



**Question(s):** 2/20

Geneva, 1-12 July 2024

**TD**

**Source:** Editors

**Title:** Output text of draft Recommendation ITU-T Y.IIoT-infra-SM-fr “Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing”, Q2/20 meeting (Geneva, 1-12 July 2024) - for consent

**Contact:** Keng Li  
 CICT  
 China  
 Tel: +86 13907151603  
 E-mail: [kli@fiberhome.com](mailto:kli@fiberhome.com)

**Contact:** Yu Zhang  
 CICT  
 China  
 Tel: +86 13986098493  
 E-mail: [yzhang862@fiberhome.com](mailto:yzhang862@fiberhome.com)

**Contact:** Xiongwei Jia  
 China Unicom  
 China  
 Tel: +86 15611092296  
 E-mail: [jiawx9@chinaunicom.cn](mailto:jiawx9@chinaunicom.cn)

**Abstract:** This document contains the output text of draft Recommendation ITU-T Y.IIoT-infra-SM-fr “Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing” for consent, Q2/20 meeting (Geneva, 1-12 July 2024).

This updated version of draft Recommendation ITU-T Y.IIoT-infra-SM-fr “Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing” for consent, is the output of the Q2/20 meeting (Geneva, 1-12 July 2024). It is based on TD1219, output of Q2/20 e-meeting (Virtual, 15-17 and 20-21 May 2024), according to the July 2024 Q2/20 agreements on meeting discussions, including on the received contributions as follows:

No.	Source	Title	Proposals	Discussion and results
SG20-C453	China Information Communication Technologies Group (CICT), China Unicom	Y.IIoT-infra-SM-fr on “Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing”, proposed text for consent	This contribution proposes to modify text for consent.	The draft Recommendation was revised to reflect this contribution.

## **Draft Recommendation Y.4228 (ex Y.IIoT-infra-SM-fr)**

### **Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing**

#### **Summary**

Industrial Internet of things (IIoT) infrastructure for smart manufacturing refers to common facilities based on IoT that support smart manufacturing in industries or sectors. It is independent from the products and production process in specific enterprises. This Recommendation provides requirements and reference framework of the IIoT infrastructure capabilities for smart manufacturing to help service providers implementing their system according to the needs of smart manufacturing, and merge existing and newly developed IIoT infrastructure, in order to give the stakeholders of smart manufacturing guidance for their applications.

#### **Keywords**

IIoT, Industrial Internet of things, infrastructure, smart manufacturing

## CONTENTS

	<b>Page</b>
1	Scope.....4
2	References.....4
3	Definitions.....4
3.1	Terms defined elsewhere .....4
3.2	Terms defined in this Recommendation .....5
4	Abbreviations and acronyms.....5
5	Conventions .....8
6	Introduction of industrial Internet of things infrastructure .....8
6.1	Device layer .....9
6.2	Network layer .....10
6.3	Service support and application support layer .....13
6.4	Industrial SDN .....13
6.5	Identification facilities .....14
6.6	Security and information protection facilities .....14
7	Common characteristics and requirements of IIoT infrastructure for smart manufacturing .....15
7.1	Common characteristics.....15
7.2	High-level requirements .....17
7.3	Layer level requirements .....19
8	Reference framework of the IIoT infrastructure capabilities for smart manufacturing .....22
8.1	Reference framework.....22
8.2	Details on the capabilities .....25
9	Security considerations .....32
	Bibliography.....33

## Draft Recommendation Y.4228 (ex Y.IIoT-infra-SM-fr)

### Requirements and framework of Industrial IoT (IIoT) infrastructure for smart manufacturing

#### 1 Scope

This Recommendation introduces the concept of Industrial Internet of things (IIoT) infrastructure for smart manufacturing, analyses its requirements, and provides a reference framework of the IIoT infrastructure capabilities for smart manufacturing.

The scope of this Recommendation includes:

- concept, common characteristics and requirements of IIoT infrastructure;
- reference framework of the IIoT infrastructure capabilities for smart manufacturing.

#### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.
- [ITU-T Y.4003] Recommendation ITU-T Y.4003 (2018), *Overview of smart manufacturing in the context of the industrial Internet of things*.
- [ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.
- [ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

#### 3 Definitions

##### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 factory external network** [b-ITU-T Y.2623]: 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.

