Workgroup: Industrial Internet of Things
Internet-Draft:
draft-tang-iiot-architecture-02
Published: 8 June 2021
Intended Status: Informational
Expires: 10 December 2021
Authors: C. Tang
Chongqing University
H. Wen
Chongqing University
S. Ruan
Chongqing University
B. Huang
Chongqing University
X. Feng
Chongqing University

Architecture Based on IPv6 and 5G for IIoT

Abstract

As the foundation of the current new round of industrial revolution, the Industrial Internet of Things (IIoT) based on cyber-physical systems (CPS) [smart-factory] has become the focus of research in various countries. One of the key issues in the entire development stage of IIoT is the standardization of the IIoT architecture. With the development of intelligent manufacturing technology, the number of IIoT devices is expected to increase sharply, and large amounts of data will be generated in the industrial manufacturing process. However, traditional industrial networks cannot meet the IIoT requirements for high data rates, low latency, massive connections, interconnection, and interoperability. Current IIoT architectures also have various limitations, including those in mobility, security, scalability, and communication reliability. These limitations hinder the development and implementation of IIoT. As a network layer protocol, IPv6 can solve the problem of IPv4 address exhaustion. Meanwhile, as a high-speed, low-latency, wireless communication technology, 5G has great potential in promoting IIoT. To solve the aforementioned problems, this draft proposes an IIoT architecture based on IPv6 and 5G. The architecture can provide high-speed, low-latency communication services and possesses massive connectivity, mobility, scalability, security, and other features for industrial devices. It can also provide generalized, refined, flexible network services for devices outside factories. Moreover, an information model is defined to standardize the representation of information in IIoT. The security challenges in and recommendations for IIoT are also discussed.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 December 2021.

Copyright Notice

Table of Contents

1. Introduction

IIoT is an industrial and application ecology formed by the comprehensive and deep integration of the Internet, information technology, and industrial systems, and it is a key information infrastructure for the development of industrial intelligence. Its essence is based on the network interconnection between machines, raw materials, control systems, information systems, products, and people. Intelligent control, operation optimization, and production organization reform can be achieved through comprehensive in-depth perception of industrial data, real-time transmission and exchange, fast calculation and processing, and advanced modeling analysis. The IIoT foundation is the system architecture, which pertains to the interconnection and intercommunication of the entire industrial system through technologies, such as the Internet of Things and the Internet, to promote the full circulation and seamless integration of industrial data.

The communication technology in the industrial network interconnection architecture needs to meet the following major requirements.

*(1) High communication rate. The increasing number of manufacturing activities, such as real-time monitoring of all production factors and the entire production process, and the application of cloud computing, edge computing, virtual reality, and augmented reality in the manufacturing industry are expected to generate large amounts of manufacturing data, which need a stable and fast network where data should be more than 25 Mbps [iiot-5g].

*(2) High coverage. The goal of IIoT is to establish "ubiquitous communication." In other words, any area in a manufacturing plant should achieve 100% networking coverage. However, in actual factories, the current communication technology cannot meet the requirements of high coverage due to the complex production environment, such as electromagnetic interference and obstacles.

*(3) Low latency. Advanced manufacturing activities, such as human-machine cooperation, machine-machine cooperation, and remote real-time control, have strict requirements on communication delays and generally require low delays (about 1 ms). Although current wireless communication technology has made great progress and the end-to-end delay is about 20-100 ms

[iiot-5g], it still cannot meet the urgent need for low delay in IIoT.

*(4) Massive connections. Owing to the interconnection of all things in IIoT, the connected devices and the data generated increase exponentially throughout the production process. Wired communication cannot meet the requirements of massive connections due to the difficulty in arranging lines, and wireless communication cannot meet the said requirements due to the limitation in the number of access nodes.

*(5) Interconnection. Many communication protocols are adopted in the development of industrial networks. Fieldbus protocols include PROFIBUS, Modbus, and HART. Industrial Ethernet protocols include Ethernet/IP, PROFINET, and Modbus TCP, and industrial wireless protocols cover WLAN, Bluetooth, and WirelessHART. The interconnection and interoperability of these protocols are not ideal because they use different technologies at the physical, link, and application layers. This affects the expansion of IIoT to some extent.

The main work of the proposed architecture is introduced as follows.

An industrial network interconnection architecture based on IPv6 and 5G communication technology is designed by combining actual scenarios of factory intelligent manufacturing and the requirements of IIoT for communication technology. The architecture can provide high-speed, high-reliability, low-latency communication services, including factory internal and external networks. The factory internal network provides massive connection, mobility, device registration and discovery, and security for industrial production-related devices. The factory external network provides generalized, refined, flexible network services for devices outside the factory. An information model is defined to standardize the representation of information in IIoT. The current security challenges in IIoT are presented, and security recommendations are provided.

2. IIoT Architecture

In the IIoT architecture, the network is the foundation; it provides infrastructure for the comprehensive interconnection of people, machines, and things and promotes the full flow and seamless integration of various industrial data. The industrial Internet network connection involves different technical fields with multiple elements and subjects inside and outside the factory and covers a large scope of influence and many optional technologies. Various network connection technologies are available in the industrial field. These technologies are designed for specific scenarios in the industrial field and play a crucial role in specific scenarios.

However, in terms of data interoperability and seamless integration, they often cannot meet the growing demands of IIoT.

The overall goal of IIoT network connection is to enhance the interconnection and intercommunication between systems, unlock data from isolated systems and networks, and make data achieve a high value for applications within and across industries.

This chapter proposes an industrial network system architecture based on the transformation of the factory IP network, which has two major networks (factory internal and external networks), as shown in Figure 1.

The factory internal network is used to connect various elements in the factory, including people (e.g., production staff, designers, and external people), machines (e.g., devices and office equipment), materials (e.g., raw materials, work in progress, and finished products), and the environment (e.g., instruments and monitoring devices). The factory internal network is interconnected with enterprise data centers and application servers to support business applications in the factory.

The factory external network is used to connect smart factories, branches, upstream and downstream collaborative enterprises, industrial cloud data centers, smart products, and users. The data center/application server in the smart factory is interconnected with the industrial cloud data center outside the factory through the factory external network. Branches/collaborative enterprises, users, and smart products are also connected to the industrial cloud data center or enterprise data center through the factory external network. The data intercommunication in IIoT realizes the seamless transfer of data and information among various elements and systems so that heterogeneous systems can "understand" each other at the data level, thereby realizing data interoperability and information integration. IIoT requires breaking information islands, realizing cross-system data intercommunication, and fusion analysis. Therefore, on the one hand, the factory external network needs to support the aggregation of the underlying data generated by various factory elements and factory products to the data center; on the other hand, it must provide upper-layer applications with access interfaces to heterogeneous system data to support the rapid development and deployment of industrial applications.

