工业互联网产业联盟
Alliance of Industrial Internet

Alliance of Industrial Internet

Address: Building A, No.52 Huayuan Bei Road, Haidian District, Beijing, P.R.China 100191
TEL:86-10-62305887
E-mail: aii@caict.ac.cn
Website: http://www.aii-alliance.org/

Scan QR Code, follow us

工业互联网产业联盟
Alliance of Industrial Internet

Industrial Internet Architecture

(Version 1.0)

Alliance of Industrial Internet (AII)

August 2016

Forewords

In recent years, with the accelerated integration between the new generation information technologies, such as the Internet, Internet of Things (IoT), cloud computing, big data and artificial intelligence, with traditional industries, a new round of technical revolution and industrial reform is rising up, a series of new modes of production and organization ways as well as business models are keeping emerging. Under such circumstances, the industrial internet was born at the right moment, and the explorations at both home and abroad are in full swing promoting an intelligence-oriented reform of the global industrial system.

The industrial internet involves all segments and all entities of industry and ICT fields such as internet and is evolving into an entirely new and complicated eco-system. Discrepancies in understanding industrial internet may lead to divergences in choosing technologies and standard roadmaps, which will affect the interoperability and raise deployment costs. For this reason, under the guidance of the Ministry of Industry and Information Technology (MIIT), Alliance of Industrial Internet (referred to as AII hereinafter) launched the study on the industrial internet architecture, and developed this "Industrial Internet Architecture" report (version 1.0) based on summarizing development practices at both home and abroad, which introduces the connotations, targets, architecture, key elements and trends of the industrial internet. It aims to drive industry community to reach a wide consensus on industrial internet, to provide references and guidance to AII's works, such as the technical innovation, standard development, test and verification, application practices, etc. of industrial internet by taking the architecture as a traction, and to boost the healthy and fast development of industrial internet.

There's no doubt that our understanding about the industrial internet is still preliminary as the industrial interne is a long evolution. The AII will continue revising and publishing updated versions of the report on the basis of continuous and in-depth studies as well as the development of industrial internet at both home and abroad and feedbacks from the industrial communities.

Guided by: Ministry of Industry and Information Technology

Led by: China Academy of Information and Communications Technology (CAICT)

Participated by: China Telecom Group Corporation, Huawei Technologies Co. Ltd., Shenyang Institute of Automation Chinese Academy of Sciences, China Aerospace Science and Industry Corporation (CASIC), Haier Group, Sany Group, Alibaba Cloud, Qihoo 360 Technology Co. Ltd., China Mobile Communications Group Corporation, ZTE Corporation, Tsinghua University, Legendsec Information Technology (Beijing) Co. Ltd, and CDI Corporation.

Drafting group members:

CAICT: Yu Xiaohui, Li Haihua, Tian Hongchuan, Gao Wei, Liu Mo, Tian Huirong, Wei Kai, Liu Yang, Du Jiadong, Xiao Rongmei, Li Qiang, Zhang Hengsheng, Jiang Xinhao, Li Zheng, Xie Wei, Wang Feng, Zhang Xueli, Qin Ye, Huang Ying, Wang Xinyi, Wang Xiaoling, Liu Lihui, Liu Zhao, Liu Rongduo, Liu Hehe, Liu Difei, Guan Xin, Yang Xi, Yang Siwei, Song Fei, Zhang Tian, Zhao Feng, Duan Shihui, Xu Guibao

China Telecom: Sun Jian, Zhang Dong, Xia Yan

Huawei: Jiang Wangcheng, Peng Yan

Shenyang Institute of Automation, CAS: Yu Haibin, Zeng Peng

CASIC: Chai Xudong, Li Runqiang

Haier: Chen Lucheng, Zhang Weijie
Sany: He Dongdong, Wang Jinxia
Alibaba Cloud: Liu Song, Ma Tiebao, Li Junping
Qihoo 360: Tan Xiaosheng
China Mobile: Lin Lin, Wu Shuyan
ZTE: Gao Feng
Tsinghua University: Wang Jianmin, Wang Cheng
Legendsec: Tao Yaodong
CDI: Zhen Xihui, Wang Kun

Chairperson of AII and president of CAICT, Ms. Cao Shumin led the study of industrial internet architecture and related researches, set up several study groups to carry out researches on industrial internet reference architecture, requirements, networks, data, security, identifier, industry and policy respectively, as well as had lots of meetings to hear reports and give instructions, which promoted the in-depth studies on the industrial internet architecture and key directions, as well as the results refinement. Besides, other leaders of CAICT also provided guidance during developing the architecture and drafting of this report, including vice presidents of CAICT, Liu Duo and Zhang Yanchuan, director of Science and Technology Commission, Jiang Lintao, director of Technology and Standards Research Institute, Wang Zhiqin, deputy director of Technology and Standards Research Institute, Shi Youkang, chief engineer of Technology and Standards Research Institute, Xu Heyuan, deputy director Information Technology and Industrialization Integration Research Institute, Zhu Min, director of Security Research Institute Wei Liang, and deputy director of Economy and Policy Research Institute, Xin Yongfei.

During drafting the report, to fully understand the industrial development status and requirements from industrial communities, the drafting group surveyed hundreds of representative enterprises and institutions, including industrial companies like GE, CASIC, Haier, Sany, Bosch, Foxconn, iSESOL, Weichai Power, SINOPEC Jiujiang Branch, CAS Shenyang Institute of Automation, ZOOMLION, HollySys, Supconit, COMAC, INESA, and SMTCL; ICT companies like Huawei, Intel, China Telecom, ZTE, Cisco, SAP, China Mobile, CAXA, and PCITC; Internet companies like Alibaba, Tencent, Baidu, JD, Suning.cn, Zhaogang.com, and Ouyeel; and institutions like Industrial Internet Consortium (IIC), National Institute of Standards and Technology (NIST), United States Information Technology Office (USITO), Germany Federal Ministry of Education and Research, ZVEI, Germany Industrie 4.0 Scientific Advisory Committee, and Fraunhofer. Through these surveys, the drafting group further learned about the understanding of the industrial communities and governments towards industrial internet and the explorations they carry out, and these offer significant references to the study of industrial internet architecture and the writing of this report.

During drafting the report , the drafting group consulted more than 30 academicians and experts for critical questions in architecture design for several times, and they are Wu Hequan, Hu Qiheng, Zhu Gaofeng, Li Guojie, Wu Cheng, Shen Changxiang, Liu Jie, Li Bohu, Li Peigen, Li Yunjie, Tan Jianrong, Gui Weihua, Wang Endong, Chai Hongfeng, Chen Chun, Wu Jianping, Yu Shaohua, Gao Xinmin, Zhu Sendi, Dong Jingchen, Yu Haibin, Qian Hualin, and Mao Wei. This report is a result of several revisions and improvements based on the experts' opinions. Moreover, Gao Xinmin, Vice President of Internet Society of China gave many suggestions in detail to the report.

Hereby, we'd like to thank all persons participating in writing of this report, as well as all experts, companies and institutions providing guidance and suggestions to the report.

目录 CONTENTS

List of Figures

I、Industrial Internet Connotation and its Relationship with Intelligent Manufacturing

(I) Connotation of Industrial Internet

The connotation of industrial internet is used to define the scope and characteristics of industrial internet, and to clarify the overall objectives of industrial internet. It is the basis and starting point for industrial internet study. In our opinions, industrial internet is a kind of industry and application ecology generated from the all-round deep integration of the Internet and the new generation information technology with the industrial system, and is the key comprehensive information infrastructure for industrial intelligent development. In essence, it is designed to realize intelligent control, operation optimization and reform of production and organization ways based on the network interconnection among machines, raw materials, the control system, the information system, products and human, through the overall deep perception, real-time transmission and exchange, fast computing and advanced modeling analysis of the industrial data. It can be comprehended from three main aspects - “network”, “data” and “security”. Of them, network is the foundation, which means to achieve the whole industrial system’s interconnection via IoT, Internet and other technologies so as to facilitate the full flow and seamless integration of industrial data; Data is the core, which means to generate data-based systematic intelligence through the whole-cycle perception, collection and integrated application of the industrial data to enable flexible manufacturing, operation management optimization, collaborative production organization and business model innovation, which driving industry’s intelligent development; and Security is the guarantee, i.e. to ensure the realization of industrial intelligence through constructing a security protection system that covers the whole industrial system. The evolution of industrial internet represents the integration of several industrial sector’s ecosystems. It is an inevitable course to build the industrial ecosystem and implement industrial intelligent development.

The integration of industrial internet and the manufacturing will bring intelligent improvements in four aspects. First, Intelligent production, which means to realize intelligent decision-making and dynamic optimization from single machine to the production line, the workshop and even the whole factory, to significantly improve the whole-process productivity, quality and reduce costs. Second, networking collaborative, which means to form a series of new models such as crowdsourcing, collaborative design, collaborative manufacturing, and vertical e-commerce to greatly reduce the development and manufacturing costs of new products, and shorten products’ time-to-market. Third, personalized customization, which means to realize low-cost largescale customization based on users' personalized needs learned from the Internet and through flexible design, manufacturing resources and production processes. Fourth, servicization extension, which means to provide remote maintenance, shutdown prediction, performance optimization, etc. through real-time monitoring of product operation and offer feedback for product design optimization, enabling service-oriented enterprise transformation.

The manufacturing reform driven by industrial internet will be a long course. New industrial production models and resource organization ways will not be built at one stroke as well. Instead, it is a process from partial to whole, from shallow to deep, and to finally realize the deep integration and integrated application of ICT in industry's all factors, all fields, the whole industrial chain and value chain.

(II) Industrial Internet's Relationship with Intelligent Manufacturing

As the core driving force and strategic focus of the currently new round of industrial reform, intelligent manufacturing is a general term for advanced manufacturing processes, systems and models that are based on the new generation information technologies like IoT, Internet, big data, and cloud computing, run through all links of the manufacturing activities such as design, production, management and service, and feature in deep self-perception of information, self-decision making by intelligent optimization, self-implementation from precision control. It has four characteristics, which are intelligent factory as the carrier, intelligence of critical production links as the core, end-to-end data flow as the basis, and overall deep interconnection as the support.

Intelligent manufacturing is closely related with industrial internet as its accomplishment mainly relies on two basic capabilities: the first is industrial manufacturing technologies which are the fundamental, determining the manufacturing boundaries and capabilities, including advanced equipment, materials and techniques; and the second is the industrial internet, which includes intelligent sensing controlled software and hardware, new type of industrial network, industrial big data platform and other comprehensive information technology elements, and is the key to fully develop the potentials of industrial equipment, techniques and materials, improve production efficiency, optimize resource allocation efficiency, create differentiated products and add value to services. Therefore, we believe, industrial internet is the key foundation of intelligent manufacturing, providing necessary common infrastructure and capabilities to its reform, and can be used to support the intelligent development of other industry sectors as well.

II. Industrial Internet Architecture

(I) Business requirements of Industrial Internet

The business requirements of industrial internet can be analyzed through two perspectives as shown in Figure 1, that is, industry perspective and Internet perspective.

From industry perspective, industrial internet mainly refers to the intelligence of the production system to the intelligence of the business system, developing from the inward to the outward. By employing information and communications technologies, the production system will enable the real-time connection and intelligent interaction between the machines, the machine and the system, and the upstream and downstream enterprises, and drive the optimization of commercial activities. The business requirements include industrial system-oriented optimization of various levels, such as ubiquitous sensing, real-time monitoring, precision control, data integration, operation optimization, supply chain collaboration, needs matching and service value adding.

From internet perspective, industrial internet mainly refers to business system reforms, which driving the intelligentization of the production system, developing from the outward to the inward, i.e., the new Internet business models and services in the marketing, service and design links spur the intelligent reform of the production organization and manufacturing models. Its business requirements consist of Internet-based precision marketing, customization, intelligent services, crowdsourcing, collaborative design, collaborative manufacturing, flexible manufacturing, etc.

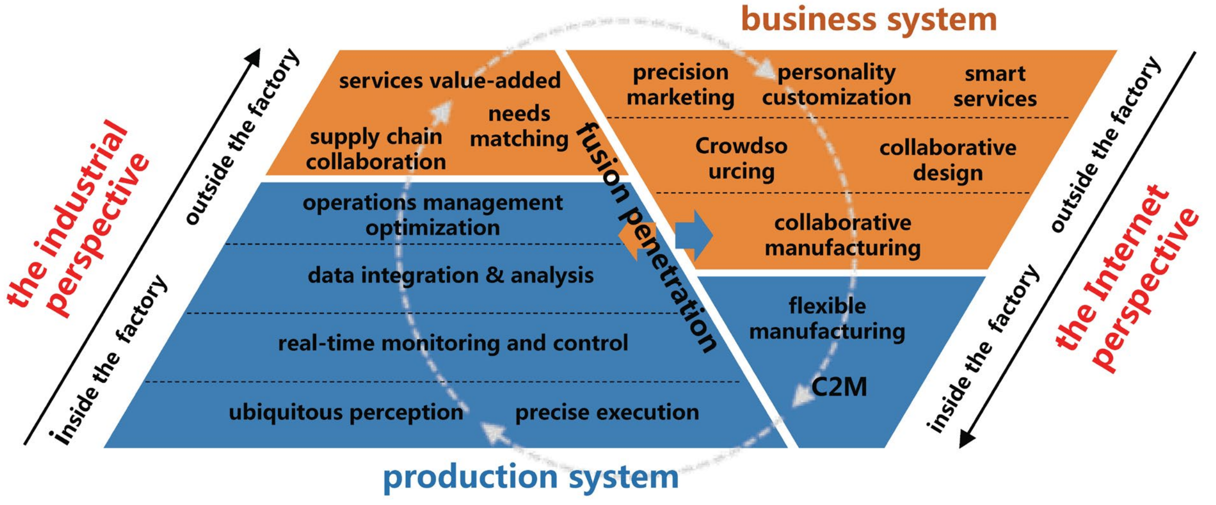

Figure 1 Industrial Internet Business Requirements

(II) Architecture of Industrial Internet

The core of industrial internet is the data-driven intelligence that is based on overall interconnection. For both of the industry perspective and Internet perspective, network, data and security are their common foundation and common support.

"Network" is the supporting basis for industrial system interconnection and industrial data transmission and exchange, including the network interconnection system, identifier resolution system and application supporting system. It can realize the seamless delivery of information data between the production system units, and between the entities of the production systems and business systems with the ubiquitous and interconnected network infrastructure, robust and deployable identifier resolution system, as well as the central and generic application supporting system, thereby to build new type of machine communication ways, equipment connection ways by wired and wireless technology, and supporting production models with features of real-time sensing and collaborative interaction to generate.

"Data" is the core driver of industrial intelligence, including functional modules such as data collection and exchange, integrated processing, modelling and analysis, decision optimization, and feedback and control. It can enable precision computing and complicated analysis of the production site, information of the collaborative enterprises, and customer needs through collection and exchange of massive data, by collection and exchanging of massive data, integrated processing of heterogeneous data, edge computing of machine data, fixed iteration of experience models, and cloud-based big data computing and analysis, thereby producing management decisions for enterprises operation and control commands for machine running to drive the intelligence and optimization of equipment, operation management and commercial activities.

"Security" refers to the protection of networks and data in industrial internet, including equipment security, network security, controlling security, data security, application security and comprehensive security management. It tries to protect network infrastructure and system software from internal and external attacks, reduce the risk of unauthorized access of enterprise data, guarantee the data transmission and storage security, and realize the all-around protection of both the industrial production system sand the business systems. The industrial internet architecture is shown in Figure 2 as below.

