee.

#### 2.2.2. Inter Network

The inter network is the network outside the factory which is used to connect entities such as smart factories, enterprise branches, upstream and downstream cooperative enterprises, public industrial cloud data centers, smart products (such as smart family appliances, smart medical instruments, smart cars and smart engineering machineries) and users [29].

The application servers of the data center inside the smart factory are interconnected with the industrial cloud data centers outside the factory through the inter network. Enterprise branches, cooperative enterprises, smart products and users are also connected to the industrial cloud data centers or enterprise data centers through the inter network according to the requirements.

The inter network adopts those network technologies such as SDH, DWDM, OTN, IP and microwave via cellular or satellite communications. From the perspective of industrial enterprises, the inter network provides dedicated lines (such as Internet dedicated line, enterprise interconnection dedicated line and cloud dedicated line) to fulfil the requirements of industry and cross industry communications [30].

#### 1. Internet dedicated line;

The Internet dedicated line enables connections between smart factory and the Internet. It may also allow the access of users or smart products to the smart factory. This is the basic dedicated line of industrial enterprises. The users or smart products are connected with the smart factory via the Internet, then interconnected with public industrial cloud data centers. This is the basis for industrial enterprises to realize intelligent services for SM.

#### 2. Enterprise interconnection dedicated line;

The enterprise interconnection dedicated line enables safe and reliable interconnections among the smart factories, enterprise branches and cooperative enterprises. This is commonly used by large and medium-sized enterprises.

#### 3. Cloud dedicated line.

The cloud dedicated line enables interconnections between the smart factory and the public industrial cloud data centers [31]. It is usually a dedicated line from an enterprise to a public cloud service provider.

### 2.3. Service Support and Application Support Layer

The IIoT infrastructure part in the service support and application support layer consists of hardware facilities and software facilities, as well as the cross layer industrial SDN.



These facilities as the infrastructure in this layer provide integration capabilities of users and resources (such as data and services) inside and/or outside the factories, and further provide capabilities of industrial data integration analysis, in order to support the various industrial applications [32]. They are a critical foundation for building industrial ecosystems for SM.

#### 2.3.1. Hardware Facilities

The hardware facilities in this layer include different types of hardware such as application servers, edge computing nodes and storage. This is in order to help building hardware-type infrastructure for further building software-type infrastructure (the software facilities in this layer), and provide multi-purpose solutions for SM, such as industrial services and applications.

The hardware facilities facilitate interconnections among devices, systems, smart products and people for enabling collection of historical and real-time data [33]. They can also interconnect with various platforms which provide data, in order to enhance comprehensive data collection and intelligent analysis.

#### 2.3.2. Software Facilities

The software facilities in this layer include different types of software such as systems, platforms, operating systems, message brokers, message queues and databases.

In this layer, the cloud-based software provides virtualized computing, storage and network resources [34], as well as fundamental cloud-based capabilities (such as Hadoop, OpenStack and Cloud Foundry), storage capabilities (such as Hadoop distributed file system, cloud databases, blob storage), computing capabilities (such as MapReduce and SPARK), and information system capabilities, in order to provide supporting capabilities for industrial services and applications. The users and industrial applications can use these resources and supporting capabilities.

#### 2.4. Industrial SDN

The industrial SDN which is used throughout the network layer and the service support and application support layer, is quite a challenge for the network operators and the system administrators. Because of the traditional methods for handling IT systems and Communication Technology (CT) networks, the relevant management personnel are only qualified from IT or CT domain, but not needed to know both, while the industrial SDN, as it takes so many benefits, also with much higher requirements for the administrators who know ICT well enough. The industrial SDN uses network controllers to uniformly manage the network resources [35] in the factory, so as to ensure the network quality of service required by key businesses.

The IT and OT network in the factory are traditionally operated independently of each other, both network topologies are rigid, and the cross-network information interaction and management are very difficult [36]. The industrial SDN enables the deep integration of the IT and OT network to build a flexible and agile industrial network.

The industrial SDN is composed of multiple protocol terminal equipment, programmable industrial software-defined networking devices and centralized industrial SDN controllers. The terminal equipment submits the data flow characteristics and transmission requirements to the industrial SDN controller through the northbound interface, and the industrial SDN controller generates the forwarding rules according to the received data flow characteristics and transmission requirements. Those forwarding rules are implemented in the industrial software-defined networking devices through the standardized southbound interface.

The industrial SDN can have one or multiple network controllers. Due to different types of northbound interfaces (such as RESTful) and southbound interfaces (such as OpenFlow, Netconf, YANG, BGP-LS, BGP Flowspec, segment routing and PCEP) of the networking devices, different network controllers control different types of networking

devices (such as industrial switches, routers, gateways, firewalls, IPS, open vSwitches (OVS), industrial PON and OTN) or the networking devices from different vendors. It is difficult to merge many protocols of northbound and southbound interfaces into one unified network controller to achieve interoperability, so multiple network controllers can be used, which can be categorized as domain controller and super controller. Each domain controller handles a part of the network (a domain), while the super controller controls all the domain controllers. These network controllers can be formed as a vertical tree topology, or a horizontal same layered topology without using super controller, in order to realize cross layer and/or cross domain management and coordination of the networking devices.