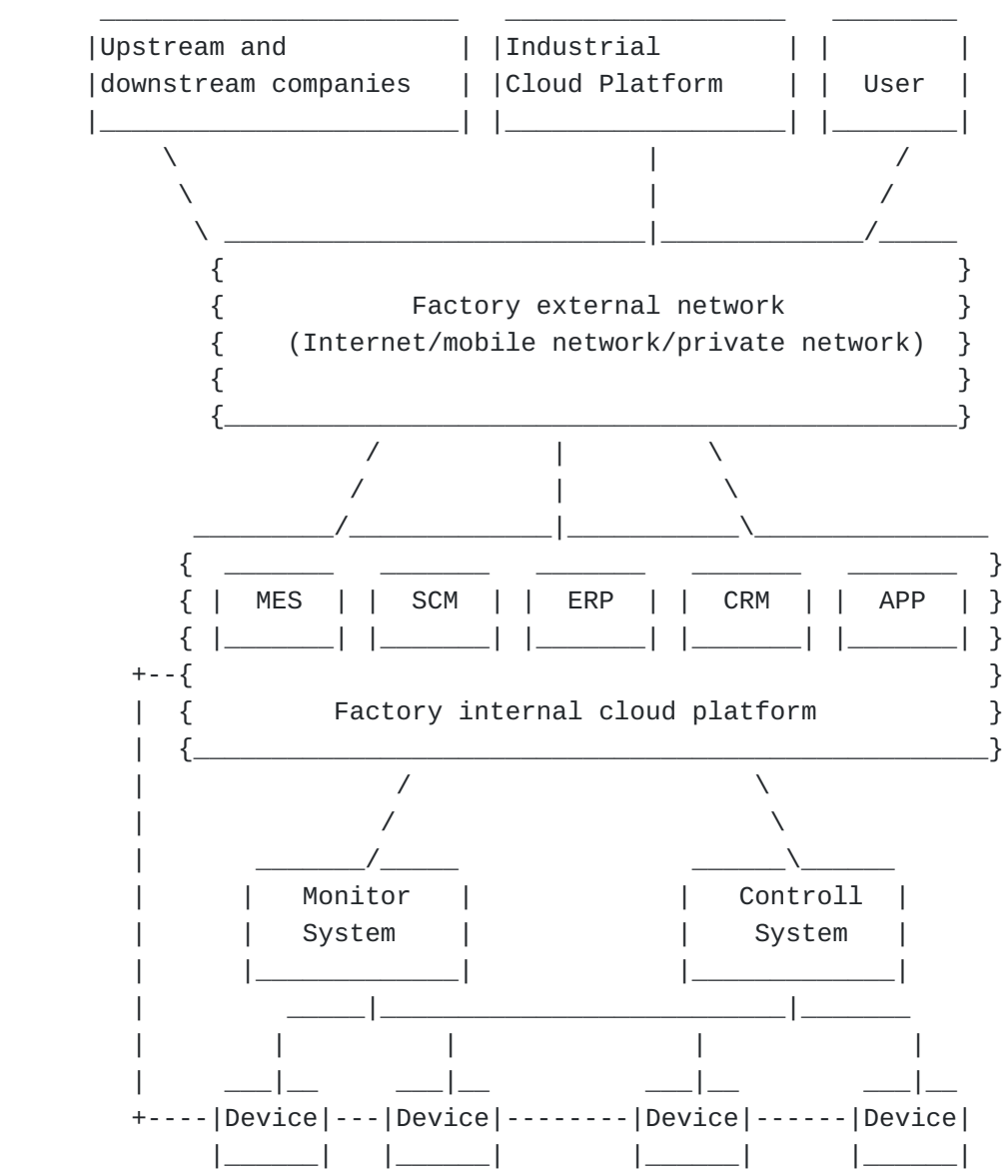

Figure 1: IIoT architecture

Architecture advantages:

*(1) High communication rate. The factory network adopts industrial PON and 5G technology, which can realize high-speed data transmission.

*(2) Low communication delay. The Ethernet-based TSN network [tsn] and 5G wireless network can realize low-latency communication and ensure real-time industrial production.

*(3) Massive connections. IPv6 [I-D.ietf-6lowpan-usecases] can assign an IP address to each industrial IoT device, and the 5G network supports the wireless access of numerous IIoT devices.

*(4) Scalability. When a new industrial device joins the network, it can register with the edge server. The name and IP address of the device are registered. When another industrial device has data and service requirements for the new industrial device, the new industrial device can be found on the edge server to access data or services.

*(5) Mobility. After a device moves in multiple networks, it registers with the edge server again and obtains a new address from the edge server to perform subsequent communication.

*(6) Localization of computing and storage. Edge computing technology is used to perform computing or data storage services in edge servers close to industrial sites [edge-computing].

*(7) Support multiple communication protocols. The OPC UA protocol, support TCP, WebSocket, HTTP, and other transmission protocols are used. These protocols can realize device-to-device communication; support UDP broadcast, MQTT, AMQP, and other protocols; and realize Pub/Sub communication [I-D.ietf-core-coap-pubsub].

*(8) Cloudization of network services outside the factory. On the basis of cloud computing and enterprise-dedicated line technology, the enterprise business system is deployed to the cloud to facilitate external services. It can also provide segmented services for different scenarios, such as public and private clouds. Network virtualization technology is used to improve the flexibility of network services so that the factory external network can quickly open and adjust services according to enterprise requirements.

3. Factory Internal Network

3.1. Status and Development Trends

In an IIoT factory, on the one hand, the digitization of the factory requires that the digitization of many existing business processes be carried by the corresponding network. On the other hand, a large number of new networked devices (e.g., AGVs, robots, and mobile handheld devices) and new business processes (e.g., performance management, predictive maintenance, and personnel/material positioning) have been introduced. The introduction of new devices and business processes creates new demands on the network. As a result, the two traditional networks (production and office networks) in the factory become multiple networks, which

correspondingly cause changes in the network architecture in the factory.

To break information islands and improve operational efficiency, companies deploy business systems that were originally deployed on various servers, such as MES, PLM, ERP, SCM, and CRM, to the data center/cloud platform in the factory. The data generated by each networked device and business process must be able to be aggregated in the data center/cloud platform in real time for joint analysis and rapid decision-making. Changes in business system deployment also cause changes in the network architecture.

The IIoT demand for flexible manufacturing and personalized customization requires the production domain to be flexibly reconfigured according to requirements, and intelligent machines may be adjusted and migrated between different production domains. This procedure requires the network architecture in the factory to be able to adapt to the needs of fast networking and flexible adjustment.

The factory internal network proposed in this chapter can be understood from two aspects: functional and network views.

3.2. Functional View

According to the specific functions of the system and devices and the location of the network, the factory internal network can be divided into device, control, and factory management layers, as shown in Figure 2.