**3.1.2 factory internal network** [b-ITU-T Y.2623]: A network used for connection between the production factors, and between the corporate information technology (IT) management systems within a factory.

**3.1.3 Industrial Internet of things (IIoT)** [ITU-T Y.4003]: An Internet of things based enabling approach for industrial transformation, by taking advantage of existing and emerging information and communication technologies.

NOTE 1 – Emerging information and communication technologies include technologies for smart machines, robots, advanced industrial networks, industrial cloud computing and industrial data processing.

NOTE 2 – The industrial transformation enabled by the industrial Internet of things empowers the industry with, but not limited to, improved efficiency, intelligent production, reduced energy consumption, advanced collaboration modes and new business models. Industrial Internet of things enables smart manufacturing providing enhanced capabilities in support of manufacturing.

**3.1.4 Internet of things (IoT)** [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

**3.1.5 smart manufacturing** [ITU-T Y.4003]: A generic term for advanced processes, systems, methods and organizations throughout the manufacturing ecosystem based on advanced computing and manufacturing technologies, as well as existing and evolving interoperable information and communication technologies, aiming to integrate this ecosystem, innovate the development of products and services and improve the efficiency and reliability of manufacturing's life-cycle management, together with increasing performance, safety and environmental sustainability.

NOTE – The concept of smart manufacturing encompasses all aspects of the manufacturing activities, from design, sales, production, logistics and service.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

None.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4G	4 <sup>th</sup> Generation
5G	5 <sup>th</sup> Generation
ACL	Access Control List
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
API	Application Programming Interface
BGP	Border Gateway Protocol
BGP-LS	Border Gateway Protocol - Link State
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CoAP	Constrained Application Protocol
CRM	Customer Relationship Management
DCS	Distributed Control System
DMZ	Demilitarized Zone
DTLS	Datagram Transport Layer Security

DWDM	Dense Wavelength Division Multiplexing
E2E	End-to-End
EDP	Enhanced Device Protocol
ERP	Enterprise Resource Planning
FCS	Fieldbus Control System
Flowspec	Flow Specification
GRE	Generic Routing Encapsulation
HA	High Availability
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IaaS	Infrastructure as a Service
ID	IDentifier
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Invasion Protection System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
L2TP	Layer 2 Tunnelling Protocol
MES	Manufacturing Execution System
MPLS	Multiprotocol Label Switching
MQTT	Message Queuing Telemetry Transport
NB-IoT	NarrowBand Internet of Things
NETCONF	Network Configuration Protocol
NFV	Network Functions Virtualization
NoSQL	Not only SQL
OA	Office Automation
OAM	Operation, Administration and Maintenance
OID	Object IDentifier
ORS	OID Resolution System
OSI	Open Systems Interconnection
OT	Operational Technology
OTN	Optical Transport Network
PaaS	Platform as a Service

PC	Personal Computer
PCEP	Path Computation Element Communication Protocol
PDE	Packet Duplication and Elimination
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
PON	Passive Optical Network
QoS	Quality of Service
R&D	Research and Development
RFC	Request For Comments
RFID	Radio Frequency IDentification
RS	Recommended Standard
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SCM	Supply Chain Management
SDH	Synchronous Digital Hierarchy
SDN	Software-Defined Networking
SDO	Standards Development Organization
SD-WAN	Software-Defined Wide Area Network
SLA	Service Level Agreement
SM	Smart Manufacturing
SMPP	Short Message Peer-to-Peer
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SR	Segment Routing
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
ULSIN	Unified Large Scale Industrial Network
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VXLAN	Virtual eXtensible Local Area Network
WIA-FA	Wireless network for Industrial Automation - Factory Automation
WIA-PA	Wireless network for Industrial Automation - Process Automation
Wi-Fi	Wireless Fidelity
WPAN	Wireless Personal Area Network
YANG	Yet Another Next Generation

## **5 Conventions**

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement needs not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