The key mechanism of the industrial SDN is to manage and configure network devices such as switches through software definition. It can also support future oriented time-sensitive networking (TSN) devices. The industrial SDN can support unified access and flexible networking of equipment in the IT and OT network, provide high bandwidth transmission guarantee and end-to-end real-time guarantee for the services. The equipment and traffic in both networks can be uniformly monitored and managed.

### *2.5. Identification, Privacy and Security Facilities*

The security-related facilities for IIoT infrastructure across all the three layers should provide relevant security capabilities not only in independent layers, but also, and mostly important, they should provide end-to-end security mechanisms for SM services and applications throughout the edge devices, networks, hardware and software facilities.

As one of the components of the IIoT infrastructure for SM, the identification, privacy and security facilities provide identification, security and protection capabilities for different factory functions [37], including device identification and authentication, privacy protection, physical security, functional security and information security. Those facilities are mainly used to protect various physical or virtual infrastructure resources, data analysis services, development kits, industrial applications, etc. They run through all three layers in the IIoT infrastructure and address the different dimensions of IIoT security, including reliability, confidentiality, integrity, availability, privacy and data protection.

In the device layer, a unique identifier (ID) could be used to register and identify different kinds of devices, services and applications. In the network layer, an ID based network communication could be leveraged to provide authentication and authorization capabilities to ensure the integrity and security of the information exchange. In the service support and applications support layer, the ID could be used as an entry to resolve the attributes, capabilities and services that are linked with the corresponding devices.

## **3. Common Characteristics and High-Level Requirements of IIoT Infrastructure for SM**

### *3.1. Integration*

The IIoT infrastructure supports the full and efficient integration of information and data, connects elements within and among enterprises, as well as between enterprises and customers, improves the response and delivery speed of enterprises to market changes and needs [38], in order to provide quick response by enterprises in terms of capabilities.

The IIoT infrastructure is based on ubiquitous perception, comprehensive connection and deep integration. It supports the collaboration of different businesses such as R&D, production and management inside the enterprise and production resources and social resources outside the enterprise, in order to explore the optimal operation efficiency of the enterprise and the optimal industrial resource allocation efficiency, and finally enables the capabilities of global collaboration.

The IIoT infrastructure is required to support capabilities of integration-including collaboration-as opposed to an isolated and silo-based approach of system development and deployment, in order to have the ability to support an ecosystem that includes all relevant stakeholders in the manufacturing value chain.



### 3.2. Compatibility

The IIoT infrastructure supports the transformation from existing industrial infrastructure in overlay mode or upgrading mode.

The overlay mode is overlaying a new network and related equipment supporting the new business processes on the existing facilities to build another system other than the original system (e.g., deploying new monitoring equipment, sensing equipment, execution equipment, etc. on the existing industrial infrastructure to realize safety monitoring, data acquisition, analysis and optimization).

The upgrading mode is upgrading the existing industrial facilities, network equipment and platform to realize the upgrading of system technologies and capabilities (e.g., at the process manufacturing site, original analog instruments can be upgraded and replaced with intelligent instruments supporting 4G/5G, in order to realize the intelligent collection and aggregation of on-site data and the unmanned operation of dangerous sites).

The IIoT infrastructure should not be bound to specific hardware or software facilities (e.g., hardware from specific vendor, software working with support of specific operating systems/database types, software using specific technologies which are capability limited or software structure/function which is hard to be modified and optimized), so as to ensure the flexibility of maintenance and expansion [39].

The IIoT infrastructure is required to be compatible with existing facilities to interact with. This includes identification capabilities compatible with heterogeneous identification systems.

The network of the IIoT infrastructure supports the capability of upgrading to, and to be compatible with networks enabling advanced technologies such as TSN and SDN.

### 3.3. Scalability

The IIoT infrastructure supports the flexibility and scalability capabilities of computing, storage, and network resources. Those IIoT resources can be automatically scaled according to the business load, in order to adapt to the continuous evolution of functional modules, data resources and application capabilities.

The IIoT infrastructure is required to be upgradable and expandable (diversity and number of devices, facilities, capabilities) according to the changing requirements of applications.

### 3.4. Efficiency and High Performance

The IIoT infrastructure supports comprehensive adaptation to the efficiency and high-performance requirements [40] of IIoT under the conditions of sensitive industrial access data, complex application scenarios and high requirements for network service performance.

The IIoT infrastructure can ensure the access quality (bandwidth, rate, delay, priority, etc.) of the connected facilities, in order to provide efficiency and high-performance capabilities.

The IIoT infrastructure is required to enable data exchanges of high volume, high quality of service, high reliability and strict latency guarantees, according to the requirements of network services and applications.

### 3.5. Heterogeneous Connectivity

The IIoT infrastructure meets the heterogeneous capabilities of the facilities in different layers of IIoT infrastructure, such as data collection and control devices in the device layer, diverse network type connectivity in the network layer and diverse computing and storage resources in the service support and application support layer, in order to provide services and capabilities across heterogeneous systems.