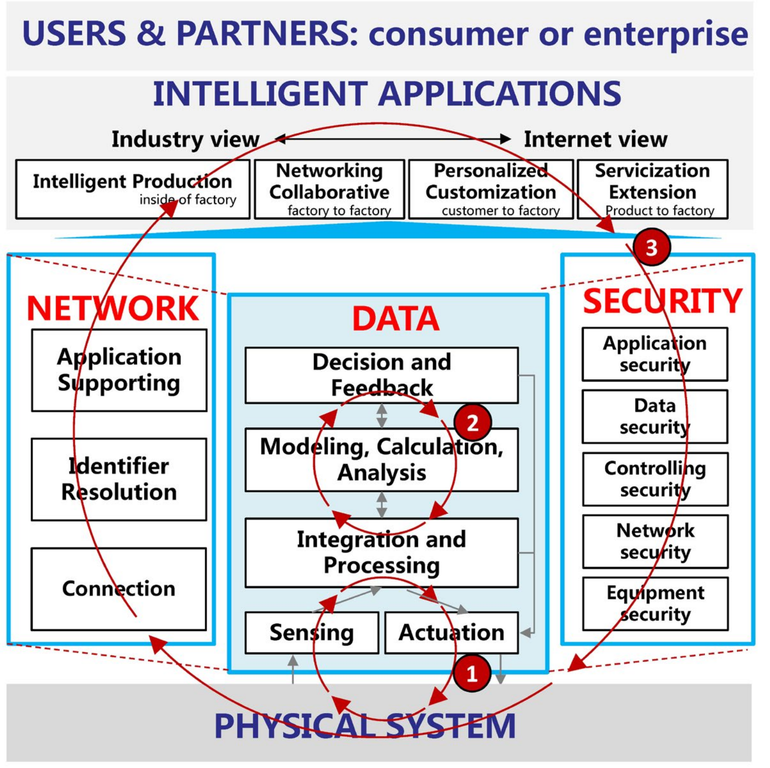

Figure 2 Industrial Internet Architecture

Based on network, data and security, the industrial internet will build three optimization close loops oriented to intelligent industrial development. The first close loop is oriented to equipment operation optimization, the core of which is real-time sensing and edge computing based on machine operation data and production environment data, to bring about dynamic optimization and adjustment of the machines and equipment, and develop smart machines and flexible production lines; the second is oriented to production operation optimization, the core of which is integrated processing and big data modelling analysis based on information system data, manufacturing execution system data, and control system data, to realize dynamic optimization and adjustment of production operation management and generate intelligent production models for various scenarios; and the third is oriented to enterprise collaboration, user interaction and optimization of products and services, the core of which is comprehensive integration and analysis based on supply chain data, user requirement data and product and service data, to produce new models like network-based networking collaboration, personalized customization and servicization extension.

III. Network Systems of Industrial Internet

(I) Network System Frame of Industrial Internet

With the development of intelligent manufacturing, the needs of digitalization, networking and intellectualization within the factory and data exchange needs between inside and outside of the factory are increasing. Under such circumstance, the industrial internet presents as an interconnected system which involves three types of enterprise entities, seven interconnected elements and eight interconnection types as shown in Figure 3.

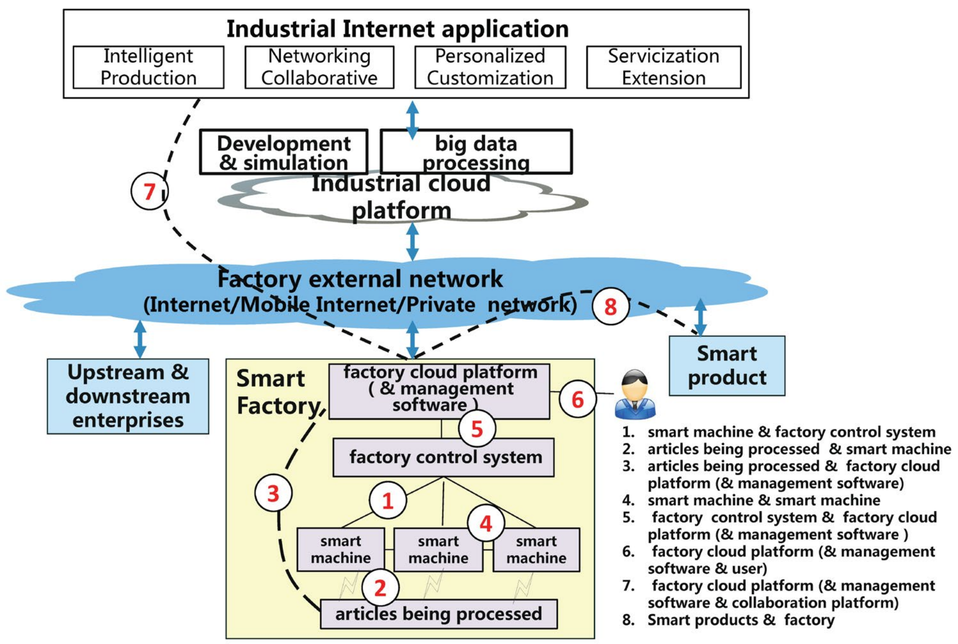

Figure 3 Industrial Internet Interconnection

The three types of enterprise entities refer to industrial manufacturing enterprises, industrial service enterprises (enterprises providing services around design, manufacturing, supplying and service links) and Internet enterprises, the roles of which are penetrating and mutually shifting. The seven interconnection elements include articles in process, smart machines, factory control system, factory cloud platform (and management software), intelligent products, and industrial internet applications, which are expanded to all segments of a product's whole life cycle from traditional automation control by the industrial internet. The eight interconnection types consist of the complex and diversified interconnection relations among the seven interconnection elements, becoming a complicated network system that connects the design capability, manufacturing capability, commercial capability and user services.

The development of the above interconnection needs impels the factory network to reform and form an overall network frame for the industrial internet as shown in Figure 4.

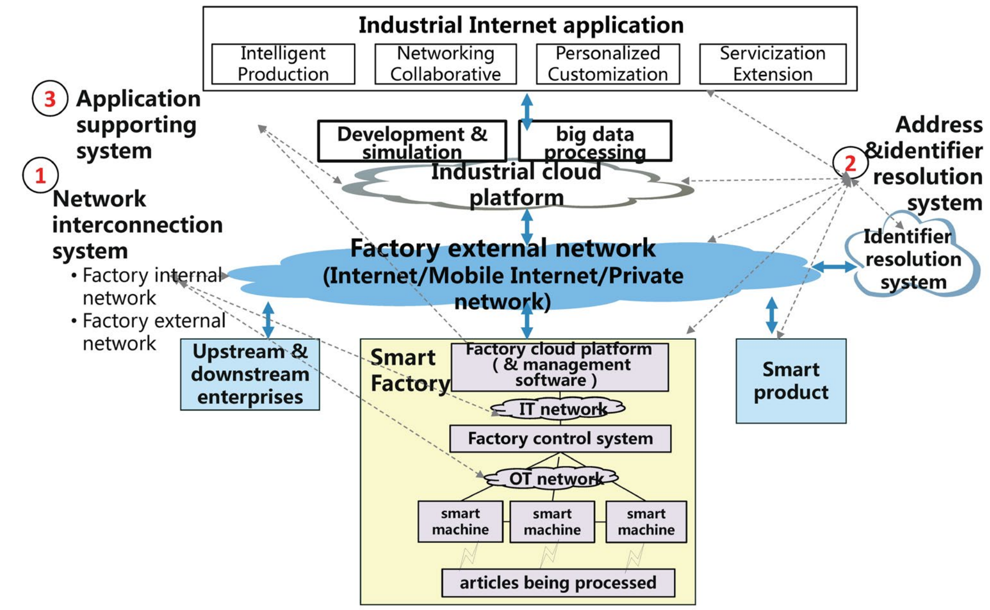

Figure 4 Target Framework of the Overall Network System of the Industrial Internet

Similar to the existing Internet which has three core systems, i.e., IP-based interconnection system, DNS system, and application service system, the industrial internet also consists of three main systems. First, network interconnection system, which refers to an industrial network system developed on the basis of IP-based reform of factory network and includes a factory internal network and a factory external network. The factory internal network is designed to connect articles in process, smart machines, industrial control system and human, further divided into a factory IT network and a factory OT (industrial manufacturing and control) network. The factory external network is used to connect the upstream and downstream of an enterprise, enterprise and intelligent products, as well as enterprise and users. Second, address and identifier system, which is a critical basic resource system consisting of network address resources, identifiers, and a resolution system. Similar to Internet domains, industrial internet identifiers are used to identify products, equipment, raw materials and other items. Therefore, the function of the industrial internet identifier resolution system is to resolve the items mentioned above. It translates the industrial internet identifiers into the items' communication addresses or addresses of their corresponding information servers, then finds the items or their relevant information. Third, application supporting system, which means the industrial internet's application interaction and supporting capabilities, which consists of an industrial cloud platform and a factory cloud platform, the service descriptions and application protocols of the resources they provide.

(II)Network Interconnection System of Industrial Internet

1. Factory internal network

(1) Status quo analysis

Factory internal network is a network that is used for connecting manufacturing factors and the IT system within a factory. In general, its structure has "two layers" ("factory OT network" and "factory IT network") and "three levels" (the network is divided into three levels in according to the current factory management architecture— "field level", "plant level", and "enterprise level" with the network configuration and management strategies of each level is independent from each other) as shown in Figure 5.

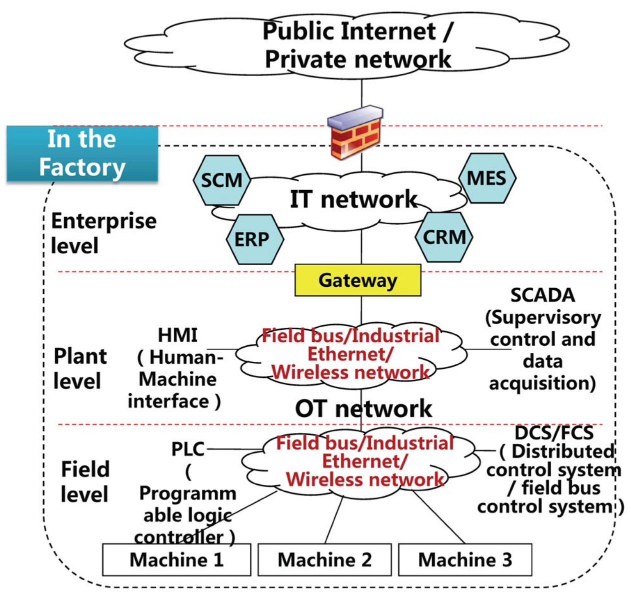

Figure 5 Status Quo of Factory Network Connection

The factory OT network mainly aims to connect devices such as controllers (PLC, DCS, FCS), sensors, servos and monitoring equipment at the manufacturing site, and its enabling technologies include the filed bus and industrial Ethernet. The factory IT network is composed of IP networks, and connected with and security separated from the Internet and factory OT network via gateway.

(2) Problem statements

The current two-layer and three-level technical system and separated network structure of the factory internal network lead to many obstacles for communication between the IT system and the manufacturing site: firstly, different technical standards of the industrial control network and the factory information network make them hard to be integrated and connected; secondly, it's urgent for the network to develop with full coverage as there are a lot of "information blind spots" in the whole industrial manufacturing process; thirdly, the static configuration and rigid organization of the factory network cannot satisfy users' future needs of customization and flexible manufacturing.

(3) Development trends

In order to adapt to the evolution of intelligent manufacturing, the factory internal network is developing towards flattening, IP-based, wireless and flexible networking.

Flattening development of factory internal network. It has two meanings. Firstly, with the development of smart machines and centralization of intelligent analysis, the factory OT system will gradually break down the layered networking model of field level and plant level, instead, achieving direct horizontal interconnection among the smart machines. Secondly, the whole factory management and control system will be flat via the partial functions integration of IT system and OT system (e.g. HMI), or via the industrial cloud platform, the real-time control function descend to be implemented by smart machines, so as to promote the IT and OT networks to be gradually integrated into a fully-connected network.

Ethernet/IP-based development of factory internal network. With the evolution of industrial network technologies, field bus is being replaced by industrial Ethernet gradually. In the future, the wired connection in industry will be dominated by a network with Ethernet physical interface. Meanwhile, various private industrial Ethernets will be gradually replaced by general standard-based industrial Ethernet. Moreover, the control data and information data will be transmitted through the same interface. The wide usage of Ethernet will make the IP trend of industrial internet more prominent that the IP technology will be extended to OT network, enabling IP to go throughout the IT network as well as OT network, and thereby making IT and OT nodes (machines) directly accessible. In this case, IPv6 will be widely applied in factories to solve the access problem for numerous IP-supported equipment.

Wireless network becomes an important supplement to the wired in the factory. Wireless technology is penetrating into the industry field, from information acquisition to manufacturing control and from partial plan to the whole-network plan. At present, the wireless technology is mainly used for information acquisition, non-real-time control and informatization within the factory. Wi-Fi, Zigbee, 2G/3G/LTE, WIA-PA, WirelessHART and ISA100.11a have been partially applied in factories. For industrial information acquisition and control scenarios featuring low power consumption, wide coverage and huge connectability, NB-IoT could be a better technical option recently. At the same time, wireless technology is gradually permeating the real-time industrial control sector, becoming a strong supplement or substitution for the existing wired industrial control network. For example, 5G has clearly included industrial control as one of its major application scenarios with low latency and high reliability; 3GPP has rolled out studies in terms of application scenarios, requirements and critical technologies; while IEC is developing WIA-FA technical standards.

Flexible networking for the factory internal network. In the future, manufacture systems can be flexibly restructured based on smart machines to realize flexible manufacturing. Smart machines can be migrated and switched among different manufacturing domains with plug and play capabilities. To achieve that, the factory network has to be flexible and the network layer resources can be orchestrated by a control node. Software defined network (SDN) is one of such ways to implement that.