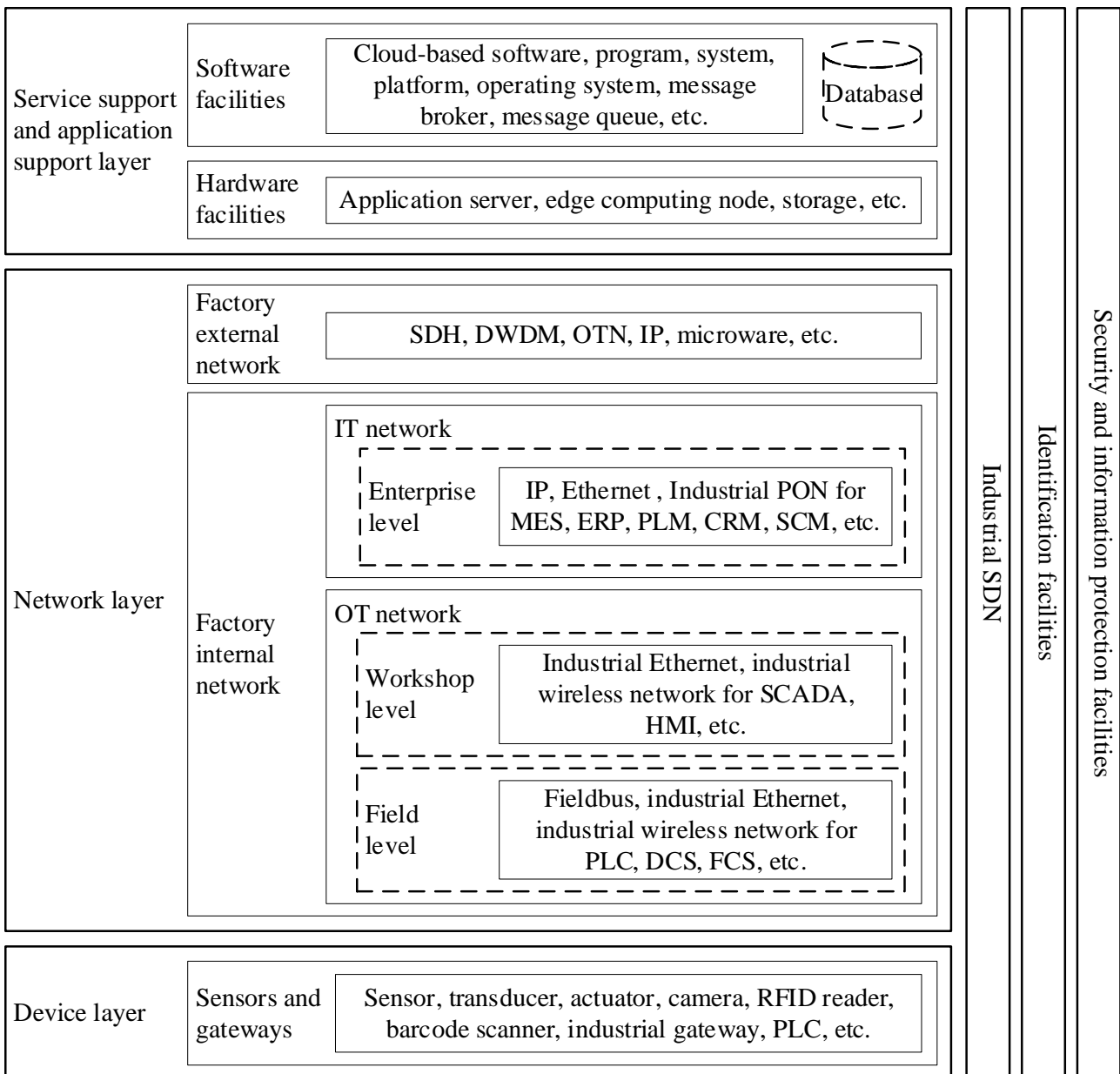
## **6 Introduction of Industrial Internet of things infrastructure**

Smart manufacturing provides an advanced production mode based on the deep integration of advanced manufacturing technology and new generation information technology, which run through the whole product life cycle such as design, production, sales, logistics and services. Smart manufacturing has the characteristics of self-perception, self-decision-making, self-performing, self-adaptation and self-learning, and it aims to improve the quality, efficiency and flexibility of manufacturing industry.