The IIoT infrastructure is required to support interworking among heterogeneous devices and facilities.

### 3.6. Interoperability

The IIoT infrastructure interconnects facilities in the inner network and inter network, builds a bottom-up, whole process and whole business information exchange system, in order to realize information exchange and interoperability within and across enterprises.

The IIoT infrastructure is required to support communications and interactions across systems for the enablement of diverse network services and capabilities.

### 3.7. Operational Safety and Reliability

The IIoT infrastructure supports operational safety capabilities such as endpoint protection, communication and connection protection, operational safety monitoring, analysis, configuration and management, and data protection. The operational safety refers to the aspects of safety that relate to the correct operation of a system or that are provided by the system itself.

The IIoT infrastructure can realize high reliability of the hardware and software facilities. When a single hardware or software facility fails, it can ensure business continuity. The reliability refers to the probability that the system operates correctly for a given period of time in a given environment.

The IIoT infrastructure is required to provide operational safety and reliability in order to exhibit low fault rates, high fault tolerance (i.e., the ability to keep correct operations even when faults occur) and robustness (i.e., the ability to guarantee basic functionalities in the event of a fault).

### 3.8. High Security and Sensitive Information Protection

The IIoT infrastructure supports capabilities to ensure security of facilities, control, network, applications and data. It supports comprehensive security capabilities such as system connection, system collaboration, data sharing and business cooperation [41]. These security capabilities can be categorized to physical security, functional security and information security. In terms of functional security, this includes support of confidentiality, integrity and availability.

The IIoT infrastructure supports access security for connected facilities, including mechanisms of authorization, authentication, encryption, interception and load balancing, in order to prevent SM applications, facilities, capabilities and products—e.g., data and technology features—from misuse and unauthorized access (trusted authentication and authorization). The object-to-object communication should be enabled by trusted authorization.

The IIoT infrastructure supports privacy and data protection, including capabilities of personal data protection owned by IIoT users and sensitive data protection owned by enterprises. This includes protection of identities in terms of application, approval, transfer, and cancellation.

### 3.9. Flexible and Secure Identification Management and Communication

An ID based network could be leveraged to run through facilities in all the three layers of the IIoT infrastructure, forming an ID registration and resolution system.

The ID registration and resolution system supports the unified operation, administration and maintenance of diverse identifiers, such as identifiers for users, devices and services.

The IIoT infrastructure provides capabilities to support multiple network technology types (such as VLAN and VXLAN), multiple encryption security protocols (such as SSL, DTLS and TLS), multiple tunnelling protocols (such as IPSec, L2TP and GRE) and IPv4/IPv6 dual stack, in order to provide flexible, efficient and trusted networking and communication capabilities.

The ID based network communication is required to enable various security functions (e.g., authentication and authorization) and protect sensitive information of the communication objects.

### 3.10. Customized Application Support

The IIoT infrastructure mainly focuses on the upstream and downstream cooperation within the industrial chain, provides reusable services from a digital catalogue, also provides mechanisms for discovery of services and service access endpoints, and accompanied with an access control policy management system that enables creation and management of policies. Those access control policies related to access of services by different users and privileges.

The customized applications of IIoT support the production and operation activities facing the whole industrial chain (such as R&D, production and manufacturing, supply chain, logistics, product operation and maintenance), also carry out the transactions of data and services throughout supply and demand, in order to realize information sharing and service collaboration within and among enterprises.

The IIoT infrastructure is required to provide application developers with development support environment, operation support environment, service invocation and orchestration support, service operation management, multiple tenant management and other support functions. Customized applications can obtain data, analysis and processing capabilities provided by the IIoT infrastructure through unified interfaces (such as APIs and web services).

## 4. The Reference Framework of Capabilities

The reference framework integrates the intelligence enablement with the different layers of the IIoT infrastructure. It is built according to the two dimensions of intelligence and IoT.

The intelligence dimension involves the enablement of different levels of intelligence (smart capabilities) in the IIoT infrastructure, from intelligence at integration level to intelligence at information fusion level. It is based on the reference model of SM in the context of the industrial IoT in the product life-cycle view [7].

The IoT dimension involves, with respect to the IoT reference model [6], the different layers of IIoT infrastructure, from specific data collection devices to the upper layer facilities.

The purpose that integrates the IoT and SM reference models in different dimensions, is because of the intelligence dimension of the SM reference model is the key of “smartness” which enables the SM. And the key of “smartness” is composed of different layers of intelligence, which can be reflected in different level of intelligence in this framework. With development of these “smart” enablement for IIoT infrastructure, the IIoT infrastructure can have different levels of “smart” capabilities according to different levels of requirements from the industrial services and applications.

Figure 2 illustrates the reference framework of the IIoT infrastructure capabilities for SM [6,7], provides different smart levels of capabilities across different IoT layers.

### 4.1. IoT Dimension

The IoT dimension consists of three layers: device layer, network layer and service support and application support layer.