(4) Target architecture

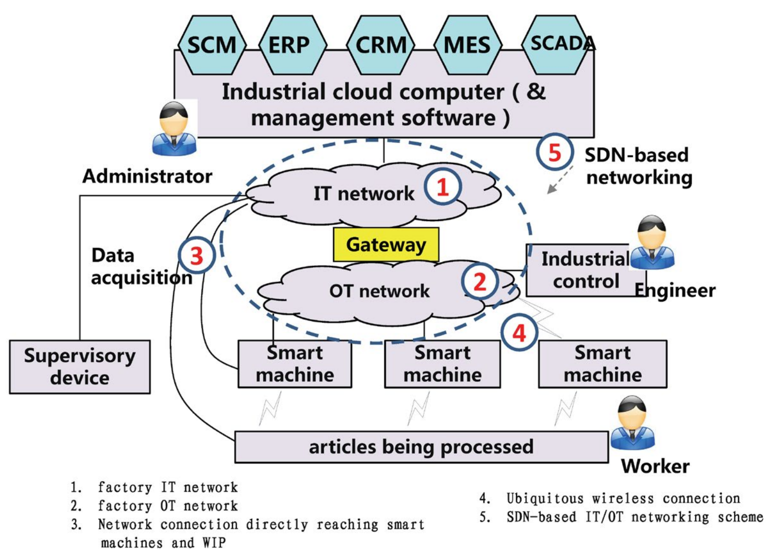

Figure 6 Target Architecture of Factory Internal Network

As shown in Figure 6, the factory internal network under the industrial internet scenario will consist of five major aspects. First, factory IT network. In order to be adapt to Internet development trends and to be convenient for the access of a large number of production and monitoring terminals, the IT network should be developed based on IPv6 or support the dual stack of IPv4/IPv6. Second, factory OT network. The industrial Ethernet will replace field bus step by step, achieving "Ethernet to the end". Besides, on the basis of Ethernet downward extension, smart machines, sensors and actuators will realize their IP-based or IPv6-based development. Third, Direct network connection to smart machines and article in process. Smart machines, sensors, article in process and other manufacturing site equipment and items will be able to directly connect to the IT network to realize real-time data acquisition of the manufacturing site. Fourth, ubiquitous wireless connection. The smart machines, article in process, sensors and transmission equipment on the manufacturing site will be able to be connected with various wireless technologies, such as Zigbee short-distance communication technology or Wi-Fi, LTE enhanced, NB-IoT, 5G and other wireless technologies according to equipment power consumption and transmission distances. Fifth, SDN-based IT/OT networking. The IT and OT networks can realize separation of the control plane and forwarding plane by employing the SDN technology; and dispatch network resources via SDN controller and manufacturing control system (e.g. MES) collaboration to support flexible manufacturing and production self-organization.

2. Factory external network

(1) Status quo analysis

Factory external network refers to the network that connects the upstream and downstream of industry chain, enterprise and intelligent products, enterprise and users with the aim to support the activities in the whole industrial life cycle. Currently, though a number of industrial enterprises have been connected to the public Internet, the value gained from the Internet is still limited. In terms of the connection way, the manufacturing and enterprise management processes are sealed within the factory so that the factory is like a "black box" from the viewpoint of the public Internet. In terms of the application approach, the integration of factory and Internet is mainly applied in sales and supply chain management links, therefore the resource optimization and allocation role of the Internet in the full industrial manufacturing life cycle has not been fully played.

(2) Problem statements

There are four main problems in bearing future industrial internet applications with the present IPv4 based public Internet. First, network performance. As the public Internet cannot guarantee the service quality, it cannot satisfy the requirements of a network with low latency, high reliability and qualified service after the integration of industrial manufacture and Internet. Second, network bearing capacity. As the existing public Internet is weak in business bearing and isolation, for example the number of VPNs is limited. It's difficult to meet the private line connection requirements of a large number of industrial enterprises. Third, network security threatening. The current Internet security capability needs to be improved with the further increase of requirements by industrial internet applications towards network security. Fourth, limited network address space. At present, the IPv4-based public Internet is facing exhaustion of address space, so it has a big problem in satisfying the access needs of tens of billions of terminals on the industrial internet.

(3) Development trends

With the development of networks, information technologies and business models, the industrial manufacturing process originally confined to factories are expanding to the external network gradually. The manufacturing information system and Internet are moving to deeper collaboration and integration, which includes integration of IT system and Internet, collaboration of OT system and Internet, integration of enterprise private network and Internet, as well as integration of product services and Internet.

The integration of the enterprise IT system and the Internet, from the network perspective, represents the outward extension of the factory internal IT network to the external network. The enterprise puts its IT system (e.g. ERP, CRM) under the hosting of a cloud service platform on the Internet or uses the enterprise IT software service provided by SaaS service providers.

The collaboration of the OT system and the Internet, from the network perspective, is the extension of partial OT system network to the external network. In situations where human power is hard to achieve while the manufacturing process needs to be adjusted and maintained, reliable Internet connection is needed for remote OT system control. The current Internet quality cannot bear the real-time control that has high requirements towards latency, jitter and reliability.

The integration of enterprise private network and the Internet will generate an independent network plane for the enterprise in the public network and can offer fast and flexible customization of bandwidth and service quality. However, such business scenarios require independent network resource controllability, open network programmable capability and customized network resources (e.g. bandwidth, service quality), which cannot be supported by existing Internet technologies. It needs the further development and deployment of network virtualization and software defined network technologies.

The integration of product services and the Internet will offer new product service models to industrial enterprises through the intelligent industrial products' information acquisition and network connection capabilities. Based on these platforms, the industrial enterprise could provide users extended services such as product monitoring and predictive maintenance, thereby extending the value chain of industrial manufacturing. However, the basis of such business lies on data acquisition and monitoring of massive products, which need wireless technologies to realize the ubiquitous access of industrial products.

With the needs of interconnection between factories and the public network being increasingly, the new requirements to the existing public network are also raised. First, support tens of billions of terminal accesses, as the number of connected industrial equipment and products will reach tens of billions. Second, support hundred-level application network plane. Considering the industrial site OT and IT applications as well as future business development, the application network plane required by

different qualities should be at the hundred-level. Third, support the segregation of millions of users. There're 500,000 to 600,000 industrial enterprises above designated size nationwide. If it is calculated based on 3~5 VPNs for each enterprise, the network's bearing capacity needs to reach the mega-level VPN. Fourth, provide whole-process service quality guarantee to satisfy the end-to-end network quality reliability requirements of different industrial internet applications. Fifth, provide network service orchestration capability. The network should support industrial users and users in other fields to make customization on network functions and protocols by open interfaces. Sixth, provide embedded security capability to realize endogenous security and network traceability so as to protect the security of critical applications.

The further integration of industry and external network will drive the development of customization, remote monitoring, intelligent product services and other brand-new manufacturing and service models. Therefore, the factory external network needs to be faster in speed, better in quality, lower in latency, safer and reliable, and flexible in networking. However, these requirements cannot be met with the current Internet. A series of new network technologies such as 5G, SDN and NFV need to be studied and deployed to support the development of industrial internet.

(4) Target architecture

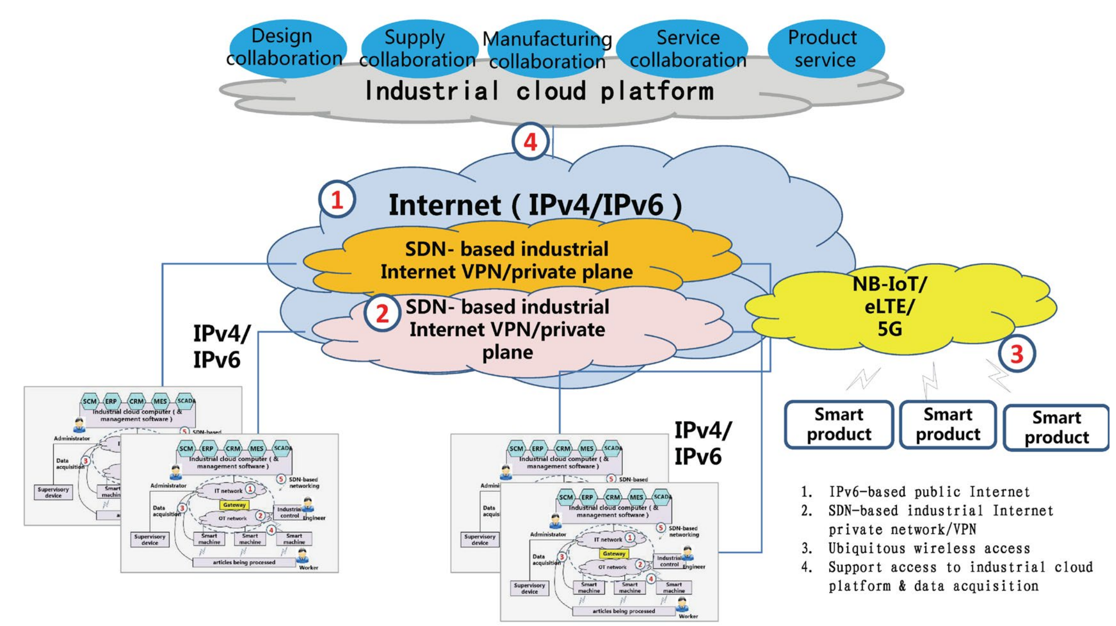

Figure 7 Target Architecture of Factory External Network

In the scenario of industrial internet, the factory external network will consist of four major aspects as shown in Figure 7. First, IPv6-based public Internet. As the industrial internet terminals will reach tens of billions, it's imperative to deploy IPv6 in the public Internet and take into consideration the transition from IPv4 to IPv6. Second, SDN-based industrial internet private network or VPN. For some businesses that have higher network quality requirements or are critical, they need to be carried by private network or VPN, where SDN and NFV are employed to separate businesses and data traffic, and to enable an open, programmable network. Third, ubiquitous wireless access, which means to use NB-IoT, LTE enhanced, and 5G etc., to achieve the wireless access of massive intelligent products. Fourth, support access to the industrial cloud platform and data acquisition. The factory external network supports the enterprise's information system, manufacturing control system, data transmission from various intelligent products to the industrial cloud platform and relevant service quality guarantee.

(III) Industrial Internet Addresses and Identifier Resolution System

1. Identifier and Identifier Resolution System

(1) Status quo analysis

The Identifier Resolution System (IRS) is to the industrial internet what Domain Name System (DNS) is to the current Internet, playing the role as the industrial internet's neural center. Similar to the domain name of the Internet, the identifier of the industrial internet is the critical basic resource to identify and manage things, information and machines. Similarly to the DNS for the Internet, the IRS for the industrial internet is the key infrastructure for interconnection and interoperability.

Currently, multiple different identifier encoding and resolution methods has been proposed and used at both home and abroad. In terms of identifier encoding, there is still no unified answer. Most small and medium enterprises (SME) choose to use self-defined private identifier in their factories, while few of them has begun to try to use public identifier in circulation node among different enterprises, such as supply chain management and product traceability. In terms of identifier resolution system, according to if it is based on the DNS, it can be divided into two development models: the modified path and the reform path. The modified path is still based on the present DNS, and accomplishes identifier resolution by adding some necessary modifications to DNS. For example, the Object Name System (ONS) proposed by GS1/EPCglobal for EPC is relatively mature. And most of the main international identifier resolution systems have set up branches in China through authorization, such as the OID registration center, and GS1 China. Meanwhile, some institutions in China are actively exploring other modified methods based on DNS, such as the NIOT plan proposed by Computer Network Information Center (CNIC) of the Chinese Academy of Sciences (CAS). These Chinese organizations build domestic identifier resolution systems by registrating

second level domains under China's top level domain ".CN". Besides, Bii Group has also carried out a root node expansion project—"Yeti DNS Project" based on IPv6 technology. On the contrary, the reform path takes different technologies apart from DNS, just like the Handle system. It employs multiple parallel roots to jointly manage and maintain the root zone files. Now, there has been 6 Multi-Primary Administrators (MPA) respectively in the USA, China, United Kingdom, Germany, Saudi Arabia and ITU. The Handle system can be both independent from and compatible with the existing DNS. Yet, some new technologies may also appear in the future.

For the moment, those systems have been deployed and formed a certain pattern in China, which can be compatible, communicate and co-exist with each other.

(2) Existed problems

In order to support the development of the industrial internet, the identifier resolution system faces some new requirements and challenges that cannot be fully satisfied at the moment. First, in the case of functions, since the objects in the industrial internet have complicated sources, diversified identifier forms that are hard to unify, it needs to support heterogeneous compatibility and effective scalability. Second, in the case of performance, as the industrial internet identifier data will be much more than the existing Internet identifier data, it requires the industrial internet identifier resolution system to be highly efficient and reliable. Especially for supporting the flexible manufacturing in factories, identifier resolution system must guarantee lower resolution latency for certain scenarios. Third, in the case of security, because the industrial internet identifier resolution system saves lots of data which is related to national and people's interests privacy, it needs to have capabilities including privacy protection, authentication, and anti-attack and attack traceability. Fourth, in the case of management and control, as identifiers are important basic resources of the industrial internet, which can reflect and be used for statistics and analysis of the industrial operation status, it needs a fairer and more equal governance modes. For now, it still needs further tests to determine if the existing main identifier resolution systems could satisfy the industrial internet's requirements in terms of functions, performance, security, and management and control.

(3) Development trends

The private closed-loop identifier resolution system is evolving towards public and open. In the past, the identifier technology is mainly being applied and promoted in asset management and logistics management. Now, it is penetrating into the production process. For example, the production line can automatically read the labels and identifiers of the goods in process to match corresponding treatment. The increasing needs for whole life cycle-oriented product management and trans-enterprise products information interaction will drive the docking between the enterprise identifier system and the public identifier resolution system. Accordingly, the identifier objects will gradually expand along with the development of the automatic identifier technology. Initially it will focus on product identifiers, and then expand to raw materials, software systems and other management objects and factors.

During certain period, several identifier resolution systems will co-exist. For now, the modified path and reform path have all been launched and formed a certain pattern at home and abroad. The existing identifier application deployment situation is impossible to break and the identifier resolution system is hard to be unified in a short term. .

Fairness and equality are also very important factors to be considering. The traditional Internet governance pattern has been maintained for a long time, and the centralized administration mechanism not only is easy to be attacked but also has an issue of control dispute. Now, both China and many other countries have put forward and started to deploy multiple new plans for identifier resolution systems. For example, ONS system has supported MONS architecture framework in its version 2.0, and Handle employs parallel root in initial design. They are commonly inclined to use a distributed multi-lateral management mechanism, and emphasize more on fairness and equality.

2. Industrial Internet Addresses

In order to support the access of massive smart machines and products, the industrial internet needs a large number of IP addresses. However, the IPv4 addresses are being exhausted and cannot meet the massive address requirement of industrial internet's future development. Therefore, IPv6 becomes the inevitable choice. Besides satisfying industrial internet's address requirements, it also can provide the globally unique addresses to devices in the factory internal network, facilitating better data exchange and information integration.

IPv6 technologies and management to be applied in industrial internet will become the research focuses. Although IPv6 has been studied for years, the industrial application has its own special features, particularly, the factory internal network has high-level requirements for security, reliability and network performance. For this reason, the technologies used for IPv6 and industrial internet integration need further in-depth studies. Furthermore, industrial production matters a lot to national interest and people's livelihood, early studies on allocation and management of IPv6 addresses in industrial internet can help the administrative authority to improve its Internet regulation level.

(IV) Industrial Internet Application Supporting System

(1) Status quo analysis

The industrial internet application supporting system consists of three parts: first, the application enabling technologies that achieve data integration among the industrial internet applications, systems and equipment; second, the industrial internet application service platform; and third, service-oriented encapsulation and integration.

The enabling technology for integration among industrial internet applications, systems and equipment is the basic protocol that supports data integration and interoperation within an industrial enterprise or between the industrial enterprises and the Internet data analysis platform. Similar to HTML and other Internet protocols, the industrial internet application enabling technology is used to achieve mutual "understanding" between heterogeneous systems (different operating systems, different hardware architectures, etc.) at the data layer, thereby realizing information integration and interoperation. OPC is one of the currently widely used inner-factory application enabling technologies, which defines a set of general data description and grammar expression methods (information models). Each system can organize its data information in the format of OPC, which then can be obtained and integrated by other systems.

The industrial internet application service platform mainly refers to a platform that can integrate and deploy various industrial cloud service capabilities and resources with an aim to perform online designing R&D, collaborative development and other industrial cloud computing services that are oriented to small and medium industrial enterprises. First, with the online integrated design cloud service, it can provide design resources and tool services to industrial enterprises. Second, with cloud platform-based new development approaches like multiparty collaboration and crowdsourcing design, the manufacturing resources can be efficiently integrated. Now there are some industrial cloud service platforms that can effectively collect and analyze manufacturing site data through the application enabling technology and use the results for enterprise management and decision making.