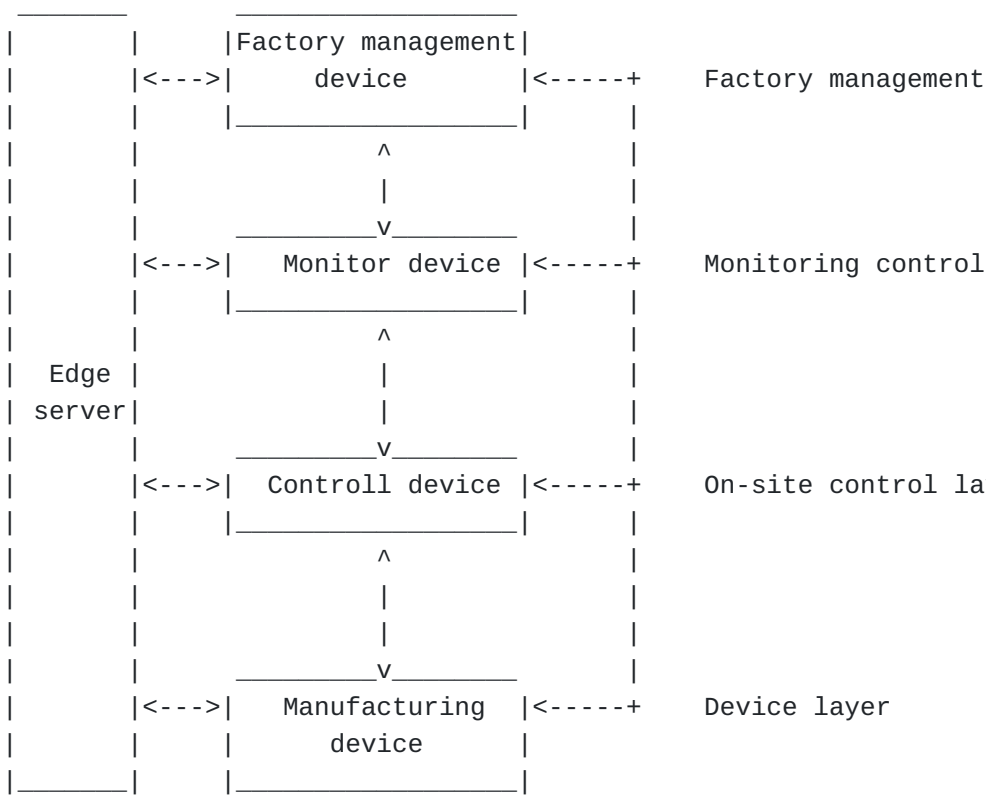

Figure 2: Functional View

(1) The device layer participates in data perception and task execution in the manufacturing process. The time resolution granularity can be seconds, milliseconds, and microseconds. Various sensors, transmitters, actuators, RTUs, barcode scanners, RFID readers, and intelligent manufacturing devices (e.g., CNC machine tools, industrial robots, AGVs, and conveyor lines) run on this layer. These devices are collectively referred to as field devices.

(2) The control layer realizes the monitoring and control of field devices in the manufacturing process. The time resolution granularity can be hours, minutes, seconds, and milliseconds. According to different functions, this level can be further subdivided into the following:

*(i) Monitoring control layer: With operation monitoring as the main task, it has other management functions, such as advanced control and fault diagnosis. The visual data acquisition and monitoring system (SCADA), human-machine interface (HMI), DCS operator station, real-time database server, and other components run on this layer.

*(ii) On-site control layer: It measures and controls the production process, collects process data, performs data

conversion and processing, outputs control signals, and realizes logic control, continuous control, and batch control functions. Various programmable control devices, such as PLC, DCS controller, industrial computer (IPC), and other special controllers, run on this layer.

(3) The factory management layer realizes the production management of the factory and manages workflow/recipe control activities, including maintenance records, detailed production scheduling, and reliability assurance. The time resolution granularity can be days, shifts, hours, minutes, or seconds. The manufacturing execution system (MES), supply chain management (SCM), enterprise resource management (ERP), and customer relationship management (CRM) run on this layer.

To achieve IIoT scalability (after a new device joins the network, other devices can access data or call-related services), this architecture adopts device registration and device discovery functions.

Device registration: When a new device is connected to the network, it registers its name with the edge gateway. The format of the registered name is /Service-Name/Gateway-Name/Device-Name, and the IP address of the device is stored and bound with the name.

Device discovery: When a device needs to access data in other devices or call services in other devices, it can make a query in the edge gateway. It can find the IP address of a corresponding group of devices based on the service name and gateway name; it can also find the corresponding IP address of a certain device based on the service name, gateway name, and device name. After finding the IP address, the device can communicate with the corresponding device.

3.3. Network View

The factory internal network can be divided into three parts: edge network, backbone network, and factory cloud platform. These parts can be interconnected through industrial PON, as shown in Figure 3.

Given the diversification of connected production factors, the edge network presents various types as follows: according to business needs, the edge network can be an industrial control network, an office network, a monitoring network, a positioning network, etc.; according to real-time requirements, the edge network can be a real-time or a non-real-time network; according to the transmission medium, the edge network can be a wired or wireless network; and according to the communication technology adopted, the edge network can be an industrial Ethernet network, a 5G wireless network, etc.

The range of the edge network may be a workshop, an office building, a warehouse, or others. Each edge network is composed of edge servers, edge gateways, and field devices. Enterprises can comprehensively consider business requirements and costs and select appropriate technologies to deploy in accordance with edge networks.

The backbone network is used to realize interconnection between edge networks, cloud platforms/data centers in the factory, and other parts requiring high bandwidth and high speed. The backbone network can be large or small depending on the size of the enterprise. It can be a cluster of fully interconnected routers, or it can include only one or two backbone routers.

For example, industrial, control, and monitoring devices that need wired connections can be connected to switches that support industrial Ethernet protocols through optical fibers. The specific physical layer protocol can use industrial PON, and the data link layer protocol can use the TSN protocol to form a TSN Ethernet edge network.

Industrial, control, and monitoring devices that need wireless connections can be connected to 5G base stations through 5G wireless connections to form a 5G wireless edge network.