IIoT infrastructure plays a crucial role in smart manufacturing, and provides supporting smart manufacturing capabilities, as presented in [ITU-T Y.4003]. This clause introduces technical aspects with regard to the IIoT Infrastructure utilized for smart manufacturing.

NOTE – With respect to smart manufacturing, the IIoT constitutes a critical foundation. As an IoT-based enabling approach [ITU-T Y.4003], IIoT is the approach to support smart manufacturing, but the IIoT infrastructure is not specifically dedicated only to the support of smart manufacturing, i.e., other applications or industries can be supported by the IIoT infrastructure. However, there is a strong crossover between “IIoT” and “Smart Manufacturing” (SM) in terms of public recognition by global advanced manufacturing and IoT engaged standards development organizations (SDOs), organizations and other interested groups [b-ISO/IEC TR 30166].

Figure 1 depicts a conceptual framework of the IIoT infrastructure from the IoT and smart manufacturing points of view, based on the IoT reference model layering [ITU-T Y.4000]. The following clauses describe the facilities of the three layers, as well as the cross-layer facilities, of this framework.



**Figure 1 – Conceptual framework of the IIoT infrastructure from the IoT and smart manufacturing points of view**

## 6.1 Device layer

Due to many communication technologies in the industrial network, the relevant communication media in the IIoT infrastructure physical layer are very diverse. The devices connected in the industrial network are not only personal computers (PCs), printers and other equipment, but also industrial control and management equipment, such as industrial PCs, human machine interface (HMI), programmable logic controllers (PLCs), motion controllers, remote terminals, and radio frequency identification (RFID) equipment. These devices work at different layers or across multiple layers of the open systems interconnection (OSI) [b-ITU-T X.200] reference model, provide data in standardized or non-standardized format, receive control and adjustment signals from the upper layers, and perform comprehensive sensing and control of relevant hardware and processes in the industrial production environment.

These devices can be distinguished into sensors and gateways, which directly interact with machines, robotics, environment equipment and other field facilities for smart manufacturing production.

### 6.1.1 Sensors

They belong to different categories, such as sensors of resources, security, presence, lighting, motion, environment and position, and are installed on the physical facilities for smart manufacturing. These devices make it possible to collect and track status of smart manufacturing machines, operations, environment, etc., in order to help the facilities in the upper layers in gathering, processing, analysing and eventually generating valuable information throughout services for smart manufacturing.

### **6.1.2 Gateways**

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

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

## **6.2 Network layer**

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

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

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

The network layer consists of two sub-layers, factory internal network sub-layer and factory external network sub-layer [b-ITU-T Y.2623].

### **6.2.1 Factory internal network**

The factory internal network is the network inside the factory or the enclosed area for production, which is used to connect smart manufacturing related industrial resources [b-ISO/IEC TR 30166]: personnel (such as production personnel, designers and external personnel), machines (such as production equipment and office devices), materials (such as raw materials, semi-finished and finished products), processes (such as exchange of materials and control of production), environmental assets (such as instruments and monitoring equipment), etc. Through the factory internal network, these resources are interconnected with the enterprise data centre and application servers to support services and applications.

From the smart manufacturing point of view, the factory internal network encompasses operational technology (OT) network and information technology (IT) network [b-ITU-T Y.2623].

NOTE 1 – The OT network is a network which support hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices and systems, processes and events in the organization [b-ISO/IEC TR 23188]. The OT network mainly facilitates smart manufacturing and control, while the IT network mainly aims to connect office systems, mail servers, production management systems, data centres, and more [b-ITU-T Y.2623].

Given the industrial digitalization, to make optimal use of diverse industrial data, these data need to be comprehensively networked, which means interconnecting the OT network with the IT network. The OT network and the IT network are interconnected with each other via industrial gateways (such as firewalls, data-diodes and invasion protection systems (IPSS)) while enabling physical network isolation for security reasons [b-ITU-T Y.2623].

NOTE 2 – A common practice is to have a demilitarized zone (DMZ) between the OT network and the IT network.