For the moment, the industrial enterprise service-oriented integration is mainly used in a factory's operation-level information system, where large enterprises organize resources from information systems like ERP, CRM and MES in SOA form via the enterprise service bus (ESB), to provide basic management support to enterprise operation. On such basis, the MES or SCADA system sinking toward factory/workshop generally falls into a database-focused interaction model with preset development of business logic while the SOA-based service resources dispatching still cannot be achieved for equipment, materials and other manufacturing resources at the bottom layer.

(2) Problem statements

At present, the industrial internet application supporting system is still in its initial development stage and has three problems. The first is related to industrial cloud platform's standardization and regulation. Since there are lack of relevant standards and regulations for industrial cloud platform, enterprises may hesitate and have some considerations in terms of cloud service providers' business bundling, data migration and data security. The second is related to the application enabling technology's universality. Although OPC has been widely applied in factories and solved the information interaction and integration issue between equipment and systems to some extent, OPC just regulates the reading and writing formats, and has no structured and modeled regulation representations. Therefore, for up layer application systems, it is still an independent I/O variable or function. The system integration and business logic are complicated. Third, its service-oriented development needs further exploration. The enterprise-level information systems have been able to achieve SOA-based integration, but the manufacturing control layer is still based on customized protocol and logic. So it's difficult to organize and design services fast. Besides, it needs further exploration as to how to realize Internet service-based development of the businesses and data within manufacture enterprises.

(3) Development trends

Cloud computing is gradually applied to factory internal and external. First, build factory private cloud and public cloud based on the IaaS model. Cloud computing provides a more efficient, low-cost and scalable way for industrial enterprises IT development. With IaaS, the smooth migration from systems to the cloud end can be accomplished without making a big change to the existing enterprise IT architecture. Some large enterprises can build its own private cloud platform or use the hybrid cloud model to take full advantage of the public cloud. For small and medium enterprises, they are more likely to use the public cloud to improve their IT building capability. Second, develop new industrial application models on the basis of PaaS platform. With powerful computing and storage capabilities at the back end and easy-to-use REST interface at the front end for fast application construction, the PaaS platform can satisfy the industrial enterprises' requirements of predictive maintenance and other innovative applications in terms of rapid development and deployment. Facing industrial internet's application requirements, the traditional PaaS platform has to be able to collect data from various links including design, manufacture and supply, to build special analysis models oriented to the industrial fields at the cloud end, as well as to have the general application supporting capability. Third, provide IT application services directly to enterprises via the SaaS platform. Now, some vendors have already provided SaaS in the fields of enterprise management and collaborative R&D. With the development of industrial internet, the industry-oriented SaaS service will be diversified and develop into a whole-process application product that covers R&D design, collaborative manufacturing, enterprise management and product services. Small and medium enterprises can develop diversified applications covering the whole life cycle in a rapid way with the SaaS service.

The application enabling technology reflects different trends inside and outside of the factory. First, data integration protocol between different systems in the factory. Within the factory, the data integration protocol represented by OPC-UA will be applied more widely, becoming the "data bus" that connects the manufacture equipment and the IT system, to solve the problem of unable to be "understood" and treated by other systems due to different data formats and models from multiple manufacturing control systems, IT systems and manufacturers. Second, data integration protocol between the industrial equipment,

products and the cloud platform. The data integration protocol between the industrial equipment, products and the cloud platform will form a protocol set focusing on open standards. In order to fully analyze and utilize the data from process like product manufacturing, utilization and maintenance, as well as maximize the value of manufacture and product data, it needs to transform the heterogeneous data from manufacturing sites and intelligent products into information that is in a unified model via the gateway or through switching the message-oriented middleware, and send such information to the cloud end for centralized analysis and processing. Currently, there are many protocol types that can accomplish application data integration from the manufacturing site to the cloud end, such as the MQTT and AMQP of OASIS, as well as the CoAP and XMPP of IETF.

Service-oriented encapsulation and integration becomes a major means to collaborate heterogeneous applications, systems and equipment. Accompanying the development of the industrial internet, all kinds of intelligent equipment, control systems, information systems and intelligent products will be connected and collaborative within the factory and the whole Internet. By encapsulating the functions of those devices and systems as services, for example transforming the manufacturing equipment from traditional data sources to reconfigurable service units via servitization, the businesses and application system development processes can be simplified, which is becoming an important development orientation. Among others, the semantics-based service-oriented encapsulation can effectively solve the abstraction and recognizable problem of the heterogeneous devices and systems. For this reason, it has received active promotion by the industry.

(4) Target architecture

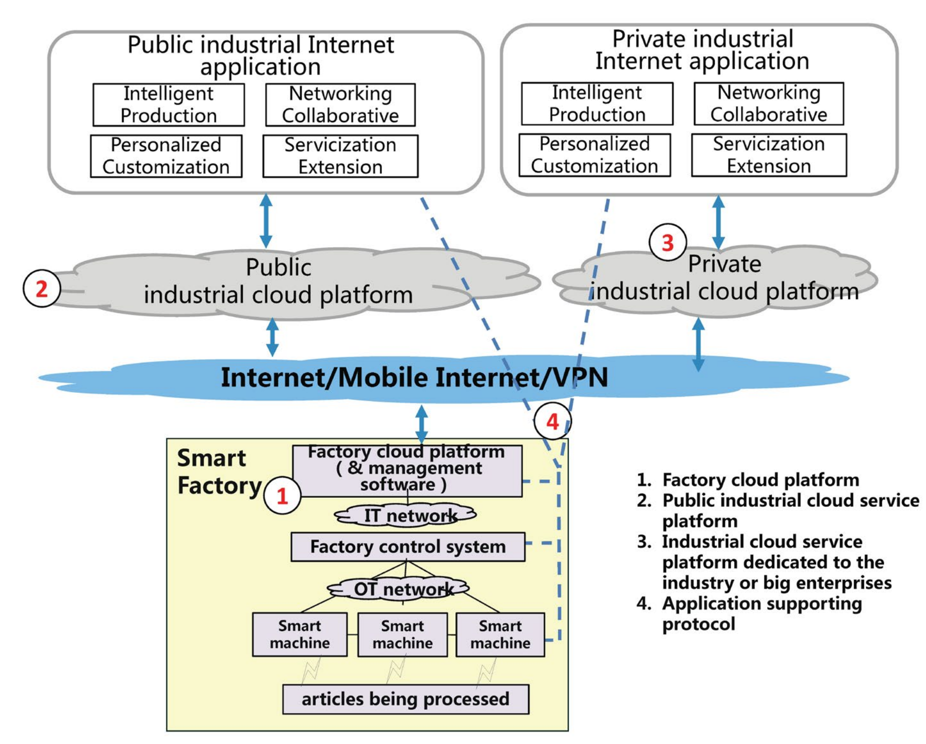

Figure 8 Industrial Internet Application Supporting System

The application supporting system under the industrial internet scenario will consist of four main links as shown in Figure 8. First, the factory cloud platform. Build private cloud platforms within large enterprises to facilitate the centralized IT system construction and perform data analysis and operation optimization in the enterprises/factories through standard data integration. The hybrid cloud is an alternative model, through which to transplant part of the data capacities and information systems to the public cloud platform to achieve Internet-based information sharing and service collaboration. Second, the public industrial cloud service platform. Implement new industrial internet application models such as design collaboration, supply chain collaboration, manufacturing collaboration and service collaboration for small and medium industrial enterprises and provide SaaS services. Third, the private industrial cloud service platform oriented to the industry or large enterprises. It means to provide industrial data analysis-based private cloud computing service to large enterprises or special industries. Fourth, the data integration protocol among the manufacturing devices, control systems and IT systems in the factory, together with the data integration and transmission protocols among the manufacturing devices, IT systems and factory external cloud platforms.

IV. Data System of Industrial Internet

(I) Definition and Characteristics of Industrial Big Data

Industrial big data refers to the data generated from information application in industrial fields, which is the core of Industrial Internet development. Industrial big data generated throughout the product design phase, production phase, management phase and service phase of industry. Industrial big data analytics equips the industrial system with intelligent functions including description, diagnostics, prediction, decision making and control.

Industrial big data can be divided into three types, i.e. onsite equipment data, production management data and external data. Onsite equipment data comes from industrial production line equipment, machines and products and they are mostly collected by sensors, devices and instruments, as well as the industrial control system, including equipment's operation data and production environment data. Production management data generated by traditional information management systems, such as SCM, CRM, ERP and MES. And external data, which includes information and data from Internet market, environment, customers, governments, supply chains and other factory external environment.

Industrial big data has five features. First, huge data volume. With the continuous influx of massive machines' high frequency data and Internet data, the data set of large industrial enterprises will reach the level of PB even EB. Second, wide distribution of data in links such as machines and equipment, industrial products, management systems and Internet. Third, complicated structures as there are structured and semi-structured sensor data as well as unstructured data. Fourth, diversified data processing speed requirements. At the production site level, it requires the real-time analysis to reach milliseconds. And the management and decision-making applications are required to support interactive or batch data analysis. Fifth, high confidence of industrial big data analysis is usually required. Correlation analysis is not sufficient in many industrial scenarios such as failure diagnostics, predictive warning and other industrial applications. It requires to combine the physical model and data model, to track and dig out the causal relationship.

(II) Functional Architecture of Industrial Internet Big Data

From the function perspective, the industrial internet's big data architecture consists of four layers and five parts as shown in Figure 9, which are data acquisition and exchange, data pre-processing and storage, data modeling, data analysis, and the data driven decision-making and control applications.

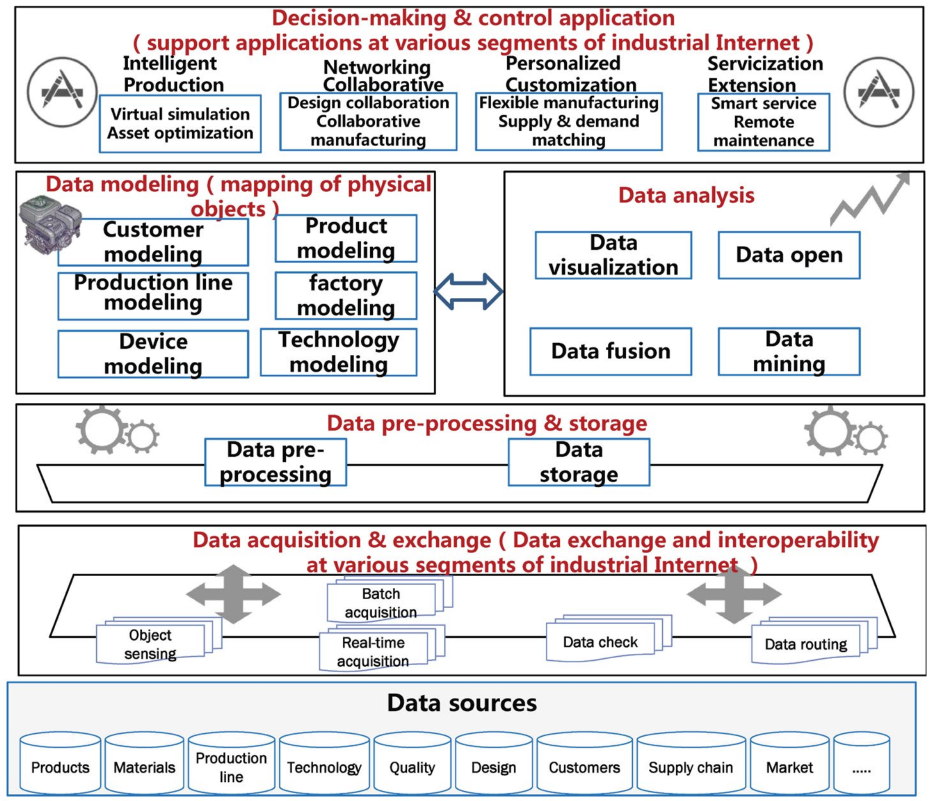

Figure 9 Reference Architecture of Industrial Internet Data System

The Data Acquisition and eXchange (DAX) layer is mainly designed for collecting and exchanging data of each industrial link. The data sources include both internal system data from sensors, SCADA, MES and ERP, and enterprise external data. Its functions are object sensing, real-time collection and batch collection, data verification, and data routing.

The key target of Data Pre-processing and Storage (DPS) layer is to complete the initial cleansing and integration of industrial internet data, and correlate the industrial system with the data objects. Its main functions include data pre-processing and data storage.

The Data Modeling (DM) layer aims to build digital models for users, equipment, products, production lines, factories and techniques. These digital models attach to the actual physical elements and business processes to reflect the real industrial system. At the same time, DM layer offers data description, data fusion, data analytic tools, visualization and opening data functions in combination with the data analysis layer so as to support various applications.

The Decision-making And Control application(DAC) layer is mainly used to produce different applications like description, diagnostics, prediction, decision-making and control based on data analysis results, thereby generating optimized suggestions for decision making or direct control commands, and building up innovative models such as intelligent production, networking collaborative, personalized customization and servicization extension. At the same time, store the results as data and finally we can establish a continuously optimizing closed loop for the production lifecycle.

(III) Industrial Internet Big Data Application Scenarios

The industrial big data application covers the whole process of industrial production and the whole lifecycle of a product. Its roles are mainly played in the aspects of status description, diagnostics and analysis, prediction and warning, as well as assistance in decision making. It functions as the core driving force in four scenarios: intelligent production, networking collaborative, personalized customization and servicization extension. Figure 10 shows the applications of industrial big data technologies.

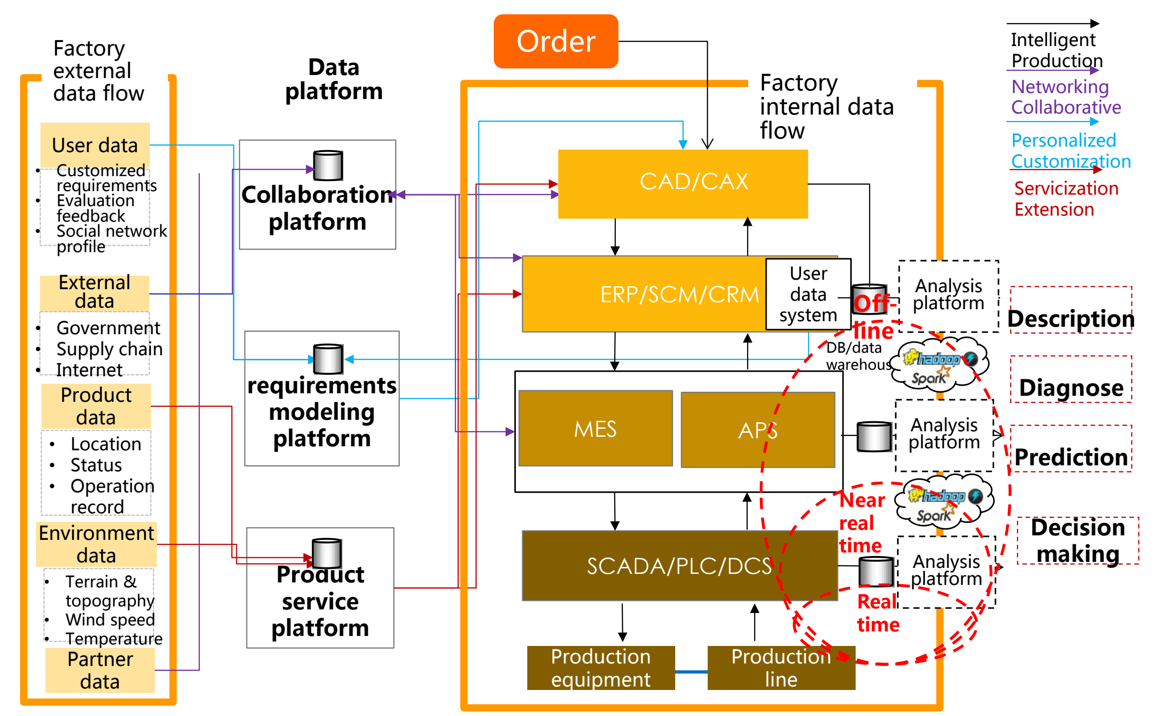

Figure 10 Industrial Internet Big Data Technology Application Diagram

(1) Industrial big data application in intelligent production

Virtual design and manufacturing. It refers to combining the big data technology with CAD, CAE, CAM and other design tools and building a design resource model library and a historical experience model library by deeply learning about the historical technique process data, finding out the models and relations among product plans, technique processes, factory layouts and investment, as well as summarizing and analyzing the isolated data in the past, in order to optimize product design, technique planning, factory layout plans and shorten products' R&D periods.