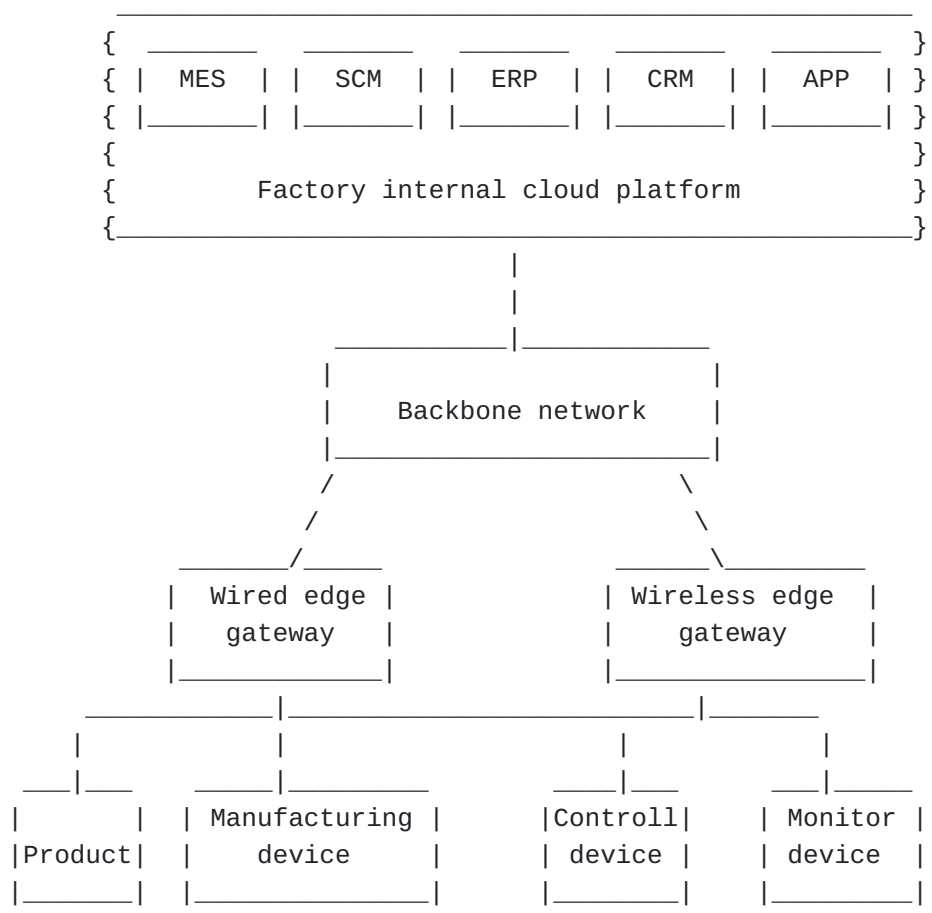

Figure 3: Network view

The IPv6 protocol can be used at the network layer to realize communication between edge networks of different protocols and the IP of industrial, control, and monitoring devices. However, the IPv4 protocol still has numerous devices and applications. In the transition phase to the IPv6 protocol, if the number of IPv4 devices and applications is large, the GI DS LITE tunnel technology solution can be used. If the number of IPv4 devices and applications is small, IPv4/IPv6 dual-stack technology solutions can be adopted.

The backbone network is used to realize interconnection between edge networks and cloud platforms in the factory, and it requires high bandwidth and high speed. The backbone network can be large or small depending on the size of the enterprise. It can be a cluster of fully interconnected routers, or it may contain only one or two backbone routers.

The factory cloud platform can be upgraded to a TSN network on the basis of the original standard Ethernet, which can meet the high bandwidth and low latency requirements of industrial cloud platforms. TSN also has excellent upper-layer support compatibility

and can support various upper-layer communication protocols. For example, TSN and OPC UA can solve data intercommunication problems in a factory, and OPC UA data collection and cloud services can be extended to the field level. The proposed architecture can realize all-around, real-time data collection and real-time operation in the production environment.

3.4. Communication Manner

Relationship between functional and network views: The communication between the device layer and the control layer can be realized in the edge network. The factory management layer is deployed in the factory cloud platform, and the backbone network is responsible for the communication among device, control, and factory management layers.

(1) Communication between devices: One-to-one communication between devices uses the C/S architecture in OPC UA and supports the transmission protocols of TCP, WebSocket, and HTTP. The OPC UA server and client are separately deployed in the two devices. When a device needs to access data or send instructions, it can use its own client to initiate communication with the other device's OPC UA server, as shown in Figure 4.

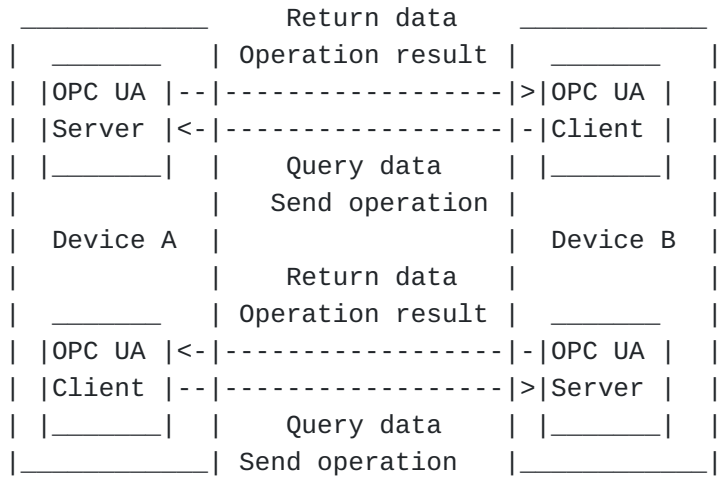

Figure 4: C/S architecture in OPC UA

The communication between one-to-many devices uses the Pub/Sub mechanism in OPC UA and supports multiple mechanisms, such as UDP broadcast, MQTT, and AMQP. If multiple devices have requirements for the data in one device, these multiple devices can subscribe to this device. This device will publish the data to the multiple devices when it collects or detects data changes, as shown in Figure 5.

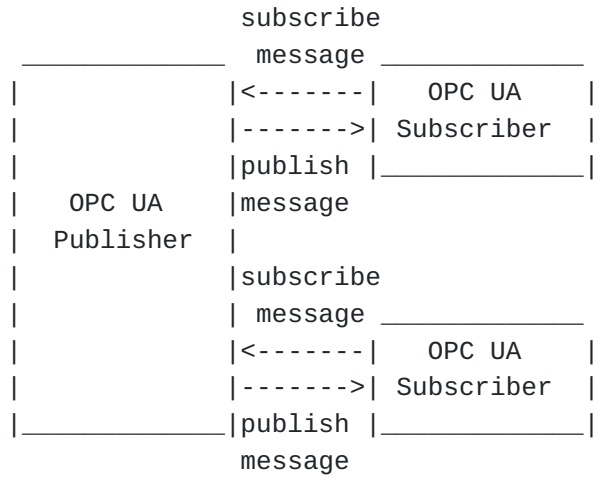

Figure 5: Pub/Sub mechanism in OPC UA

(2) Communication between a device and the edge server:

(i) The C/S mode in OPC UA, which is suitable for application scenarios involving a large data volume and industrial automation control, is used. For example, in machine vision product quality inspection, a device uses a camera to collect machine vision pictures of the product after the product is manufactured or assembled. The pictures are sent to the edge server's intelligent detection algorithm for analysis and processing through the OPC UA protocol. Then, the edge server returns the detection result to the industrial device, and the industrial device performs the next step in accordance with the detection result.

(ii) The Pub/Sub mode in MQTT, which is suitable for communication between devices with a small data volume, low bandwidth, and low hardware resources and edge servers, is utilized. For example, in factory temperature intelligent adjustment, the energy-saving management program in the edge server needs to automatically turn on or control the adjustment device according to the change in temperature and humidity. The energy-saving management program in the edge server can initially subscribe to the edge gateway with the theme of temperature and humidity. After the sensor device in the factory periodically collects temperature and humidity data, it publishes relevant messages to the edge gateway with the theme of temperature and humidity. Then, the edge gateway pushes the messages to the energy-saving management program in the edge server and realizes automatic adjustment.

(3) Communication between a device and the cloud server: Various production management applications run on the factory cloud platform, which realizes data collection, process monitoring, industrial device management, quality management, production

scheduling, and data statistical analysis for the entire production process to achieve the informatization, intelligence, and flexibility of the smart manufacturing management. To realize communication between a device and the cloud server, the OPC UA protocol can be utilized to deploy the OPC UA server on the device and to deploy the client on the cloud server so that the cloud server can read real-time production data on the device and send it control instructions. Alternatively, the cloud server subscribes to the device for data, and when the data are ready, the device sends the data to the cloud server. The cloud server sends instructions or management data to the device.

4. Factory External Network

The factory external network is designed to support various activities in the entire life cycle of the industry and used to connect the upstream and downstream of the enterprise, the enterprise and the product, and the enterprise and the user.

4.1. Situation

The breadth and depth of the development and utilization of industrialized data and information vary because of the different levels of informatization development in different industries and fields of industry. Thus, uneven network construction and development exist outside the factory, and several industrial enterprises only apply for ordinary Internet access. Islands of information are still present between different areas of several industrial enterprises.