#### 4.1.1. Device Layer

The “Device layer” represents devices, such as sensors and gateways. It is the physical foundation of the data collection facilities. It supports the basic level of intelligence in the integration level of the intelligence dimension. It provides capabilities of access management, data collection and monitoring, identification and edge computing support.

##### (1) Access management support;

The device layer facilities support different security strategies for access management, including authentication, authorization, encryption and protection. For those connected objects, illegal access and access rights limitation should be supported.

The data flow within the devices should be classified by priority differentiation for different service-level agreements.

The devices can adopt device management protocols such as OMA DM, LwM2M and oneM2M, as well as support of remote configuration, operation and upgrading.

(2) Data processing support;

The devices should collect data via diverse protocols in different layers of OSI reference model, such as Ethernet, RS232/RS485, industrial fieldbuses, MQTT, OPC UA, CoAP and SMPP. The collected data should have unified data formats and can be stored locally, further be sent to upper layer facilities for integrated analysis.

Some industrial services and applications require real-time monitoring of operational status and network status, so that the devices should meet the real-time and non-real-time monitoring of operational and network status of the devices.

(3) Control support;

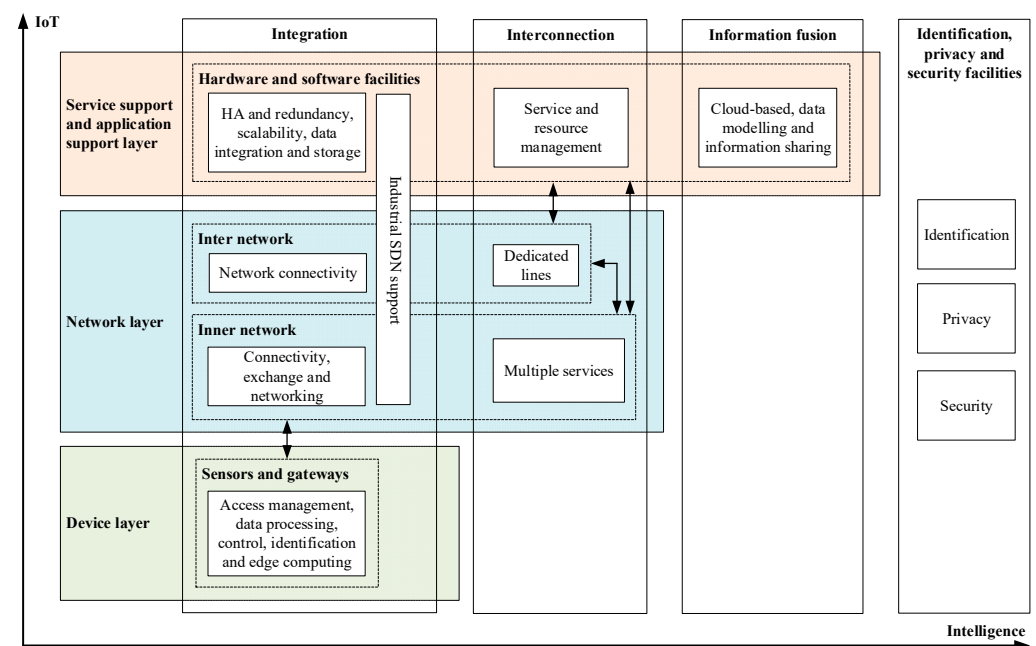
The industrial environment requires the devices to have specific control capabilities to make changes in the physical environment, the devices should convert the expected target into specific control signals and change the asset status according to the control signals.

(4) Identification support;

The collected data with unique ID should be registered, resolved and identified by the devices, and resolved in the unified ID registration and resolution system.

(5) Edge computing support.

The devices should have the capabilities of data pre-processing, detecting and locating faults, determining and executing emergency actions and edge application development environment.



**Figure 2.** Reference framework of the capabilities of IIoT infrastructure for SM.

#### 4.1.2. Network Layer

The “Network layer” represents the network infrastructure between devices and service support and application support layer facilities, and it is composed by inner network and inter network.

The inner network interconnects facilities in the device layer, the inter network and the service support and application support layer. It supports the basic and medium levels in the integration and interconnection levels of the intelligence dimension. It provides capabilities of connectivity, exchange, networking and multiple services support [42].

(1) Connectivity support for the inner network;

The network should support interconnection among diverse connected industrial objects (such as sensors, gateways, SM devices, smart products and other resources) via diverse technologies (industrial fixed and wireless communication technologies).

(2) Exchange support for the inner network;

The network supports forwarding of real-time and non-real-time data, and backwards compatible and interoperable with the legacy industrial systems with network control and management functionalities.

(3) Networking support for the inner network;

The network supports diverse network types (such as VLAN and VXLAN), encryption security protocols (such as TLS and DTLS), tunnelling protocols (such as IPsec, MPLS VPN and SD-WAN) and IPv4/IPv6 dual stack.

The network should specifically support high performance networking according to the different industrial-specific service and application requirements. Those high performances include high bandwidth, strict latency, high reliability, high frequency transmission, high-capacity connectivity, high mobility, high data forwarding priority, long transmission distance and high communication anti-interference. Especially, the video-based services normally require specific delay and bandwidth performances, and the control services normally require different low latency and low packet loss transmission performances.