Production technique and process optimization. It refers to using the big data analysis function to evaluate and improve the current operation and technique processes, warn the cases that deviate standard technique processes, and identify errors or bottlenecks in a fast way, so as to rapidly optimize and adjust the technique processes in production.

Predictive equipment maintenance. It means to build a big data platform where the data, in terms of equipment vibration, temperature, pressure, and flow, collected from the onsite equipment status monitoring system and the real-time database system, are stored and managed. Then perform equipment failure prediction and diagnostics through data analysis and by building models such as rules and cases-based failure diagnostics, equipment deterioration trend prediction and parts' remaining lives prediction.

Intelligent production scheduling. It refers to developing preplanned production schedules, and dynamically changing the planned schedule by monitoring the differences between the planned and the actual situations. In order to achieve this, it needs to collect data in terms of customer orders, production lines and staff, discover the deviation probability between the historical predictions and the reality with big data technology, take into consideration restrictions in capacity, staff skills, materials availability, and tools and tooling, as well as employ intelligent optimization algorithms.

Product quality optimization. It means to trace the whole production processes for products with quality defects, and find out the reasons rapidly by collecting the real-time and historical data of production lines and products and building big data models based on previous experiences, so as to improve production and optimize products' qualities.

Energy consumption control. It refers to the real-time monitoring of energy consumption & emission in the critical links as well as the assistive transmission and distribution link; collection of data related to production lines and energy consumption of the critical links; building of a simulated energy consumption model and conducting multi-dimensional predictive analysis based on consumption model simulation to obtain energy-saving spatial data of each link on the production line; collaborative operation of intelligent optimization to balance the loading and energy consumption, thereby realizing the flexible energy conservation and emission reduction on the production line in general, timely noticing abnormal or peak situations in energy consumption, and achieving real-time optimization of energy consumption in the production process.

(2) Industrial big data application in network-based collaboration

Collaborative R&D and manufacturing. Generally, it can integrate the design tools library, model library, knowledge library and manufacturing enterprises' production capacity information into one based on a unified design platform and a manufacturing resource information platform. Enterprises or branches in different regions can obtain the same design data through accessing the design platform via the industrial internet networks. Moreover, they also can obtain the idle production capacity of the peer manufacturing enterprises. In this way, the allopatric collaborative design and manufacturing requirements can be satisfied with multi-site collaboration, multi-task running in parallel and multi-corporate cooperation.

Supply chain distribution system optimization. The process is like this: first, use RFID product electronic labelling, IoT and mobile Internet technologies to acquire the big data of the complete product supply chain including the data of suppliers, inventories, logistics, production and sales; then use the data for analysis and determine the quantity of materials purchased and their delivery time, thereby optimizing the supply chain.

(3) Industrial big data application in customization

User needs mining. It refers to building a system to analyze users' needs towards goods, dig out their in-depth requirements and develop a scientific analysis system for goods production plans. Then combine users' needs and production to produce production plans for various products satisfying consumers' expectations and make predictive judgements about the market.

Customized production. It means to build individualized product models by collecting data related to customers' individualized requirements, industrial enterprises' production, and external environment; send product plans, materials lists, and technical plans to the production site quickly via the manufacturing implementation system; and adjust the production lines and prepare the materials needed so as to produce customized products meeting the individualized needs in a fast way.

(4) Industrial big data application in service-oriented extension

Remote product services. It refers to collecting data of diversified intelligent products such as intelligent equipment, smart home, wearables and intelligent connected cars by building a data platform for corporate products; then developing models for predictive analysis of products performances, providing remote monitoring, diagnostics, and operation & maintenance services to those intelligent products, creating new values for them, and accomplishing manufacturing enterprises' service-oriented transformation.

(IV)Challenges

The main challenges for industrial big data application are as the following. First, bad corporate data source. Especially for machines, equipment, production lines and other real-time production data, there is large improvement space in terms of data acquisition quantity, type, precision and frequency.

Second, it's prevalent for information isolation between enterprises and between different departments within a same enterprise. Data is difficult to make interaction, be shared or integrated, and the application value of data integration is also hard to be effectively exploited.

Third, currently there are lack of mature application models or successful projects for industrial big data application. Although some leading enterprises are on trial in this aspect, most of those projects are in the proof of concept stage. Industrial big data application in production environment is still rare. There is a long way ahead to promote big data analytics in industrial internet.

Fourth, the core technologies, software platform products, system integration and application development capabilities for industrial big data still need to be strengthened and improved. The security controllability is not enough as well.

(V)Development Trends

With the deepening of industrial internet development and application, the value and role of data will be more and more important, enabling data analysis to penetrate into all industrial links; more intelligent application including prediction, decision making and control will be the orientations; and finally a closed loop from data acquisition, through equipment, production sites to enterprise operation and management will be formed.

In future, the industrial data will develop towards the following directions. First, cross-level and cross-domain data integration. Currently, the industrial data is distributed in links including R&D design, production management and corporate operation horizontally, and in levels like production site and enterprise management (MES, ERP) vertically. In the next stage, the data in the horizontal and vertical directions will be integrated to lay a data foundation for overall view analysis. What is worth mentioning is that the semantic technology will play a great role, with which the industrial internet data meaning can be labeled so that the data can be understood correctly and processed between heterogeneous systems.

Second, intelligent processing of data on the edge. On the network edge nodes close to the data source, edge processing, analysis and filtration of data will be realized through functions such as integrated computing, storage and control, to meet the needs of real-time connection, real-time control, real-time analysis, security and privacy of the industrial production sites as well as to complement with the cloud platform.

Third, cloud platform-based data integration and management. Gathering the data together and upload it to the cloud computing platform for analysis and processing is a mainstream direction. Use mature, proved technologies and big data platform to support industrial data modeling, ETL, inquiry and computing to apply with traditional real-time database, relational database and MPP data is a major direction for the building of a cloud-based industrial big data platform.

Fourth, depth data analysis and mining. The knowledge-driven analysis approach is developed on the basis of industrial system physical/chemical principles, techniques, management experience and other knowledge. On the contrary, the data-driven analysis approach looks for laws and knowledge completely in the data space via algorithms. But in future, in most cases, the two approaches will be integrated to meet the industrial data analysis requirement of a high confidence coefficient.

Fifth, data visualization. Build simulated digital models for machines, production processes and the whole production cycle and visualize them in order to help the production managers, system developers and users to learn about relevant information in a more direct and comprehensive way, and to support the decision-making levels in links such as design, production, product circulation and transaction, and product services.

V. Security System of Industrial Internet

(I) Security Framework of Industrial Internet

The industrial internet's security requirements can be analyzed from two perspectives: industry and internet. From the perspective of industry, the security mainly refers to guaranteeing the continuity and reliability of intelligent production, focusing on the security of intelligent equipment, industrial control devices and systems. From the perspective of internet, security mainly refers to ensuring the running of customization, network-based collaboration, service-oriented extension and other industrial internet applications so as to provide continuous service capability and prevent the leakage of important data, focusing on industrial application security, network security, industrial data security and service security of intelligent products. Therefore, considering the construction of an industrial internet security system, the industrial internet security system framework should consist of five parts as shown in Figure 11: device security, network security, control security, application security and data security.

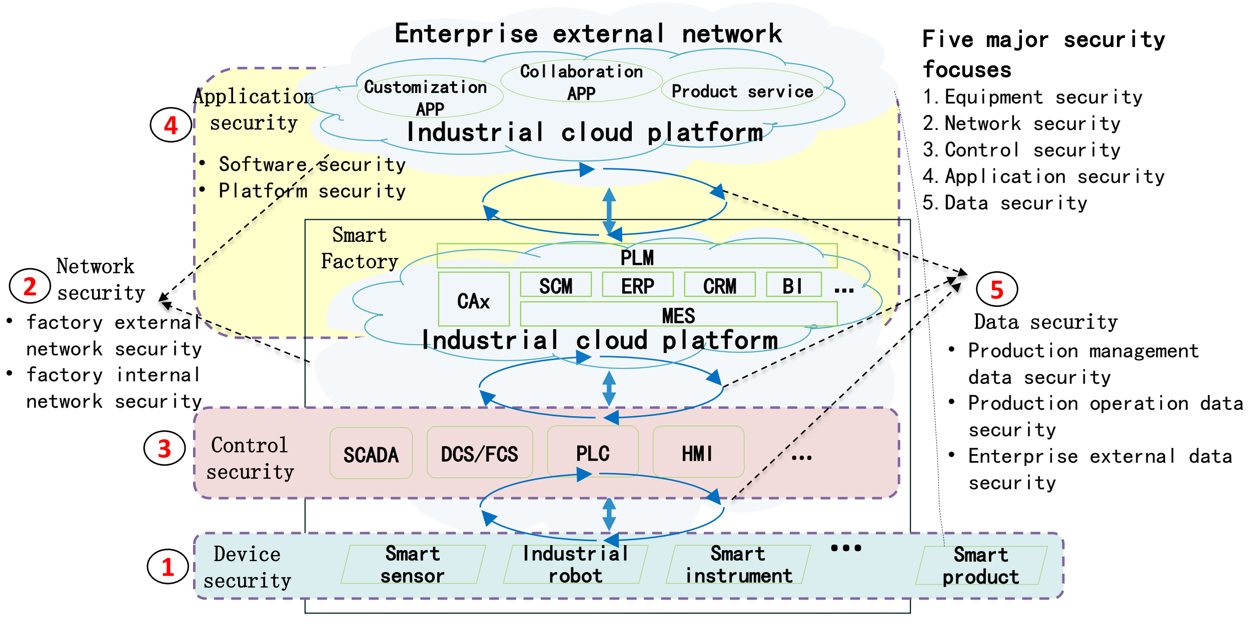

Figure 11 Industrial Internet Security System

Device security refers to the security of industrial intelligent devices and products, including chip security, embedded operating system security, related software security and safety. Network security refers to the security of wired and wireless networks in the factory, as well as that of the public network that is connected with users and collaborative enterprises outside of the factory. Control security refers to production control security, including control protocol security, control platform security, control software security, etc. Application security refers to the security of the application software and platform that supports the operation of industrial internet businesses. Data security refers to the security of important production management and production operation data in the factory as well as the external data (e.g. user data).

(II)Current Status Analysis

Driven by the integration and innovation of Internet and industry, electricity, traffic, municipal engineering and other critical information infrastructures that are related with national interests and people's livelihoods are increasingly dependent on networks and connected to the public Internet. Once a network attack is staged, it will not only cause huge economic losses, but generate environmental disasters and casualties, threatening public lives and state security. Hence, the security assurance capacity has become a key factor influencing the innovative development of industrial internet. In general, different information and automation levels lead to different development situations of security assurance systems in the subdivided industrial fields. For industries with higher information and automation levels, their openness levels are relative higher as well, so do the security risks they face. Therefore, they're likely to pay more attention to security and have relatively more perfect security assurance systems.

For now, the security protection in industrial fields is guided by security isolation with different layers and regions, and border protection. Usually, isolation and border protection measures are deployed between the factory internal network and external network. For example, use firewall, VPN, access control and other border protection means to guarantee the security of the factory internal network, which can be further divided into a corporate management layer (that is constituted of corporate management related systems such as ERP and CRM) and a production control layer (that is composed of work stations like engineer station and operator station, as well as PLC, DCS and other control equipment). Similar to traditional IT systems, the corporate management layer focuses on information security by employing traditional information system security protection measures like authority management and access control, deploying industrial firewall, gatekeeper and other isolation devices between it and the production control layer, and filtering OPC and other industrial protocols with a white list to prevent threats from the Internet penetrating into the production process. The production control layer is closely related with the production process, requires high reliability and instantaneity, and focuses on functional safety. For this reason, despite the fact that most of the engineer stations and operator stations use win2000/XP operating systems, considering system stability and their influences on functional safety, those systems are rarely upgraded or patched, and normally without anti-virus software. Meanwhile, in order to avoid negative impacts on functional safety, isolation devices are seldom deployed between the work stations and the control equipment. Because the traditional production control layer is mainly protected via physical isolation and the information security risk is low; as there are various private industrial protocols, the isolation devices like the industrial firewall needs to be designed based on the specific protocol; and enterprises pay more attention to the normal proceeding of the production process. In addition, at the initial designing stage, the control protocols and software lack security functions such as certification, authorization and encryption. The shortage of security assurance measures at the production control layer is a significant security issue during the evolution of industrial internet.

In general, the community is actively promoting the application of industrial firewall, industrial security monitoring and auditing, security management and other security products. But the overall research of and industrial support to industrial internet security is still in its initial stage, and the existing measures cannot effectively deal with the increasingly complicated security problems during the development of industrial internet. From the perspective of industrial internet's future evolution, guaranteeing the security of industrial network infrastructure, control system, industrial data and personal privacy, intelligent equipment as well as industrial applications is a key point for future development.

(III)Existed Problems

With the integrated innovative industrial development and continuous evolution of industrial internet, the factory environment will be more open, which will also bring some problems to future industrial internet security as the following. First, device security. Most of the traditional production device are machines focusing on physical and functional safety. Yet, the future production device and products will be increasingly integrated with general embedded operating systems and application software, which will directly expose the massive devices under network attacks. The spreading speed of Trojans and viruses among devices will see an exponential growth. Second, network security. Factory network will develop toward "three orientations (IP, flat, wireless) + flexible networking" and face more security challenges. The existing means to attack TCP/IP protocols are mature

enough to be directly used to attack the factory networks. The flexible networking requirement makes network topologies more complicated. Traditional static protection strategies and security domain division methods are challenged for dynamic and flexibility. In applying the wireless technology, it needs to satisfy factory requirements of instantaneity and reliability, and complex security mechanisms are hard to be implemented. Thus, it is easy to be attacked by illegal invasion, information leaking and denial of service. Third, control security. The current industrial control system focuses on the functional of the control process and its information security defense capacity is not sufficient. At the beginning of design, the existing control protocol and software are based on two premises: relative isolation between IT and OT, and relative reliability of OT environment. Besides, as factory control has high requirements on instantaneity and reliability, the information security functions needing additional operations such as certification, authorization and encryption are discarded. The IT-OT integration breaks the traditional security and reliable control environment, with which network attacks can penetrate from the IT layer to the OT layer, from factory external to internal. However, there are no effective APT attack detection and protection methods. Fourth, application security. New models and businesses like network-based collaboration, service-oriented extension and customization put forward higher requirements toward the security of traditional public Internet. With industrial applications being complicated and security requirements diversified, the requirements on network security in terms of segregation and protection capabilities should be elevated as well. Fifth, data security. The industrial data is switching from few, single and one-way to abundant, multi-dimensional and dual-way. In specific, it is represented as massive, diversified and complicated industrial internet, flowing and shared between the IT and OT layers, and between the factory internal and external. The complicated industrial business applications, diversified data types and protection needs, together with complex data flowing directions and paths, have increased the difficulty in protecting important industrial data and user data.