4.2. Development Trend

With the development of industrial networking and intelligence, the systems and applications in factories are gradually expanding outward, and the industrial Internet services outside factories are showing a trend of generalization, refinement, and flexibility.

Network services outside factories are universal. The traditional network outside factories mainly facilitates the communication of commercial information, and the information systems of the enterprise are deployed on the network inside its factory. The network outside factories has few connection objects and a single service. With the development of cloud platform technology, several enterprise information systems (e.g., ERP and CRM) are being externalized, and an increasing number of IT software programs are being developed based on cloud computing to provide services on the cloud. With the development of the remote service business of industrial products and devices, remote monitoring, maintenance,

management, and optimization of massive devices will be carried out based on the network outside factories in the future.

With regard to refined network services outside factories, the factory external network realizes the ubiquitous interconnection of the entire industrial chain and the value chain. The complex and diverse connection scenarios promote the refined development of services. On the one hand, the connection demand of massive devices has promoted the construction of mobile networks outside factories and the rapid development of wide-coverage services. On the other hand, enterprises need to deploy services to the cloud, which promotes the refinement of dedicated line services, and they must provide segmented services for different scenarios, such as enterprise Internet access, business system cloud access, and public and private cloud interoperability.

With regard to flexible network services outside factories, the development of network virtualization and softwareization has improved the flexibility of network services so that the network outside a factory can quickly open and adjust services according to enterprise requirements. The application of a large number of mobile communication network technologies has improved the convenience of network access. The speed of deployment provides a flexible means for enterprises to achieve extensive interconnection.

4.3. Enterprise Dedicated Line

The wide-area Internet business requirements of industrial entities include the following main aspects: the Internet access requirements of industrial entities, the interconnection and isolation requirements between industrial entities across regions, the interconnection requirements of industrial networks and hybrid clouds, and the differentiated requirements (QoS, security/ protection, etc.) of industrial Internet for wide-area bearer networks. The most widely used carrier private line services for meeting these requirements mainly include MPLS VPN dedicated line and OTN-based optical network dedicated line.

The MPLS VPN virtual private network builds an enterprise virtual private network on the public MPLS network to achieve safe, fast, and reliable industrialized communication between branches in different cities (international and domestic). It can support multimedia services that require high quality and high reliability, such as office, data, voice, and images.

The MPLS VPN dedicated line is based on IP and high-speed label forwarding technology. The distinction of service levels and quality service guarantee can be realized through the setting of QoS bits.

The intelligent optical network based on the optical transport network (OTN) is an ideal solution for large-particle broadband service transmission. If the main dispatching particle of the external private network of an enterprise reaches the Gb/s level, OTN technology can be considered a priority for network construction.

With the increase in enterprise network application requirements, the need of large enterprises for large-particle circuit scheduling also increases. The introduction of OTN technology can realize flexible large-particle circuit scheduling. Compared with MPLS VPN, OTN technology can realize an end-to-end physical private network, which is attractive for specific enterprises that require large bandwidth (above 1 Gbps) and high data and service reliability and security.

In addition, emerging technologies, such as SD-WAN and CloudVPN, can complement existing technologies, integrate various dedicated line resources, and open the call platform through a unified capability to form a transparent, integrated, shielded part of the technical complexity for users. A factory's extranet solution can economically meet the rapidly changing needs of enterprises for private line services.

(1) The CloudVPN dedicated line is a new-generation enterprise private line network solution that redefines enterprise interconnection centered on cloud services, thus simplifying business deployment to the greatest extent. CloudVPN can reduce the time for opening and adjusting VPNs traditionally on a weekly or monthly basis to the minute level, thereby providing convenient and flexible business options and realizing enterprise interconnection on demand. The CloudVPN private line solution includes the basic network device layer, management control layer, collaboration layer, and user interface. The operator's private line access capability is encapsulated as a simple OpenAPI interface. It supports developers' applications to realize enterprise private line services by directly calling the interface and supports fast ordering, opening, and on-demand adjustment of services, such as Internet access dedicated lines. The CloudVPN dedicated line network can be opened on demand in real time and elastically expanded; it also supports real-time adjustment of dedicated line network bandwidth in industrial environments, such as distance education, data intercommunication, and video conferencing.

(2) SD-WAN is an extranet interconnection service formed by applying new SDN technology to WAN scenarios. This type of service is used to connect enterprise networks, data centers, Internet applications, and cloud services in a wide geographical area. The technical features of SD-WAN include the following:

(i) SD-WAN "cloudizes" the control capabilities of hardware networks through software, thereby supporting the opening of user-perceivable network capabilities.

(ii) The introduction of SD-WAN technology reduces the complexity and technical threshold of user-side WAN operation and maintenance.

(iii) SD-WAN technology has a high degree of self-service capability, and users can open, modify, and adjust private network interconnection parameters. The core concept of SD-WAN is the users' networking requirements and networking intentions, which can be translated and managed through the centralized control orchestrator provided by the communication service provider, thus shielding users from the complexity of the underlying network technology.

(iv) SD-WAN supports heterogeneous networks (access can be done in many different ways, including the Internet, other access methods such as OTN, other dedicated lines, etc.). The access device is generally on the user side, and the service differentiation point is also on the user side. It helps users make flexible business adjustments through its self-service interface.

SD-WAN has a heterogeneous network and flexible operation, but because its virtual private network may be implemented based on Internet access, it may cause hidden dangers in network attacks and data security, and end-to-end encryption needs to be implemented through encryption protocols.

4.4. Mobile Communication Network

With the development of IIoT, the industrial production process is no longer limited to the factory. Industrial production is gradually integrated with Internet business models, factories and products, and customers through the factory external network. In certain production processes, the communication demand between the factory and the devices outside the factory has also increased significantly.

In these scenarios, mobile communication networks have been increasingly used in industrial production due to their characteristics of wide coverage, high speed, high network reliability, and mature industrial chain, which greatly expand the connotation and extension of traditional industrial networks. Mobile communication networks have provided a good foundation for the development of IIoT.

3GPP's 5G defines three types of application scenarios: enhanced mobile broadband (eMBB), large-scale machine communication (mMTC), and high-reliability low-latency communication (uRLLC). The eMBB scenario can support the gradual emergence of high-traffic services

on IIoT, such as virtual factories and high-definition video remote maintenance. Large-scale machine communication scenarios are mainly aimed at massive field device communication.

The 5G network separates control and forwarding. The forwarding plane focuses on the efficient routing and forwarding of business data. It has the characteristics of simplicity, stability, and high performance to meet the forwarding needs of massive mobile traffic in the future. The control plane uses a logically centralized approach to achieve unified policy control and ensure flexible traffic scheduling and connection management. The centralized control plane realizes the programmable control of the forwarding plane through the mobile flow control interface.

The 5G core network supports various services with low latency, large capacity, and high speed. The core network forwarding plane further simplifies the sinking and moves the business storage and computing capabilities from the network center down to the network edge to support high traffic and low time delay business requirements, thus realizing flexible and balanced traffic load scheduling.