The OT network encompasses the field level and the workshop level, while the IT network only relates to the enterprise level. Different levels of the factory internal network can meet functional requirements of different levels of management, and realize effective network management and control [ITU-T Y.4003]. Such multi-level network design promotes efficient support for manufacturing automation, achieving refined management and intelligent decision-making. Meanwhile, the multi-level network also helps establishing security isolation between different levels, protecting critical manufacturing data and systems from threats. The manageability, security and flexibility of the factory internal network can then be improved, in order to better supporting deep integration of industrial automation and informatization.

- 1) The field level of the OT network is responsible for connecting industrial field equipment. The field level network typically needs high reliability and real-time performances to ensure the continuity and stability of the production processes. The design of the field level network needs to consider the specific communication requirements of the industrial field equipment, such as resistance to electromagnetic interference and adaptability to environmental conditions.

As far as the field level of the OT network, the commonly used communication technologies are industrial fieldbus technologies, industrial Ethernet technologies and industrial wireless networking technologies.

The industrial fieldbus technologies (such as the fieldbus technologies described in IEC 61158-1 [b-IEC 61158-1], recommended standard 232 (RS232) [b-TIA-232] and RS485 [b-TIA-485]) are widely used to connect field detection sensors, actuators and industrial controllers. Industrial fieldbus technologies mainly provide data communication support from field sensors to controllers, controllers to actuators, or between controllers and each input/output (I/O) control substations, such as PLC, distributed control system (DCS) and fieldbus control system (FCS).

NOTE 3 – Comparing with other communication technologies, the industrial fieldbus technologies face some weaknesses, such as low communication ability, short distance, poor anti-interference ability and others. Their vulnerability to strong current interference, low reliability, obsolete maintenance mode, limitation of bandwidth and distance, and high cost of cable laying causes strong limitation of usage. However, industrial passive optical network (PON) [b-ETSI GR F5G 007] technology can be adopted for industrial fieldbuses. The industrial PON is based on optical communication technology, combined with capabilities of single or multiple level optical splitting and multiple terminals access via optical distribution network [b-ETSI GR F5G 007]. The industrial PON technology provides competitive performance for fieldbuses, and, further, it provides higher bandwidth and lower transmission delay than traditional fieldbus technologies.

The industrial Ethernet technologies (such as those based on the real-time Ethernet communication profiles described in [b-IEC 61784-2-3]) are customized and optimized communication technologies for industrial automation. Many industrial Ethernet protocols have gradually entered the control and communication applications in various industrial control systems. Their high communication performance and flexibility in network topology scale have laid a foundation for the improvement of industrial field control level.

The industrial wireless networking technologies include Wi-Fi [b-IEEE 802.11], Bluetooth [b-Bluetooth], wireless personal area network (WPAN), wireless network for industrial automation - process automation (WIA-PA) [b-IEC 62601], wireless network for industrial automation - factory automation (WIA-FA) [b-IEC 62948], RFID, narrowband Internet of things (NB-IoT) [b-3GPP TS 36.300], ISA-100.11a [b-ISA-100.11a]. They are mainly used in some non-critical industrial applications, such as applications for material transport, inventory management, patrol inspection, maintenance, and others. They connect mobile equipment in the enterprise where cable connection is difficult or impossible.

NOTE 4 – With the development of 5G, the performance indicators such as delay and reliability may require to be guaranteed for extreme industrial control applications. With the usage of such technologies, the 5G network can enlarge the scale of industrial wireless network applications, and enable full interconnection between the industrial wireless networks and the industrial fixed networks (e.g., industrial Ethernet based network).

- 2) The workshop level of the OT network is responsible for connecting industrial workshop equipment, such as controllers and systems. The workshop level network needs to handle more data, and support coordination and optimization of data within the workshop. The design of the workshop level network needs to consider the integration and flowing of data, as well as the interconnection and interoperability with the upper enterprise level network.

As far as the workshop level of the OT network, the workshop level network communication enables connectivity between controllers, between controllers and local or remote monitoring systems, and between controllers and operation level systems (such as supervisory control and data acquisition (SCADA) [b-SCADA] and HMI [b-ITU-T H.320]). The workshop level mainly adopts industrial Ethernet and industrial wireless networking technologies.