(IV)Development Trends

The following contents will be the ones receiving most attention and promotion with the evolution of industrial internet. First, facility embedded security mechanism. With the production equipment transforming from mechanized to highly intelligent, embedded security mechanism will become the breakthrough point for guaranteeing the security of future equipment, providing embedded security capability through security chips, security firmware, trusted computing, etc. to protect the equipment from unauthorized control or functional safety failure. Second, dynamic network security defense mechanism. Dynamically change security strategies and security domains in the light of flexible networking requirement for security defense. At the same time, add other security mechanisms such as lightweight certification and encryption to protect the transmission security of the wireless network. Third, information security-functional safety integration mechanism. With the factory control environment changing from closed to open, information security threats may directly cause failed functional safety. Considering the correlationship between functional safety and information security, the future factory control security should take into consideration their requirements in a comprehensive way and generate integrated security assurance capability. Fourth, industrial application-oriented flexible security assurance capability. As business applications are diversifying, in future, it should provide flexible security service capabilities based on the security needs of different businesses, including unified but flexible certification, authorization and auditing and supporting mega-level VPN segregation and user quantity growth. Fifth, classified and hierarchical protection mechanism of industrial data and user data. Classify and grade important industrial data and user data and protect them in a hierarchical way with different technologies. Also, monitor and audit the data flowing process with data labeling and signature technologies to achieve the whole life cycle protection of the industrial data.

VI. Implementation of Industrial Internet

(I) Status Quo and Implementation Targets of Industrial System

At present stage, digitalized and networked foundation for industrial system has been established to some extent, but compared with industrial internet visions such as ubiquitous interconnection, full life cycle digital chain, etc. there is still plenty of room for transformation and enhancement in terms of network, data and security. The implementation architecture of industrial system at this stage is shown in Figure 12. As to network interconnection, the network hierarchies of industrial system are complicated with the co-existence of multiple networking technologies including field bus, industrial Ethernet and ordinary Ethernet and wired network is used mainly, the interconnection of industrial system with outside world is very limited. As to data intelligence, data of different levels are relatively isolated, data collection by underlying devices are very limited, data integration among different systems are difficult, and technologies such as cloud and big data have not yet been applied efficiently. As to security control, it is mainly applied to satisfy the security requirements of existing industrial system, and more attentions are given to safety.,

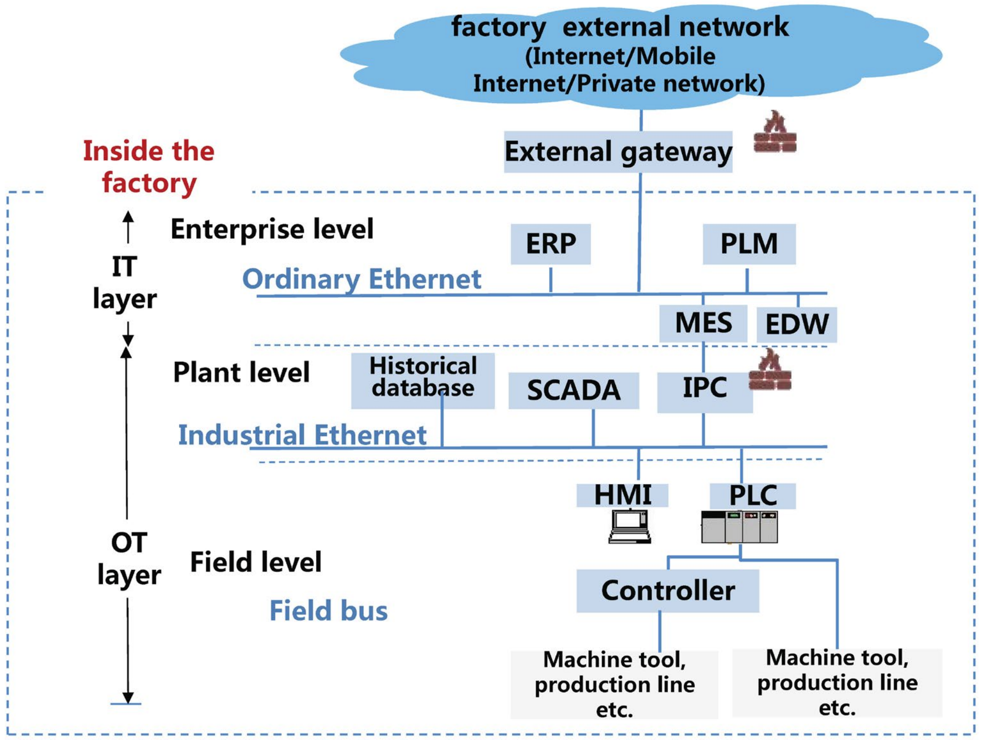

Figure 12 Current Industrial System Implementation Architecture

In the context of industrial internet, industrial system will experience rapid iterative evolution in terms of network interconnection, data intelligence and security control. With the gradual introduction of technologies such as cloud and big data, the flat deployment architecture of software and hardware has become the important development trend, leading to profound changes of network, data and security at all layers of industrial system. With the combination of the development trends of network, data and security of industrial internet, this report has provided an industrial internet target implementation architecture as shown in Figure 13.

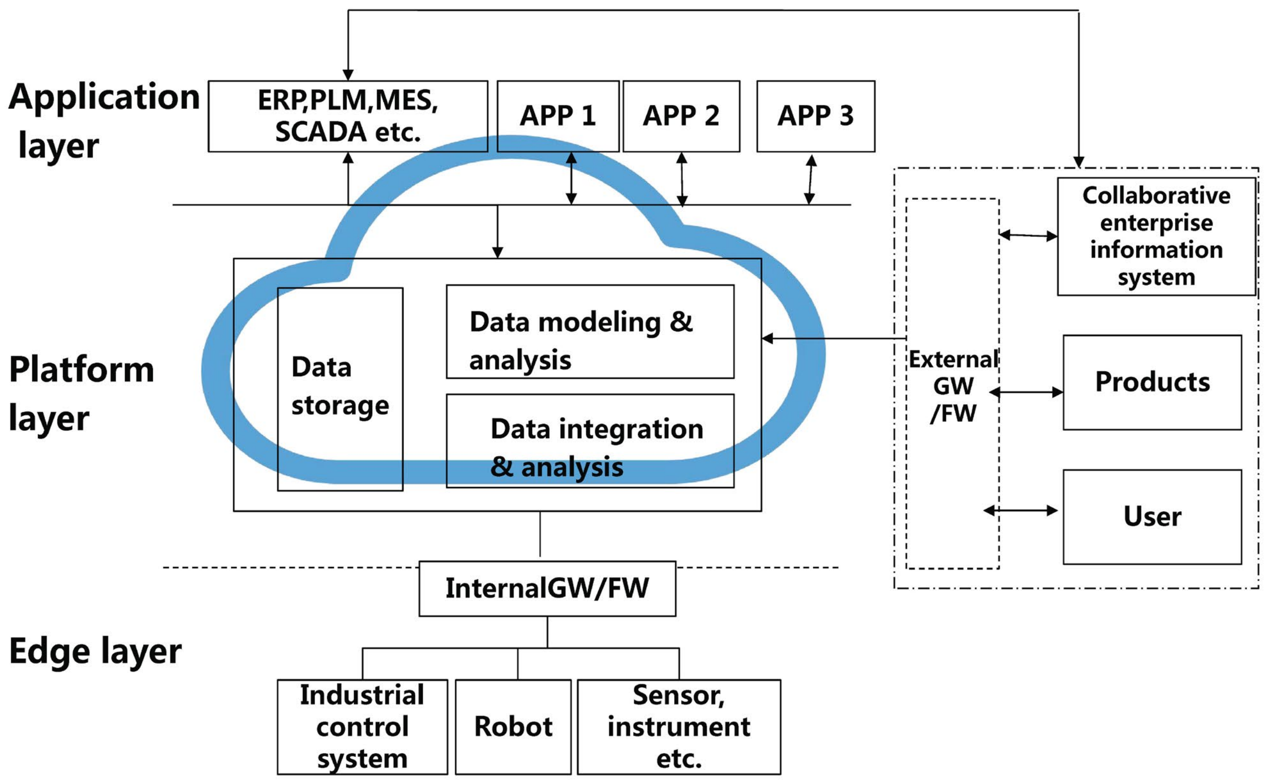

Figure 13 Target Implementation Architecture of Industrial Internet

Industrial internet target implementation architecture mainly displays four key features. First, as to system architecture, each layer will fully interconnect, and the internal and external networks will be integrated, and the traditional multi-layer architecture of industrial system will gradually evolve towards a flat architecture consisting of three layers, namely application layer, platform layer and edge layer. Second, as to network interconnection, various smart devices will become networked, wireless technology will become important complement to wired technology, new gateway will promote heterogeneous network interconnection and protocol conversion, as well as full connection will be realized between factories, products, external information systems and users. Third, as to data intelligence, industry cloud platform will become the key core, realizing full aggregation of data from outside and inside of the factory, supporting the storage, mining and analysis of data, and effectively supporting the industrial information control system and various innovative applications. Fourth, as to security control, with the in-depth integration of a variety of security mechanisms with each layer of industrial internet, defense in depth and dimensional protection are achieved, and the security of network interconnection and data integration are protected through multiple s security measures. It will take a long time to realize industrial internet target architecture, which requires synergy of many aspects including network, data and security.

(II)Implementation of Industrial Internet

(1) Implementation of network interconnection

The implementation of network interconnection mainly aims to address the interconnection and intercommunication issues between different devices and systems of industrial internet, involving the interconnection among work cell, work center and enterprise devices and systems, as well as different interconnected scenarios between enterprise information system, products, users and cloud platforms. To the current industrial system, it involves the networked transformation of existing industrial system including existing devices and systems together with the building of new type of network connection. Main factors involved in the implementation of network interconnection are shown below in Figure 14.

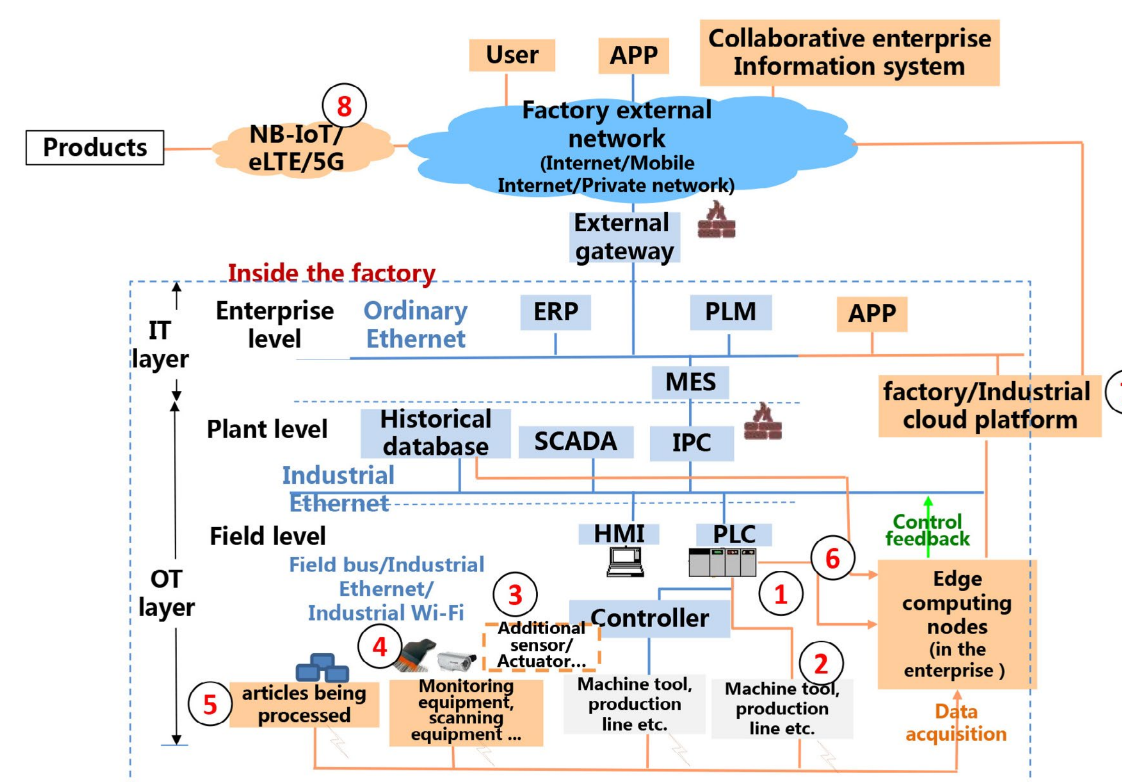

Figure 14 Implementation of Network Interconnection

At work cell and work center, it mainly realizes the lateral connection of underlying devices and their vertical intercommunication with upper-level system. First, transforming the communication methods between controller with CNC and product line etc. For example, industrial Ethernet is used to replace field bus. Second, add network interfaces to existing industrial devices or plants such as CNC and product lines. Third, add sensors and actuators to existing devices or plants to increase information interaction with the outside world. Fourth, deploy new monitoring devices, scanning devices and executors to collect work cell information or conduct feedback control. Fifth, increase information interaction functions with industrial system by means of embedding communication module or attaching tags to articles being processed. Sixth, deploy edge computing nodes to collect production work cell data and industrial control system data such as PLC and historical database data, and conduct edge processing of data. The specific networking methods will combine with communication requirements, arrangement of wire, power supply and other factors, with full consideration of IP-based and wireless-based trends. For example, for articles being processed, the short-distance communication technology, and identifier technology, such as buletooth, two bar code, RFID etc. could be applied; For production devices or equipment, the existing networking methods could be used directly, and more networking interfaces could be added using industrial Ethernet and industrial wireless technolgy; For monitoring devices, if there is not high requirements for real time, then cable broadband communication, wireless broadband, LTE enhancement, NB-IoT and 5G technology could be leveraged.

At the enterprise or outside of the factory, cloud platform and big data technology shall be introduced, and information exchange will be achieved between cloud platform with production devices or equipment, industrial control system, industrial information system and industrial internet application, as well as information exchanges with information system of collaborative enterprises, smart products and users, so as to provide lateral connection with various systems in different locations with different functions, as well as interconnection with upper-level applications and cross-enterprise/industries system to support value chain collaboration. The specific networking methods rely on interconnected scenarios. For example, for interconnection of factory/industrial cloud platform with production devices or equipment, industrial control system and industrial information system, the existing internet or enterprise information network could be used; for interconnection between factory/industrial cloud platform and information system of collaborative enterprises, the establishment of a secure and reliable VPN private line may be considered; for interconnection between factory/industry cloud platform and products, wide area mobile communication network and various types of cable communication such as NB-IoT, LTE enhancement, future 5G could be used.