Main features and advantages: The 5G network is a new type of network based on the separation of control and forwarding. It improves the overall access performance of the access network in complex 5G-oriented scenarios, simplifies the core network structure, provides flexible and efficient control forwarding functions, supports high intelligence operations, opens network capabilities, and improves the overall service level of the entire network. The separation of the control and forwarding planes makes the network architecture flat, and the gateway device can be deployed in a distributed manner, thereby effectively reducing the service transmission delay. Different business scenarios have diverse performance and functional requirements for 5G networks. The 5G network can adapt to business scenarios and provide appropriate network control functions and performance guarantees for each 5G business scenario to achieve the goal of on-demand networking.

Applicability: 5G provides a reliable, open, and on-demand network for IIoT. The 5G network can efficiently support large-traffic services that are gradually emerging in industrial Internet, such as virtual factories and high-definition video remote maintenance. This network also supports the monitoring of a large number of devices inside and outside the factory, such as remote monitoring and control of various devices, remote control of wireless video surveillance, and remote monitoring and reporting of environmental parameters and control machinery data, to meet the needs of IIoT applications.

5. Information Model

The information model is used to define information representation, standardize data generated in industrial production, and facilitate communication between different devices and applications. The information model should clarify three levels of content: (1) define objects and the data contained in the objects, (2) organize these objects and data, and (3) define the data format. The information of each device in the digital factory includes various parameters of the device itself, runtime data, and data composition of the components in the device. This information is the object to be modeled.

The device information model can be divided into static attribute, dynamic attribute, and component assembly sets. The data in a device are defined by attributes, and the collection of all information contained in the device is called the attribute set. In the information model, information is divided into static and dynamic. Static information represents data that do not change or change slowly after definition. In the device, this type of information is mainly manifested as asset identification and order data (e.g., material coding and processing device number). Dynamic information represents data that are generated, disappear, or change in real time with the production process. It is generally in the form of device status data and part production process record data, such as working status, part processing size, logistics information, and start and completion times. In accordance with the static and dynamic nature of information, attributes are divided into static and process attributes. Static attributes form a static attribute set, and process attributes form a process attribute set.

Each attribute set contains attribute data of several information objects. Information objects are described by attributes, and attributes are composed of attribute elements. This defines the hierarchical structure of the information model, as shown in Figure 6. The elements of the information model are explained from small to large in Figure 6.

Attribute elements: These are the basic elements that make up attributes or the basic units of attributes, such as attribute identification, name, and data type.

Attribute: It pertains to the data describing the nature and characteristics of an object. Each attribute consists of multiple attribute elements, but not every attribute contains all attribute elements.

Information object: It refers to the body of information in the factory domain that describes a general, real, or abstract entity

that can be conceptualized as a whole. Examples of information objects are the spindle of a machine tool, the processing route of a certain part, and the receipt of a certain material. An information object completes its digital definition and digital description through its attributes.

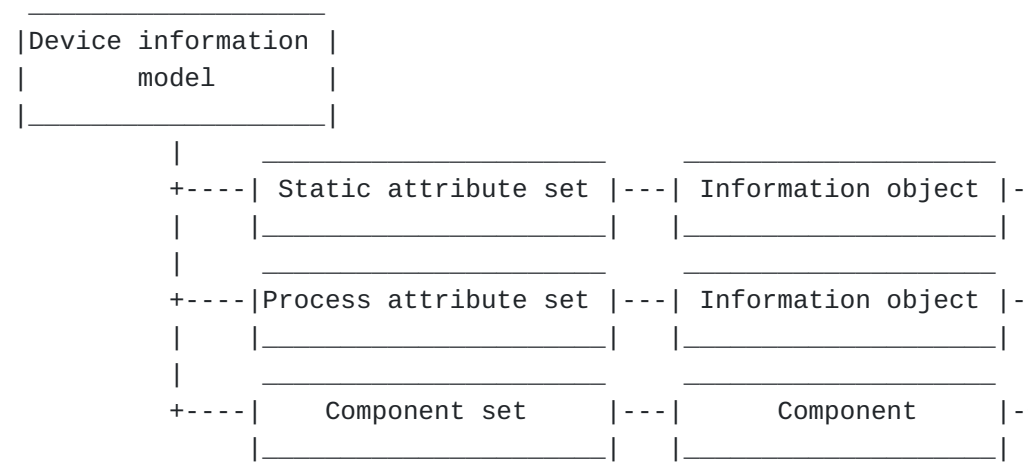

Figure 6: Information model

Attribute set: This is a collection of a series of attributes. The attribute set can be composed of sub-attribute sets or the attributes of several information objects. In accordance with the static and dynamic nature of information, the attribute set is divided into static and process attribute sets.

Component: It refers to a physical or logical object, which is a physical or logical part of the upper-level object, and its characteristics are described by the attribute set. Components can be nested, components can have their own subcomponents, and all subcomponents of the same object form a component set.

The device information model is an expandable tree structure that allows nesting between attribute sets and components. In this definition, the attribute set and the component set are structural elements that constitute the description of the factory information model. They are not a mapping of an actual object and do not contain actual content. They are only used to describe the framework and level of the organization model.

The device information model defined above is only an abstract framework. When modeling the information in an actual device and developing functions based on the information model, the actual device and function need to be based on the category and semantics of the frame. Various information model elements are filled to form an information model object with practical meaning. This process is called the instantiation of the information model. The implementation of the information model needs to be based on the specific description method and communication mechanism to realize the organization and storage of the instantiated information model. This section provides an information model implementation scheme based on the OPC UA protocol, as shown in Figure 7.

In accordance with the various information in the actual device, the device information is used model to model, and the OPC UA model generator is adopted to generate the corresponding XML file according to the established information model. The file is placed in the process model of the OPC UA server. The process model can obtain real-time data on the physical device through the data access module and save and update the value of the corresponding attribute in the information model.

The information model can be displayed through the address space of the OPC UA server, and the OPC UA client accesses the address space of the server to obtain the data defined by the information model. When the OPC UA client accesses or modifies the attribute information defined in the information model to the server, the UA service accesses or modifies the corresponding attribute information in the process model and returns the result to the OPC UA client.

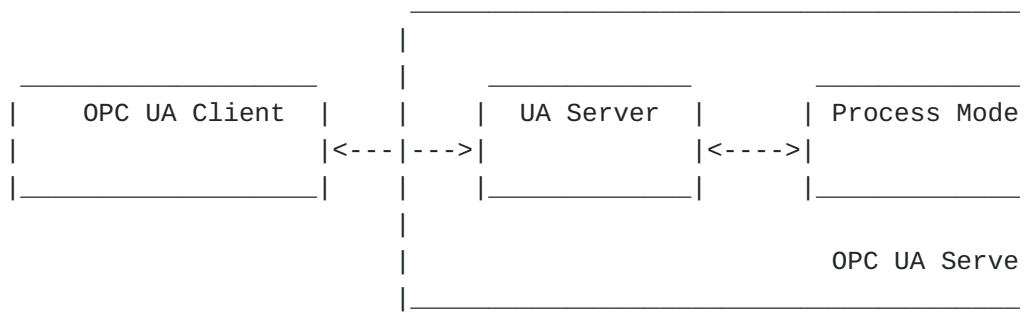

Figure 7: Information model realization scheme based on the OPC UA protocol

6. Security Challenges and Recommendations

With the rapid development of sensor networks, cloud computing, artificial intelligence, and 5G technologies, the number of network devices in the future will increase sharply, and the corresponding

market scale will be enlarged, which will cause corresponding security problems. These problems include information leakage, virus proliferation, and even the destruction of public infrastructure, such as the national grid, communication devices, and servers. Before these problems, the security of IIoT has not attracted much attention. The leakage of data collected by medical devices has aroused widespread discussions in today's Internet era. People are becoming increasingly aware of the importance of data security. With the recent extensive national-level management and control, much attention has been paid to the security of IIoT. This issue has also received attention from relevant agencies and enterprises in various countries. Regardless of life or technology, IIoT security is expected to become a problem that must be solved for future development.