The network should support load balancing and fault recovery, and support network physical or logical isolation, as well as adopt open networking architectures and protocols to not prevent network expansion.

(4) Multiple services support for the inner network;

The network should support OT and IT networking services with flexible interconnection with each other, in order to facilitate data sharing between them, and help the convergence of OT and IT.

In addition to the inter network interconnection with the inner network, the inter network also interconnects facilities of the service support and application support layer, exchanges data with facilities of the device layer and of the service support and application support layer. According to the different levels of the intelligence dimension, the capabilities of the inter network include network connectivity support in the integration level of the intelligence dimension, dedicated lines support in the interconnection level of the intelligence dimension.

(5) Network connectivity support for the inter network;

The inter network should interconnect the inner network by industrial firewalls and gateways, as well as interconnect with industrial fixed networks, wireless networks, Internet and dedicated networks.

(6) Dedicated lines support for the inter network.

The inter network mainly provides dedicated lines of Internet, enterprise interconnection and cloud, in order to facilitate data sharing and information fusion.

The industrial SDN support capability block which crosses the network layer and the service support and application support layer, provide the support of unified operation, administration and maintenance of the network via software-defined networking and network function virtualization technologies, including helping of the convergence of the IT and OT network, in order to make the network agile and smart.

#### 4.1.3. Service Support and Application Support Layer

The “Service support and application support layer” represents the infrastructure composed by hardware and software facilities for supporting services and applications. According to the different levels of the intelligence dimension, the capabilities of the service support and application support layer include support of HA and redundancy, scalability, data integration and storage in the integration level; service and resource management in the interconnection level; and cloud-based management, data modelling and information sharing support via appropriate technologies (such as cloud computing, big data, digital



twin, blockchain, information security and other emerging information technologies) [43] in the information fusion level.

(1) HA and redundancy support;

The hardware and software facilities should support high availability and load balancing of the application servers, edge computing nodes, storage and other facilities, as well as support of periodic full and incremental backup mechanism for rapid data disaster recovery and service or function migration.

(2) Scalability support;

The hardware and software facilities should support flexible scalability, in order to adapt adjustment and maintenance of data resources, functional modules and applications. These capabilities include static and dynamic (offline or online) adjustment of the hardware and software resources according to the service and application loads.

(3) Data integration support;

The diverse data that collected and generated in this layer should be properly stored in the specific databases, with limited access rights of re-organizing, splitting and mapping of those data.

The massive data processing requires HMI for enhanced user experience and adopts open integration frameworks for data integration and interconnection.

(4) Storage support;

The storage should support rational and non-rational databases, and especially have the capabilities for big data processing (such as batch computing, stream computing, real-time computing and query computing), as well as high performance data processing capabilities of high concurrency, low latency and high speed.

(5) Resource and service management support;

The hardware and software facilities support cloud-based resource management capabilities, including homogeneous and heterogeneous computing, storage and network resources, as well as monitoring of these resources to facilitate industrial data and model management.

The hardware and software facilities support centralized management of reusable services, and support service orchestration and collaboration for rapid service deployment. The adoption of low code development and graphical programming are good choices for efficient and flexible service application innovation.

(6) Cloud-based management support;

The hardware and software facilities support management of computing, storage and network resources in private, public and mixed cloud, in order to provide cloud services such as IaaS, PaaS and SaaS.

(7) Data modelling support;

The data modelling in the industrial environment requires device object modelling and production process modelling. Multiple type and dimensional semantics and models also should be supported, in order to build general semantic and model libraries for supporting data modelling from different industrial applications.

(8) Information sharing support.

The industrial information sharing is intended to break the industrial silos within and across the enterprises. The appropriate application layer communication modes could be adopted such as request/response mode and publish/subscribe mode for the help of the data sharing.

The hardware and software facilities should support distributed ledger technologies such as blockchain, in order to leverage their features for information sharing. Those features include consensus, smart contract, immutability, data sharing, decentralization and tamper-resistance.

#### 4.2. Intelligence Dimension

The intelligence dimension consists of three levels: integration, interconnection and information fusion.

#### 4.2.1. Integration Level

The “Integration” level enables the fundamental capabilities from data collection and data exchange to data storage and data management, with respect to the facilities of all layers in the IoT dimension.

In the device layer, via collecting and processing data by sensors and gateways, it interconnects devices with facilities of the network layer for transmission and exchange.

In the network layer, via interconnection between inner network and inter network, it realizes reliable transmission of data.

In the service support and application support layer, it forms the integration foundation with high performances for the support of interconnection and information fusion levels of intelligence for SM.

#### 4.2.2. Interconnection Level

The “Interconnection” level enables data interconnection capability in workshops, factories and enterprises, with respect to the network layer and the service support and application support layer in the IoT dimension.

The network layer supports data interconnection and multiple networking services among workshops, factories, enterprises and users.

The service support and application support layer supports capabilities of comprehensive services and resources management include cloud-based resource pool management and resource monitoring, as well as the capabilities of service management include resource and function allocation, application running environment and resource isolation, statistics support and billing.