(2) Implementation of identifier resolution

The implementation of identifier resolution mainly refers to the automatic reading and writing of the information on raw materials, articles being processed and products by identifier technology, and full life cycle management and information interaction among heterogeneous systems at different levels by identifier resolution system. The main parts involved in the implementation of identifier resolution is shown in Figure 15.

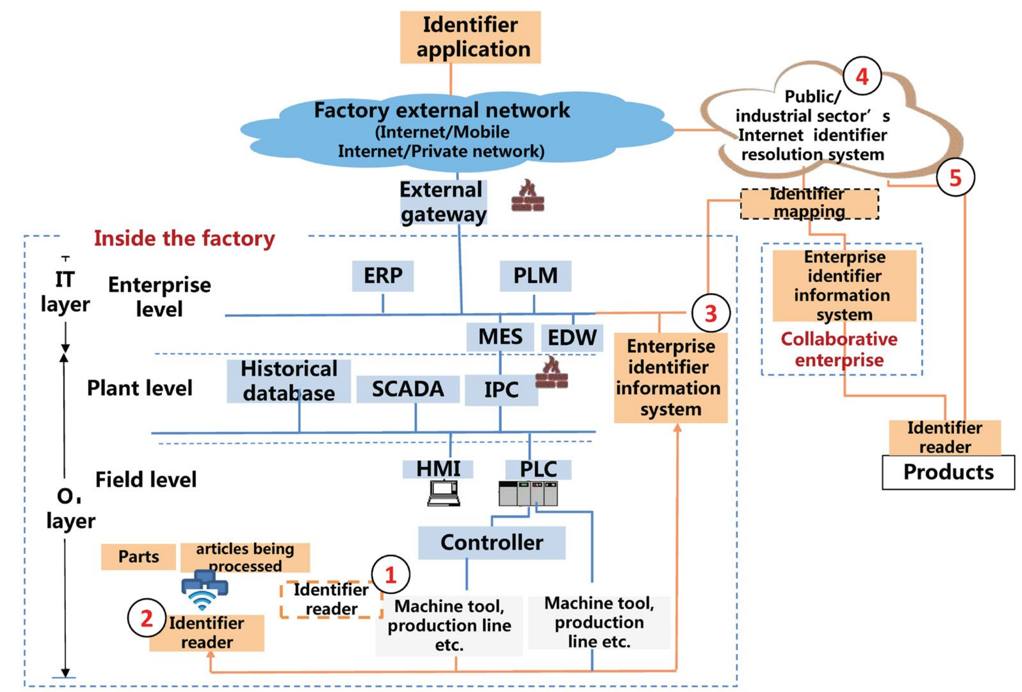

Figure 15 Implementation of Identifier Resolution

Inside the factory, to promote the application of identifier resolution technology, we shall: first, identify track objects according to requirements. The objects could be a device, raw material, articles being processed, product, as well as organization, order, craft, person, etc.; second, deploy identifier readers, which could be embedded into CNC and other devices, or deployed independently, through which we could automatically read ID and/or write information at the same time; third, set up an identifier information system to manage internal identifiers and related information while support connection with public/industrial internet identifier resolution system.

At the outside of the factory, the core is realize the cross-enterprise/industry/ reginal product information management via product identifiers. First, establish a public industrial identifier resolution system and industry-level identifier resolution system according to industrial internet identifier resolution and application requirements, and connect with enterprise identifier information system and identifier readers to support various identifier-based applications; second, while considering the fact that some enterprises or industries have deployed identifier resolution systems, but most of them are private resolutions, meanwhile considering the fact that currently there have been multiple identifier resolution systems, we need to provide identifier mapping and information matching mechanisms to realize cross-enterprise/industry exchanges of identifier and information.

(3) Implementation of application supporting

The implementation of application supporting mainly addresses the integration, analysis and usage of all kinds of data and services of industrial internet, and provides support for upper-level industrial internet applications, the key of which is to promote the construction of factory/industry cloud platform to provide data storage, analysis and processing, application supporting, open interfaces, etc.. There are three ways to implement factory/industry cloud platform, as shown in Figure 16, Figure 17 and Figure 18 separately.

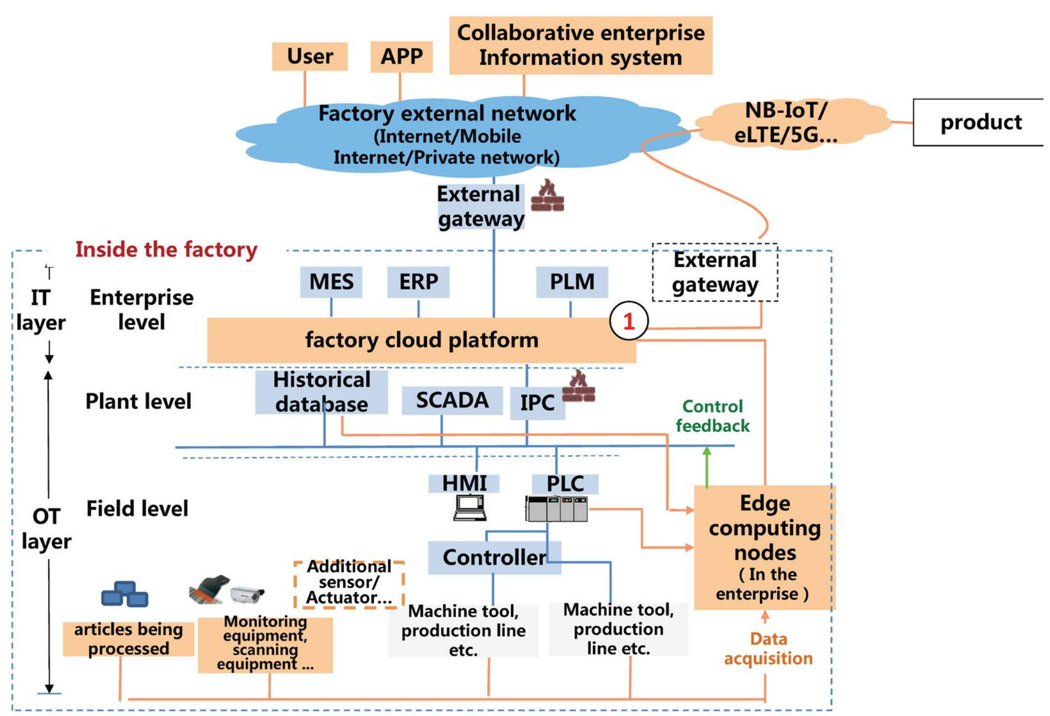

Figure 16 Approach 1: Implementation of Factory Cloud Platform

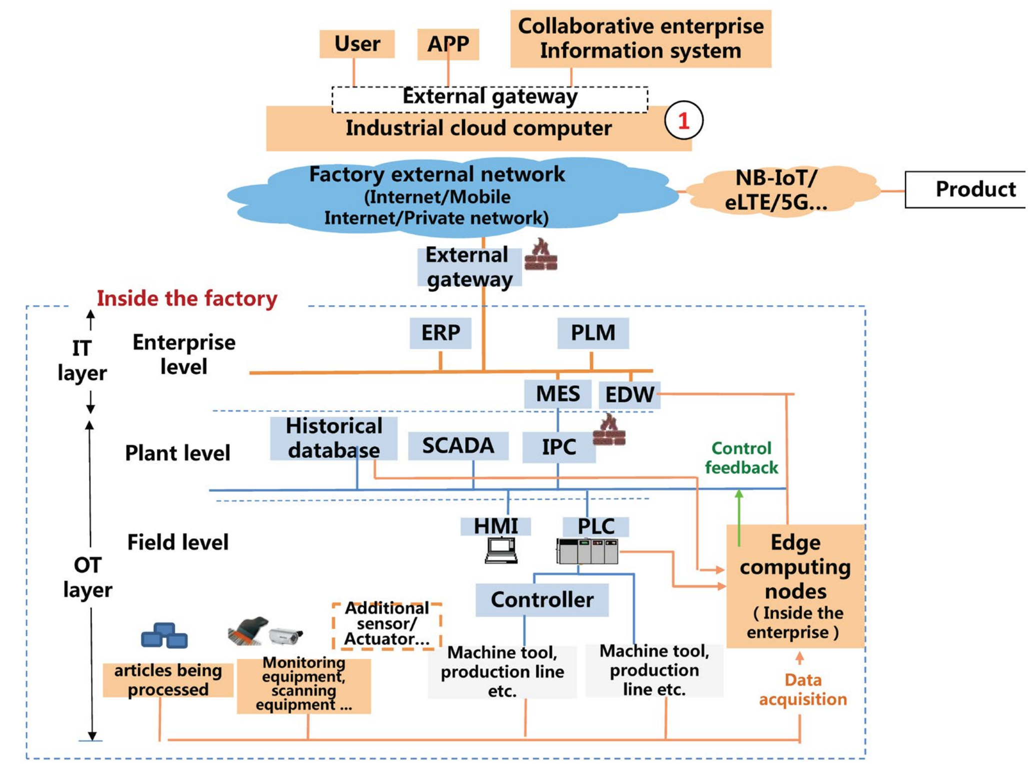

Figure 17 Approach 2: Implementation of Industrial Cloud Platform

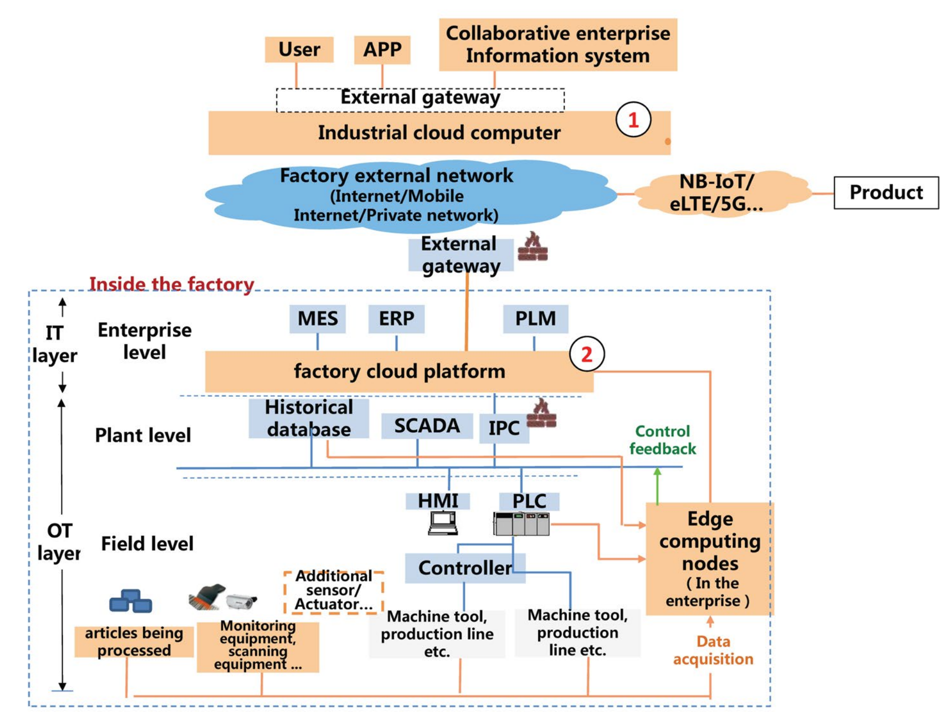

Figure 18 Approach 3: Implementation of Hybrid Cloud

Approach 1 is the implementation of factory cloud platform, which means deploying cloud platform within the factory to aggregate internal data of the factory, including the acquisited data from machines and instruments on production lines as well as data from factory information system and management system, and information of users, products and collaborative enterprises could also be aggregated as requested. The final objective is to realize lossless digitalized mapping and description of physical objectives such as devices, production lines and factories as well as crafts and processing flows, based on which the servitized combination and invocation of these software and hardware can be realized, and the operation platform environment will be provided for industrial information systems such as MES, ERP and so on.

Approach 2 is the implementation of industrial cloud platform, which is deployed on the public network such as the internet, and is able to aggregate data from value chain of industrial internet including design, production, logistics, market, product and user data, with the aim to analyze and optimize global data of full life cycle of production and full value chain. Meanwhile, industrial cloud platform could interact with factory information system, enabling the former to invoke factory internal data and vice versa.

Approach 3 is the implementation of a hybrid cloud, which means the collaborative deployment of factory cloud platform and industrial cloud platform. The internal information or system closely coupled with the enterprise will operate on the cloud platform of the factory, while the data and service that are appropriate for open to the public or external interaction system will be operated on the industrial cloud platform.

Meanwhile, factory/industry cloud platform and edge computing node are able to interact with each other, and the latter will process the data locally according to requirements of latency, privacy and security and then transmit the filtered data to factory/industrial cloud platform, thus to form the trend of "cloud-computing based global optimization + edge computing based local optimization".

As to the implementation of enabling technology, within the factory, for newly launched devices and systems (including factory cloud platform), their support for OPC-UA shall be taken into consideration; out of the factory, the industrial cloud platform shall consider the support for multiple application enabling technology together with the protocol adaptation and conversion functions, so as to support the access of devices and systems using different enabling technologies.

As to service encapsulation and integration implementation, during the transformation process of equipment and systems, consider shall be given to service abstract and encapsulation with the provision of service invocation interface. If it is difficult to directly reform equipment and systems, the deployment of a service adapter may be considered. It could be the independent hardware or software middleware. The service adapter could be used to provide service abstract and encapsulation of the function of these equipment and systems, as well as service invocation interface. Meanwhile, the cloud platform will provide service adaption, registration, discovery, combination and management functions to support the flexible orchestration and invocation. During the implementation and promotion of service encapsulation and integration, semantic technology shall be gradually introduced.

(III)Implementation of Industrial Internet Data

The implementation of industrial internet data involves the overall acquisition and flow of data, construction of industrial data cloud platform as well as the building of multi-layer data processing and analysis capacities, based on which all smart applications will be supported. Attention shall also be paid to the construction of data feedback closed loop in order to realize interaction between information systems and between information systems and physical systems. The main parts involved in the implementation of industrial internet data is shown in Figure 19.