The current IIoT architecture is roughly based on the classic three-tier model, which is divided into sensing, transport, and application.

6.1. Sensing Security

The sensing layer can perform sensing and collection of data in the physical world. It uses sensors, cameras, RFID, and other smart devices to realize data collection, and it achieves secure data transmission through limited and wireless networks. Its key technologies are RFID and sensor networks. The IIoT sensing front-end is responsible for real-time detection and collection of data and uploads the data to the cloud data center for processing through the transmission network. The presenter of the sense terminal is vulnerable to various security issues, such as virus intrusion, information leakage, and tampering. Therefore, weak terminals with a limited cost and performance should be equipped with two-way authentication, encrypted transmission, and remote upgrade capabilities. Terminals with strong resource performance should have strong security capabilities, such as security certificate management, antivirus, and intrusion detection. Smart factory application scenarios have low latency requirements and fast response to services. Therefore, efficient and lightweight security algorithms must be designed to deal with security threats. For example, PRESENT block ciphers [PRESENT], DES lightweight ciphers, KATAN/KTANTAN lightweight ciphers [KATAN], and LBlock [Lblock] provide different solutions.

6.2. Transport Layer Security

Consistent with the security requirements of the sensing layer, the task of the transport layer is to responsibly retransfer the data of the sensing layer to the application layer for processing. The task also requires the transmission network, the communication protocol,

and the network node that has been attacked (e.g., man-in-the-middle and counterfeit attacks), thereby causing node paralysis, which may further cause the leakage of communication keys and may affect the security of the entire network. The presence of many nodes and large amounts of data can easily cause network congestion and denial of service attacks, which could affect the transmission layer. Security has stringent requirements. Security issues, such as cross-network authentication, key negotiation, data confidentiality, and integrity protection of heterogeneous networks, are encountered due to the need for communication between networks with different architectures in the transport layer. Several confrontational security, homomorphic encryption, secure multi-party, and anonymization technologies are available.

6.3. Application Layer Security

The application layer is the highest layer of the architecture. The tasks implemented in it are numerous and complex, and the number of application categories, such as monitoring services, smart grids, industrial control, and green agriculture, differs. The application layer needs to process the data from the transport layer effectively. Given the massive data and network nodes of IIoT, huge storage and computing capabilities are required. Cloud computing technology can complete these tasks at a reduced cost. The current architecture is based on cloud computing. The processing response of business logic emphasizes the combination of IIoT and cloud computing. Therefore, cloud computing also has security issues, including platform data storage, exchange, processing, data security, and interaction issues arising from the connection of different platforms. At present, the cloud platform uses WAF, firewall, and HIDS. To a certain extent, it has played a role in data protection, but further security technical support is still required. The distributed architecture based on edge computing can share the computing burden, decrease the response time, and limit security risks to a certain area. It can reduce the security risk of the core network, so the application of edge computing presents a good opportunity. The cloud intelligent platform needs to deal with huge amounts of data. Many abnormal data and abnormal behaviors are difficult to detect and exclude. Security has a strong impact, and the use of various emerging technologies, such as data mining, machine learning, and AI, to analyze data can further detect data anomalies and improve data security. At the application level, many large enterprises have applications that collect a large amount of private data, such as health status, purchase behavior, travel routes, group contact, and value orientation, which also generate data privacy protection problems. Therefore, scholars have proposed homomorphic encryption algorithms. Blockchain also provides a new solution to this. For example, blockchain can realize anonymous sharing of IIoT devices [permissioned-blockchains]. It is widely

used in IIoT because it can effectively improve the lack of the traditional centralized data storage mode for IIoT. The full nodes of the blockchain network record complete data information to jointly maintain the data security of the IIoT device and reduce the traditional cost of maintaining a centralized database for IIoT application. The tamper-proof modification of blockchain technology and the timing guarantee the security and traceability of the data of the entire network node. The use of blockchain technology can thus ensure data privacy and security.

6.4. IIoT Security Solutions

By combining the security issues of the IIoT architecture, this section summarizes the existing security issues and corresponding solutions, which mainly include device protection, device identification, authentication mechanisms, secure communication mechanisms, data privacy protection, anomaly detection, and intrusion detection security status. The corresponding solutions are shown in Figure 8.

Security problem	Solutions
Device protection	Lightweight data encryption al
Device identification and authentication mechanism	RFID, blockchain
Secure communication mechanism	Edge computing, converged gate protocols, Homomorphic encrypt
Data privacy protection	Blockchain, encryption algorit computing
Anomaly detection and intrusion prevention	Machine learning, data mining

Figure 8: Security problems and solutions

7. Terms

This draft uses the following terms:

Cyber-physical systems (CPS) is a multi-dimensional complex system that integrates computing, network, and physical environments. Through the integrated design of computing, communication, and

physical systems, industrial systems become increasingly reliable and efficient and allow for real-time collaboration.

PROFIBUS is a fieldbus standard for automation technology.

Modbus is a serial communication protocol that has become the industry standard for communication protocols in the industrial field. It is now a common connection method between industrial electronic devices.

Highway addressable remote transducer (HART) is a communication protocol used between field intelligent instruments and control room devices.

EtherNet/IP is an industrial Ethernet communication protocol that can be used in program control and other automated applications.

PROFINET is an open industrial Ethernet communication protocol.

Data interoperability refers to the capability to enable distributed control system devices to coordinate their work through the digital exchange of related information to achieve a common goal.

Information integration refers to the integration of separate devices, functions, and information into an interconnected, unified, coordinated system through a structured integrated wiring system and computer network technology so that resources can be fully shared to realize centralized, efficient, convenient management.

Factory elements include various devices that appear in every link of industrial design, production, sales, and maintenance.

Industrial passive optical network (PON) is a passive optical network used in industries. It provides a comprehensive solution for the open platform of various industrial protocol conversions and the network connection in the factory to meet the requirements of various industrial scenarios and network applications of industries and enterprises.

Time sensitive networking (TSN) is a low-latency, high-reliability communication protocol based on the Ethernet/wireless network. It mainly works at the physical and data link layers for vehicle communication, industrial Ethernet, and other applications that provide infrastructure.

Edge computing refers to the use of an open platform that integrates network, computing, storage, and application core capabilities on the side close to the source of things or data to provide the nearest network service.

OPC unified architecture (OPC UA) is a machine-to-machine network transmission protocol used by the OPC Foundation for Automation Technology. It has the following characteristics:

*(1) The agreement focuses on communication for the purpose of information collection and control, which is used in industrial devices in the system.

*(2) Open source standard: The standard can be obtained for free, and the related device does not face licensing fees and other restrictions.