#### 4.2.3. Information Fusion Level

The “Information fusion” level enables information interconnection and coordination capabilities among enterprises, with respect to the service support and application support layer in the IoT dimension.

The capabilities of cloud-based management form the flexible services providing infrastructure such as IaaS, PaaS and SaaS.

The capabilities of data modelling create digitalized data models and libraries with appropriate semantics for further information sharing support.

The capabilities of information sharing enable information interconnection, collaboration among services and applications with information exchange trustworthiness.

On the premise of identification, privacy and security support, the IIoT infrastructure provides capabilities of unified identification mechanism and global security solution penetrated into every element and process for SM, in order to facilitate sustainable operation and maintenance of the IIoT infrastructure.

### 5. Conclusions

The new era of industry requires deep integration of mature and emerging technologies. These requirements reflect not only the fusion of IT and CT, but also the convergence of IT and OT, as well as leveraging other emerging advanced technologies for information fusion across enterprises and industries accompanied with end-to-end cybersecurity. In order to build a unified and open IIoT ecosystem for SM, this paper provides framework and capability of IIoT infrastructure, which integrate the views of RAMI 4.0, IIRA and other reference architectures of SM and Industrial Internet as basis. It explores a common language for the coordination of different views.

The frameworks and capabilities of IIoT infrastructure which have been promoted on the IoT and SM standardization by ITU-T, creatively integrate the intelligence dimension of the SM reference model and IoT reference model together defined by ITU-T to develop and enable the intelligence in IIoT infrastructure for SM. The “intelligence” could be considered as the advanced smart capabilities which enable “smart” manufacturing. The scope of the defined common IIoT infrastructure enables the availability of implementation, and

the flexible frameworks of IIoT infrastructure provide a roadmap for the adoption and innovation of emerging technologies.

The clear view of IIoT infrastructure in this paper can help openness and standardization of these common basic facilities for supporting SM. (1) From the edge IoT-based devices, all the different kinds of sensors and gateways can be unified or have open interfaces to interoperate with the upper layer facilities, which means all the collected data will be interoperable and access-opened to other facilities, this is the critical part at the data collection stage; (2) from the network, not only the IT and OT network should be converged in the enterprise, but also the data should be shared across the enterprises and also the users, so as to achieve interconnections everywhere required; (3) from the service support and application support aspect, IIoT and SM both require end-to-end lifecycle management of all the resources, products, processes, systems and platforms, as well as management of the manufacturing personnel and end users, this requires complex system engineering for implementing emerging ICTs to support a comprehensive, open and secured view of SM, so as to realize information sharing and fusion anywhere (within and across enterprises and users) and anytime according to the needs. Finally, this framework enables the enterprise to trace demands from market, purchase resources from supply chain, perform agile and flexible production and gather feedbacks from the market, to form a closed-loop eco-system in supporting of sustainability.

By elaborating and summarizing the general characteristics and requirements of the IIoT infrastructure from diverse use cases in industries or sectors, the capabilities distributed at all layers of the IoT dimension and at all levels of the intelligence dimension in the IIoT infrastructure capability framework are analyzed and enabled to make manufacturing intelligent point by point, layer by layer and level by level, as well as the cross-layer capabilities of industrial SDN and cybersecurity are provided. The stakeholders of SM can refer to this capability framework to integrate the relevant capabilities gradually, in order to achieve the goal of SM in the context of IIoT.

**Author Contributions:** Conceptualization, K.L. and Y.Z.; Investigation, Y.Z., Y.H. and Z.T.; Writing—original draft, Y.Z.; Writing—review & editing, K.L., Z.S. and Y.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References

1. Koschnick, G.; German Electro and Digital Industry Association (ZVEI). *Industrie 4.0: The Reference Architectural Model Industrie 4.0 (RAMI 4.0)*. 2015. Available online: [https://www.zvei.org/fileadmin/user\\_upload/Presse\\_und\\_Medien/Publikationen/2015/april/Das\\_Referenzarchitekturmodell\\_Industrie\\_4.0\\_RAMI\\_4.0\\_/ZVEI-Industrie-40-RAMI-40-English.pdf](https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2015/april/Das_Referenzarchitekturmodell_Industrie_4.0_RAMI_4.0_/ZVEI-Industrie-40-RAMI-40-English.pdf) (accessed on 15 November 2022).
2. International Electrotechnical Commission. *IEC 62264-1; Enterprise-Control System Integration*, 6th ed.; IEC: Geneva, Switzerland, 2013.
3. Industry IoT Consortium (IIC). *The Industrial Internet Reference Architecture Version 1.10*. 2022. Available online: <https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf> (accessed on 15 November 2022).
4. National Institute of Standards and Technology (NIST). *NIST Advanced Manufacturing Series 300-1—Reference Architecture for Smart Manufacturing Part 1: Functional Models*; NIST: Gaithersburg, MD, USA, 2016.
5. Alliance of Industrial Internet. *Architecture of Industrial Internet (V2.0)*. 2020. Available online: <http://www.aii-alliance.org/index/c315/n45.html> (accessed on 15 November 2022). (In Chinese)
6. *ITU-T Recommendation Y.4000; Overview of the Internet of Things*. ITU: Geneva, Switzerland, 2012.
7. *ITU-T Recommendation Y.4003; Overview of Smart Manufacturing in the Context of the Industrial Internet of Things*. ITU: Geneva, Switzerland, 2018.
8. European Commission. *The Internet of Things in Smart Manufacturing*. 2021. Available online: <https://digital-strategy.ec.europa.eu/en/library/internet-things-smart-manufacturing> (accessed on 15 November 2022).