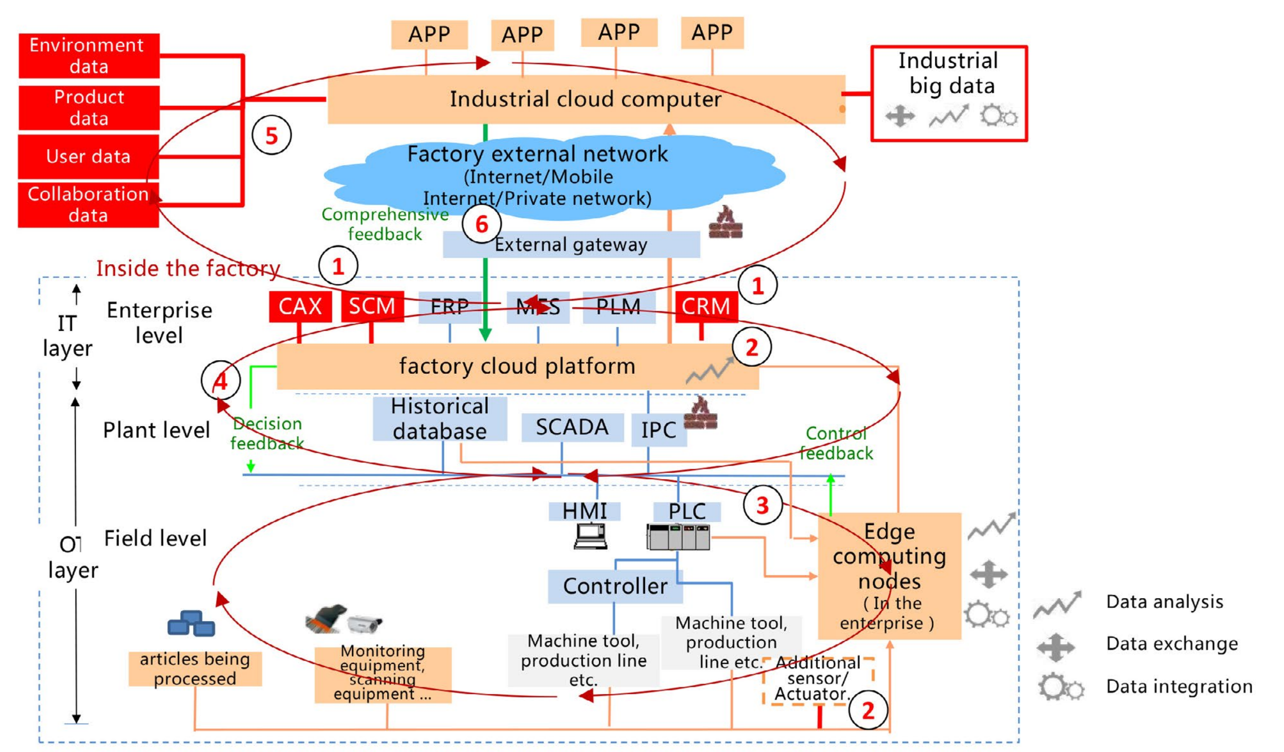

Figure 19 Implementation of Industrial Internet Data

First, promote information exchange among factory management software. At present, many enterprises have deployed management software within the factories, such as R&D design software (CAD, CAE, CAPP and CAM), production management software, customer management software (CRM), supply chain management software (SCM) and so on, but these software systems are lack of effective information exchange and integration, therefore we should promote data flow among the software systems. Second, push forward comprehensively data perception and acquisition, including the acquisition of the operation status information of machines and articles being processed, production environment information, and even industrial control system information necessarily. Third, consider deploying edge computing nodes to realize edge data analysis and processing, while setting up closed loop of edge data control to meet the requirements of real-time control and data security. Fourth, use cloud and big data technology to promote the integration and analysis of internal data of the factory, while build closed loop of decision feedback to realize industrial production control and various smart management decision applications. Fifth, aggregate product data, user data, environment data and collaborative enterprises data via industrial cloud platform outside the factory, and leverage big data technology to realize the integrated storage, analysis and processing of numerous complicated data. Sixth, build closed loop of comprehensive feedback. On the basis of the big data integration and analysis of industrial cloud platform, a closed loop of comprehensive analysis feedback from industrial cloud platform to enterprise information system will be built to enhance the linkage inside and outside of the factory.

(IV)Implementation of Industrial Internet Security

With the innovative development of industrial internet, the existing industrial system which is comparatively closed now has become more open, confronting it with newer security issues and challenges. Industrial internet shall guarantee the security of device, network, control, data and application through comprehensive security protection measures. The main parts involved in the implementation of industrial internet security are shown in Figure 20.

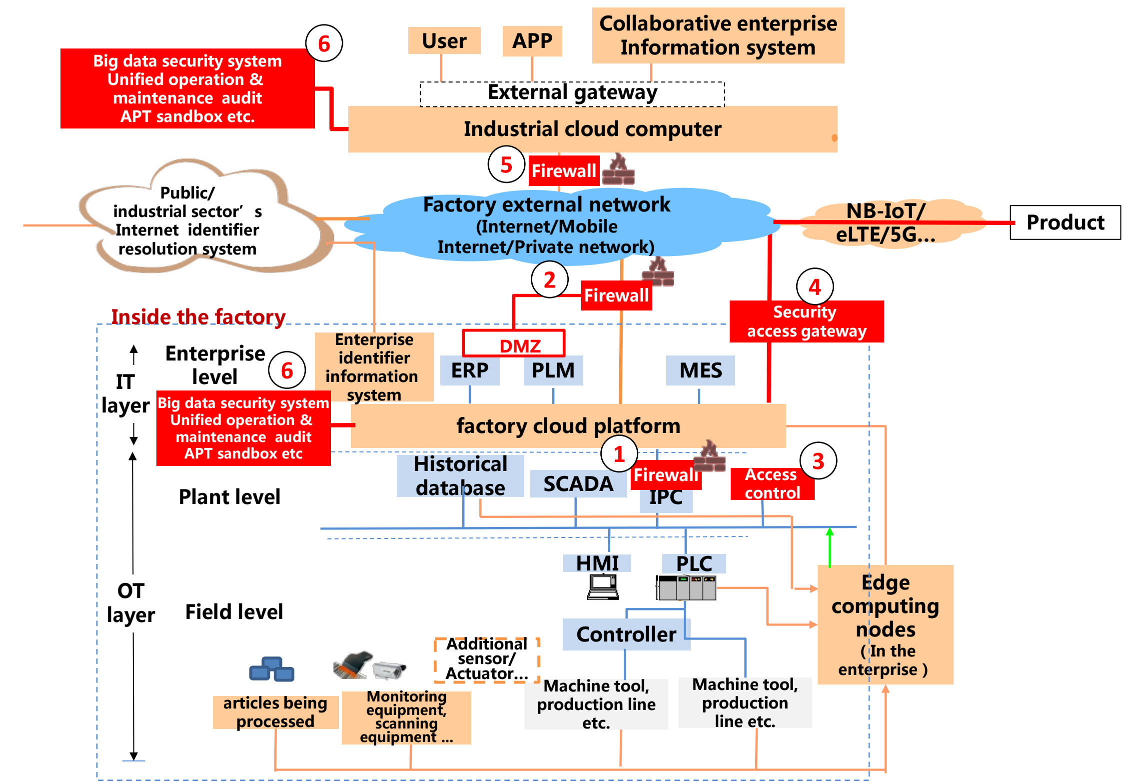

Figure 20 Implementation of Industrial Internet Security

Each connected unit of factory internet shall implement effective and accountable security isolation and control. Firstly, firewalls shall be deployed between industrial control system and industrial information system. Secondly, the access from outside of the factory to the internal cloud platform of the factory shall pass through a firewall, and the DDoS defense function shall be available. The interactive service and interface between ERP, PLM and external network shall be deployed in the DMZ, and the network invasion defense system with the ability to identify mainstream application layer protocols and contents, efficiently and effectively detect and locate the attacks and threats from business layer automatically shall also be deployed. Thirdly, all devices within the factory that can access to the internal cloud platform, factory information system and industrial control system shall be under access control with access authentication and authorization. Fourthly, smart devices, mobile office clients and information systems that are from the outside of the factory and have the access to the internal cloud platform shall pass the security access gateway equipped with remote protection software. Fifthly, for all accesses to the industrial cloud platform from the public internet, they should pass the firewall, and the DDoS defense function must be available. Sixthly, security protection technology based on big data shall be adopted, and big data security system shall be deployed at the factory cloud platform and industrial cloud platform to comprehensively defend all known and unknown threats based on external threats intelligence, log analysis, traffic analysis and sandbox linkage, and correctly display full security scenarios and realize intelligence of security situation.

In addition, the security protection of smart products and data transmitted via network shall be reinforced during the security implementation of industrial internet. Firstly, the security reinforcement of smart products. The deployment of smart products is much dispersed, so the damage, forgery, impersonation and replacement of them are easy, causing the leak of sensitive information. Therefore, specialized security reinforcement shall be conducted, such as the adoption of security software development kit (SDK), secure operation system, security chips and other technical measures to prevent hijack, impersonation, attack and leakage of secrets. Secondly, the security protection of external public network data transmission. For data that have to be transmitted through external network, they shall adopt IPSec VPN or SSL VPN or other encrypted tunnel transmission mechanisms, or private line such as MPLS VPN to prevent the leakage, interception or manipulation of data.

Appendix 1: Terms and Definitions

No.	Vocabulary	Definition	Note
1	industrial internet	Industrial internet is an industrial and application ecology generated from the overall, in-depth integration of the Internet, the next generation information technology and the industrial system. It is the key comprehensive information infrastructure for industrial intelligent development	
2	intelligent manufacturing	It is a general term for advanced manufacturing processes, systems and models that have functions of deep information self-sensing, intelligent optimized self-decision-making and precision control self-implementation based on the next generation information technologies such as IoT, big data and cloud computing, which goes throughout all links of manufacturing activities including design, production, management and service	
3	crowdsourcing	With the help of Internet and other means, assign the missions traditionally done by certain enterprises and organizations to all enterprises and individuals that are voluntarily willing to take part, to take full use of the public power, satisfy production and living service requirements with higher efficiency and lower costs, and promote the reform of production ways	See No. [2015] 53 file issued by the State Council of PRC
4	customization	Accurately match users' needs with corporate product design and production plans via the Internet platform, and realize diversified and customized product production and manufacturing models with the help of modularized production lines and new manufacturing techniques	
5	collaborative design	A product design model carried out in parallel by enterprises via a network-based design platform, which can effectively shorten products' design periods	
6	collaborative manufacturing	Based on a network-based collaboration platform, assign the manufacturing missions and order information to manufacturing enterprises in different regions with different scales, by which, the dispersive manufacturing resources and manufacturing capabilities in society can be gathered and shared on the network platform, thereby forming a network-based collaborative production organization model	

7	flexible manufacturing	An automated machinery manufacturing system that can adjust to the change of processed objects, consisting of a unified information control system, a materials storage and transmission system, as well as a set of digital controlled processing equipment	See MBAlib
8	precision marketing	A new marketing trend that carries out targeted product marketing based on customers' preferences after fully learning about their information, and that combines direct marketing and database marketing after grasping certain customers' information and market information	See MBAlib
9	supply chain collaboration	A network-typed combo formed by two or more enterprises for certain strategic purpose through a corporate agreement or a joint body	See MBAlib
10	vertical e-business	An e-commerce model to deepen the operation in some industry or subdivided market	See MBAlib
15	smart machine	Enable machines to have self-decision making, self-organization and self-adaption capabilities by adding modules of sensing, communication, computing and control	
16	edge computing	Extend the computing capability to the production site, to realize the distributed computing analysis of data and generate local real-time optimization decisions	
17	identifier	The only code or symbol that can identify the identity within certain scope	
18	resolve	A mapping process that inquires addresses and other information based on the identifier	
19	root server	The top level server in the identifier resolution system	
20	root zone file	The data file that stores the top level mapping information of the identifier resolution system	
21	factory internal network	A network used for connection between the production factors, and between the corporate IT management systems within a factory	
22	factory external network	A network aiming to support various activities during the whole industrial life cycle and used to connect the upstream and downstream of an enterprise, enterprise and intelligent products, as well as enterprise and users	
23	operation technology network	An industrial communication network used to connect the production site equipment and systems to realize automated control	

24	IT technology network	A data communication network used to connect the information system and the terminals	
25	field bus	A digital communication network with dual-transmission and multi-branch, used to connect the onsite smart equipment and the automated system	See IEC
26	industrial Ethernet	A standard Ethernet protocol-based communication network used to connect the onsite equipment and systems in industrial automation and process control	
27	software defined network	A network architecture used for network control and separation forwarding, where the upper layer applications and services can control the lower layer network equipment via the programmable interface at the network control layer	See ONF
28	network virtualization	A technology that can realize dynamic dispatching and management of network resources	
30	work cell	A physical, geographical or logical production group decided by the enterprise to finish activities of a certain process, or is known as a workshop section	See GBT 20720.1-2006
31	work center	A production workshop composed of several workshop sections to finish the production and manufacturing of some part of a product	
32	enterprise	A production place composed of several workshops, responsible for the production of a product from the prototype to the real object, as well as the development of operation management decisions	
33	supervisory control and data acquisition	A computer control system that is able to monitor programs and collect data, and is used in industrial programs, infrastructure or equipment	See Wikipedia
34	customer relationship management	The summation of methods for managing the integration of information technologies and software/hardware systems, and the application solutions in corporate management, the purpose of which is to improve the business processes related with customer relations in fields like sales, marketing, and customer services and supporting	See MBAlib
35	manufacturing execution system	A management information system oriented to the workshop level, which is in the middle of the upper plan management system and the bottom industrial control, providing the current statuses of plan implementation, tracking and all resources (people, equipment, materials, customer needs, etc.) to operators/administrators	

Appendix 2: Abbreviations

序号 No	缩略语 Abbr	英　文 English
1.	5G	the 5th Generation of communication technology
2.	AII	Alliance of Industrial Internet
3.	AMQP	Advanced Message Queuing Protocol
4.	APT	Advanced Persistent Threat
5.	CID	Communication IDentifier
6.	COAP	Constrained Application Protocol
7.	CRM	Customer Relationship Management
8.	DCS	Distributed Control System
9.	DDoS	Distributed Denial of Service
10.	DDS	Data Distribution Service
11.	DMZ	DeMilitarized Zone
12.	DNS	Domain Name System
13.	DONA	Digital Object Numbering Authority
14.	Ecode	Entity Code
15.	EPC	Electronic Product Code
16.	ERP	Enterprise Resource Planning
17.	ESB	Enterprise Service Bus
18.	ETL	Extract-Transform-Load
19.	FCS	Field Bus Control System
20.	GS1	Globe Standard 1
21.	HMI	Human Machine Interface
22.	HTML	HyperText Markup Language
23.	IaaS	Infrastructure as a Service
24.	IETF	Internet Engineering Task Force
25.	ISA	International Society of Automation
26.	LTE	Long Term Evolution
27.	MPLS	Multi-Protocol Label Switching
28.	MES	Manufacturing Execution System
29.	MPP	Massive Parallel Processing
30.	MQTT	Message Queuing Telemetry Transport
31.	NB-IoT	Narrow Band Internet of Things
32.	NIOT	National Internet of Things Name Service Platform
33.	OASIS	Organization for the Advancement of Structured Information Standards
34.	OID	Object Identifier
35.	OMG	Object Management Group
36.	ONS	Object Name Service
37.	OPC	OLE for Process Control
38.	OPC-UA	OPC Unified Architecture
39.	ORS	Object Identifier Resolution System
40.	OS	Operating System
41.	OT	Operation Technology
42.	PaaS	Platform as a Service
43.	PLC	Programmable Logic Controller
44.	PLM	Product Lifecycle Management
45.	REST	Representational State Transfer
46.	RFID	Radio Frequency Identification
47.	SaaS	Software as a Service
48.	SCADA	Supervisory Control And Data Acquisition
49.	SCM	Supply chain management
50.	SDK	Software Development Kit
51.	SDN	Software Defined Network
52.	SOA	Service-Oriented Architecture
53.	SOAP	Simple Object Access Protocol
54.	SSL	Secure Sockets Layer
55.	VPN	Virtual Private Network
56.	WIA-FA	Wireless Network for Industrial Automation – Factory Automation
57.	WIA-PA	Wireless Networks for Industrial Automation Process Automation
58.	HART	Highway Addressable Remote Transducer
59.	XMPP	Extensible Messaging and Presence Protocol