*(3) Cross-platform: No restrictions are imposed on operating systems or programming languages.

*(4) Service-oriented architecture (SOA).

*(5) Robust information security features.

*(6) Integrated information model. In information integration, by using the advantages of OPC UA service-oriented architecture, manufacturers and organizations can model their complex information in the OPC UA namespace.

WebSocket is a network transmission protocol that can carry out full-duplex communication on a single TCP connection and is located in the application layer of the OSI model.

UDP broadcast uses the UDP protocol to send messages to every host in the same broadcast network.

Message queuing telemetry transport (MQTT) is a message protocol based on the publish/subscribe (Pub-Sub) paradigm under the ISO standard and can be regarded as a "bridge for information transmission." It works on the TCP/IP protocol suite. It is a Pub-Sub message protocol designed for remote devices with low hardware performance and poor network conditions. For this reason, it needs message middleware, such as HTTP, to solve the current heavy workload.

Advanced message queuing protocol (AMQP) is an open application layer protocol for message middleware. Its design goal is to sort and route messages (including point-to-point and Pub-Sub), maintain reliability, and ensure safety.

Pub-Sub is a message paradigm. The sender of the message (called the publisher) does not send the message directly to the specific receiver (called the subscriber). Instead, messages are divided into different categories and published without knowing which subscribers exist. Similarly, subscribers can express interest in one or more

categories and only receive messages of interest without knowing which publishers exist.

Enterprise private lines have the characteristics of direct connection, and compared with ordinary access services, they possess higher speed, higher reliability, and better services.

Network virtualization is the process of combining hardware and software network resources and functions into a single software-based management entity (virtual network).

Automatic guided vehicle (AGV) is a type of wheeled mobile robot that moves along wires, markers, or magnetic strips on the floor or through visual or laser navigation. It is commonly used in industrial production to transport goods in workshops and warehouses.

Manufacturing execution system (MES) is a set of production information management systems for the executive level of the manufacturing enterprise workshop.

Product lifecycle management (PLM) is a complete, open, interoperable set of application programs in the entire process of product management, and it covers the product life cycle from product birth to death.

Enterprise resource planning (ERP) is a large-scale, modular, integrated, process-oriented system that integrates internal financial accounting, manufacturing, purchase, sales, and inventory information flows within the enterprise to quickly provide decision-making information and improve the company's operational performance and rapid response capabilities.

Supply chain management (SCM) is the management of material (product), information, and capital flows. SCM is an important component of enterprise operation management.

Customer relationship management (CRM) is a management system for the relationship between an enterprise and existing and potential customers.

Flexible manufacturing is an engineering manufacturing system that allows flexible and automated production due to predictable or unpredictable changes in the industry.

A transmitter is an instrument that converts non-standard electrical signals into standard electrical signals.

A remote terminal unit (RTU) is an electronic device controlled by a microprocessor and used as an interface of the device. It introduces

data into a distributed control system or a data acquisition and monitoring system (SCADA) and transmits remote measurement data to the main system. It also uses the data of the main monitoring system to control the connected device.

RFID is a wireless communication technology that can identify specific targets and read and write related data through radio signals without requiring mechanical or optical contact between the identification system and specific targets.

The conveyor line is an intelligent conveying system that uses PLC control technology through the system's automatic identification function and transmission system. The production material is conveyed with the best path and the highest speed.

The programmable logic controller (PLC) is a digital logic controller with a microprocessor for automation control.

The distributed control system (DCS) is a computerized control system used in factories. Generally, it entails several control loops, and autonomous controllers are scattered in the system without the monitoring by a central operator.

Gateway Initiated Dual-Stack Lite (GI DS-LITE) is an IPv4-in-IPv6 tunnel proxy technology that can realize IPv6 communication without modifying the terminal.

Homomorphic encryption is an encryption method that allows people to perform specific algebraic operations on ciphertext, and the result obtained is still encrypted. The result obtained by decrypting it is the same as performing the same operation on the plaintext. The result is the same.

The theory of secure multi-party computing focuses on collaborative computing between participants and the protection of private information. Its characteristics include input privacy, calculation accuracy, and decentralization.

*(1) Input privacy: When all parties are involved in collaborative computing, the privacy data of all parties are protected, with focus on the privacy and security of each party; that is, in the process of secure multi-party computing, it is necessary to ensure that the private input of each party is independent and that any local data will not be disclosed at any time when computing.

*(2) Calculation accuracy: For a certain agreed calculation task, the parties involved in the multi-party calculation perform collaborative calculations through the agreed MPC protocol. After

the calculation is completed, all parties receive correct data feedback.

*(3) Decentralization: In traditional distributed computing, the central node coordinates the computing process of each user and collects the input information of each user. In secure multi-party computing, all participants have equal status, and no privileged participant or third party exists. A decentralized computing model is provided.

Anonymization technology can realize the anonymity of personal information records, and identifying specific "natural persons" becomes impossible.

Web application firewall (WAF) is a product that provides protection for web applications by implementing a series of security policies for HTTP/HTTPS.

The host-based intrusion detection system (HIDS) is an intrusion detection system that can monitor and analyze the internal computing system and network packets in its network interface, similar to the operation mode of a network-based intrusion detection system.

8. IANA Considerations

This document does not require any actions by IANA.

9. Acknowledgments

We thank all the contributors and reviewers and are deeply grateful for the valuable comments offered by the chairpersons to improve this draft.

10. Informative References

[smart-factory] Chen, B., Wan, J., and S. Lei, "Smart factory of industry 4.0: key technologies, application case, and challenges", 2017.

[iiot-5g] Cheng, J., Li, D., and W. Chen, "Industrial IoT in 5G environment towards smart manufacturing", 2018.

[tsn] DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking, detnet., "https://tools.ietf.org/html/draft-ietf-detnet-ip-over-tsn-03", 2020.

[I-D.ietf-6lowpan-usecases] Design and Application Spaces for 6LoWPANs, ipv6., "https://tools.ietf.org/html/draft-ietf-6lowpan-usecases-10", 2012.

[edge-computing]
Mach, P. and Z. Becvar, "Mobile edge computing: a survey on architecture and computation offloading", 2017.

[I-D.ietf-core-coap-pubsub] Publish-Subscribe Broker for the Constrained Application Protocol, pubsub., "https://tools.ietf.org/html/draft-ietf-core-coap-pubsub-09", 2020.

[PRESENT] Bogdanov, A., Knudsen, L., and G. Leander, "PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems", 2007.

[KATAN] Canniere, C. and O. Dunkelman, "KATAN and KTANTAN -- A Family of Small and Efficient Hardware-Oriented Block Ciphers", 2009.

[Lblock] Wu, W. and Lei. Zhang, "Lblock: a lightweight block cipher", 2011.

[permissioned-blockchains] Hardjono, T., "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains", 2016.

Authors' Addresses

Chaowei Tang
Chongqing University
No. 174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: cwtang@cqu.edu.cn

Haotian Wen
Chongqing University
No. 174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: wenhaotianrye@foxmail.com

Shuai Ruan
Chongqing University
No. 174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: rs@cqu.edu.cn

Baojin Huang
Chongqing University
No. 174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: baojin-huang@foxmail.com

Xinxin Feng
Chongqing University
No. 174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: xxfeng@cqu.edu.cn