9. Ministry of Industry and Information Technology (MIIT). National Intelligent Manufacturing Standard System Construction Guidelines. 2021. Available online: [http://www.gov.cn/zhengce/zhengceku/2021-12/09/content\\_5659548.htm](http://www.gov.cn/zhengce/zhengceku/2021-12/09/content_5659548.htm) (accessed on 15 November 2022). (In Chinese)
10. VDI/VDE GMA, ZVEI: Status Report—Reference Architecture Model Industrie 4.0 (RAMI 4.0). July 2015. Available online: [https://www.zvei.org/fileadmin/user\\_upload/Presse\\_und\\_Medien/Publikationen/2016/januar/GMA\\_Status\\_Report\\_Reference\\_Architecture\\_Model\\_Industrie\\_4.0\\_RAMI\\_4.0/GMA-Status-Report-RAMI-40-July-2015.pdf](https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report_Reference_Architecture_Model_Industrie_4.0_RAMI_4.0/GMA-Status-Report-RAMI-40-July-2015.pdf) (accessed on 15 November 2022).
11. ISO/IEC TR 30166; Internet of things (IoT)—Industrial IoT. ISO/IEC: Geneva, Switzerland, 2020.
12. Yang, H.; Kumara, S.; Bukkapatnam, S.T.S.; Tsung, F. The internet of things for smart manufacturing: A review. *IISE Trans.* **2019**, *51*, 1190–1216. [[CrossRef](#)]
13. Canavan, L. What is IIoT? The Industrial Internet of Things Primer, September 2019. Available online: <https://www.iiconsortium.org/2019/09/what-is-iiot-the-industrial-internet-of-things-primer/> (accessed on 15 November 2022).
14. Dai, Y.; Zhao, L.; Lyu, L. MEC Enabled Cooperative Sensing and Resource Allocation for Industrial IoT Systems. *China Commun.* **2022**, *19*, 214–225. [[CrossRef](#)]
15. Kumar, A. Methods and Materials for Smart Manufacturing: Additive Manufacturing, Internet of Things, Flexible Sensors and Soft Robotics. *Manuf. Lett.* **2018**, *15*, 122–125. [[CrossRef](#)]
16. Evjemo, L.D.; Gjerstad, T.; Grøtli, E.L.; Sziebig, G. Trends in Smart Manufacturing: Role of Humans and Industrial Robots in Smart Factories. *Curr. Robot. Rep.* **2020**, *1*, 35–41. [[CrossRef](#)]
17. Dorst, W.; Scheibe, A. Implementation Strategy Platform Industrie 4.0. January 2016. Available online: [https://www.zvei.org/fileadmin/user\\_upload/Presse\\_und\\_Medien/Publikationen/2016/januar/Implementation\\_Strategy\\_Industrie\\_4.0\\_Report\\_on\\_the\\_results\\_of\\_Industrie\\_4.0\\_Platform/Implementation-Strategy-Industrie-40-ENG.pdf](https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/Implementation_Strategy_Industrie_4.0_Report_on_the_results_of_Industrie_4.0_Platform/Implementation-Strategy-Industrie-40-ENG.pdf) (accessed on 15 November 2022).
18. ISO 22400-2; Automation Systems and Integration—Key Performance Indicators (KPIs) for Manufacturing Operations Management—Part 2: Definitions and Descriptions. ISO: Geneva, Switzerland, 2014.
19. ITU-T Recommendation Y.3300; Framework of Software-Defined Networking. ITU: Geneva, Switzerland, 2014.
20. Zhang, X.; Ming, X. An implementation for Smart Manufacturing Information System (SMIS) from an industrial practice survey. *Comput. Ind. Eng.* **2021**, *151*, 106938. [[CrossRef](#)]
21. Cigref report, IT/OT convergence: A Fruitful Integration of Information Systems and Operational Systems. 2019. Available online: <https://www.cigref.fr/cigref-report-it-ot-convergence-a-fruitful-integration-of-information-systems-and-operational-systems> (accessed on 15 November 2022).
22. IEC 61158-1 Ed.2.0; Industrial Communication Networks—Fieldbus Specifications—Part 1: Overview and Guidance for the IEC 61158 and IEC 61784 Series. IEC: Geneva, Switzerland, 2019.
23. Lu, Y.; Xu, X.; Wang, L. Smart manufacturing process and system automation—A critical review of the standards and envisioned scenarios. *J. Manuf. Syst.* **2020**, *56*, 312–325. [[CrossRef](#)]
24. Abubakr, M.; Abbas, A.T.; Tomaz, I.; Soliman, M.S.; Luqman, M.; Hegab, H. Sustainable and Smart Manufacturing: An Integrated Approach. *Sustainability* **2020**, *12*, 2280. [[CrossRef](#)]
25. Yu, H.; Zeng, P.; Xu, C. Industrial Wireless Control Networks: From WIA to the Future. *Engineering*. **2022**, *8*, 18–24. [[CrossRef](#)]
26. Cao, W.; Jiang, P.; Fu, Y. Ubiquitous data computing and information using in a smart factory with wireless manufacturing. *Eng. Sci.* **2013**, *11*, 2–9.
27. Suvarna, M.; Büth, L.; Hejny, J.; Mennenga, M.; Li, J.; Ng, Y.; Herrmann, C.; Wang, X. Smart Manufacturing for Smart Cities—Overview, Insights, and Future Directions. *Adv. Intell. Syst.* **2020**, *2*, 2000043. [[CrossRef](#)]
28. European Telecommunications Standards Institute (ETSI). Fifth Generation Fixed Network (F5G), F5G Technology Landscape. 2021. Available online: [https://www.etsi.org/deliver/etsi\\_gs/F5G/001\\_099/003/01.01.01\\_60/gs\\_F5G003v010101p.pdf](https://www.etsi.org/deliver/etsi_gs/F5G/001_099/003/01.01.01_60/gs_F5G003v010101p.pdf) (accessed on 15 November 2022).
29. Lenz, J.; MacDonald, E.; Harik, R.; Wuest, T. Optimizing smart manufacturing systems by extending the smart products paradigm to the beginning of life. *J. Manuf. Syst.* **2020**, *57*, 274–286. [[CrossRef](#)]
30. Li, B.; Zhang, L.; Chai, X. Smart Cloud Manufacturing (Cloud Manufacturing 2.0)—A New Paradigm and Approach of Smart Manufacturing. *ISPE CE* **2014**, *26*.
31. Mittal, S.; Khan, M.A.; Romero, D.; Wuest, T. Smart manufacturing: Characteristics, technologies and enabling factors. *Proc. Inst. Mech. Eng. Part B J. Eng. Manuf.* **2019**, *233*, 1342–1361. [[CrossRef](#)]
32. Moghaddam, M.; Cadavid, M.N.; Kenley, C.R.; Deshmukh, A.V. Reference architectures for smart manufacturing: A critical review. *J. Manuf. Syst.* **2018**, *49*, 215–225. [[CrossRef](#)]
33. Yao, X.; Zhou, J.; Lin, Y.; Li, Y.; Yu, H.; Liu, Y. Smart manufacturing based on cyber-physical systems and beyond. *J. Intell. Manuf.* **2017**, *30*, 2805–2817. [[CrossRef](#)]
34. Ghahramani, M.; Qiao, Y.; Zhou, M.C.; O'Hagan, A.; Sweeney, J. AI-based modeling and data-driven evaluation for smart manufacturing processes. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1026–1037. [[CrossRef](#)]
35. Jiang, J.; Lin, C.; Han, G.; Abu-Mahfouz, A.M.; Shah, S.B.H.; Martínez-García, M. How AI-Enabled SDN Technologies Improve the Security and Functionality of Industrial IoT Network: Architectures, Enabling Technologies, and Opportunities. *Digit. Commun. Netw.* **2022**. [[CrossRef](#)]

36. Parhi, S.; Joshi, K.; Akarte, M. Smart manufacturing: A framework for managing performance. *Int. J. Comput. Integr. Manuf.* **2021**, *34*, 227–256. [[CrossRef](#)]
37. Tuptuk, N.; Hailes, S. Security of smart manufacturing systems. *J. Manuf. Syst.* **2018**, *47*, 93–106. [[CrossRef](#)]
38. Zenisek, J.; Wild, N.; Wolfartsberger, J. Investigating the Potential of Smart Manufacturing Technologies. *Procedia Comput. Sci.* **2021**, *180*, 507–516. [[CrossRef](#)]
39. Cheng, J.; Chen, W.; Tao, F.; Lin, C.L. Industrial IoT in 5G environment towards smart manufacturing. *J. Ind. Inf. Integr.* **2018**, *10*, 10–19. [[CrossRef](#)]
40. Kim, H.; Shon, T. Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. *J Supercomput* **2022**, *78*, 13554–13563. [[CrossRef](#)] [[PubMed](#)]
41. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. [[CrossRef](#)] [[PubMed](#)]
42. Lu, Y.; Asghar, M.R. Semantic communications between distributed cyber-physical systems towards collaborative automation for smart manufacturing. *J. Manuf. Syst.* **2020**, *55*, 348–359. [[CrossRef](#)]
43. Xia, K.; Sacco, C.; Kirkpatrick, M.; Saidy, C.; Nguyen, L.; Kircaliali, A.; Harik, R. A digital twin to train deep reinforcement learning agent for smart manufacturing plants: Environment, interfaces and intelligence. *J. Manuf. Syst.* **2021**, *58*, 210–230. [[CrossRef](#)]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.