- 3) The enterprise level of the IT network is the top level of the factory internal network. The enterprise level network connects different workshops and enterprise level systems of the entire enterprise. The enterprise level network not only needs to handle a large amount of data and information, but also support advanced functions such as enterprise decision-making, resources management and strategic planning. The design of the enterprise level network needs to consider the scalability, security and connectivity to other networks.

As far as the enterprise level of the IT network, the commonly used communication technologies for network interconnection among enterprise level systems are high-speed Ethernet [b-IEEE 802.3], transmission control protocol / Internet protocol (TCP/IP) (request for comments (RFC) 1180 [b-IETF RFC 1180]) and industrial PON.

NOTE 5 – The enterprise level systems include manufacturing execution system (MES), enterprise resource planning (ERP), product lifecycle management (PLM), customer relationship management (CRM) and supply chain management (SCM).

### **6.2.2 Factory external network**

The factory external network is the network which is used to connect different entities of the smart manufacturing production cycle, including enterprise branches, enterprises and industrial data centres.

NOTE – As an example, the application servers of an industrial data centre inside an enterprise are interconnected with the industrial data centres outside the enterprise through the factory external network. As another example, enterprise branches and enterprises are connected to the industrial data centres inside an enterprise through the factory external network.

The factory external network can adopt different network technologies, including synchronous digital hierarchy (SDH) [b-ITU-T G.803], dense wavelength division multiplexing (DWDM) [b-ITU-T G.671], optical transport network (OTN) [b-ITU-T G.872], IP [b-IETF RFC 791] and cellular or satellite communication technologies. From the industrial perspective, the factory external network

provides dedicated lines, including Internet dedicated line, enterprise interconnection dedicated line and cloud dedicated line:

- The Internet dedicated line enables interconnection between enterprises and the Internet. This is the basic dedicated line for industrial enterprises.
- The enterprise interconnection dedicated line enables safe and reliable interconnection between enterprise branches and enterprises. This is commonly used by large and medium-sized enterprises.
- The cloud dedicated line enables interconnection between enterprises and cloud-based industrial data centres. It is usually a dedicated line from an enterprise to a cloud service provider.

### **6.3 Service support and application support layer**

The IIoT infrastructure part in the service support and application support layer consists of hardware facilities and software facilities.

These facilities as the infrastructure in the service support and application support layer provide capabilities of integration of users and resources (such as data and services) inside and/or outside the enterprise, and further provide capabilities of industrial data integration analysis, in order to support the various industrial applications. They are a critical foundation for building industrial ecosystems for smart manufacturing.

#### **6.3.1 Hardware facilities**

The hardware facilities in the service support and application support layer include different types of hardware such as application servers, edge computing nodes and storage. This is in order to help building hardware-type infrastructure for further building software-type infrastructure (the software facilities in the service support and application support layer).

The hardware facilities facilitate interconnections among devices and systems enabling collection of historical and real-time data, in order to achieve comprehensive and intelligent analysis.

#### **6.3.2 Software facilities**

The software facilities in the service support and application support layer include different types of software such as programs, systems, platforms, operating systems, message brokers, message queues and databases.

In this layer, the cloud-based software provides virtualized computing, storage and network resources, as well as fundamental cloud-based capabilities (such as distributed computing frameworks, cloud operating systems, development platforms for cloud-native applications, container engines, registries and container orchestration platforms), storage capabilities (such as distributed file systems and cloud databases), computing capabilities (such as big data programming paradigms and executing engines), and information system capabilities with help of coordination and cooperation mechanisms, in order to provide supporting capabilities for industrial services and applications. The users and industrial applications can use these resources and supporting capabilities.

### **6.4 Industrial SDN**

The industrial software-defined networking (SDN) [b-ITU-T Y.3300] uses network controllers to uniformly manage the network resources, so as to ensure the network quality of service required by applications. The key mechanism of the industrial SDN is to manage and configure networking devices through software definition.

With the utilization of advanced networking technologies, such as SDN and network functions virtualization (NFV) [b-ETSI NFV], the network can be virtualized. In this perspective, a SDN-based

network can have different logical slices, which provide network services with different service level agreements (SLAs) [b-ITU-T M.1301]. And these network services can be rapidly deployed, adjusted and recycled with high quality of service (QoS) [b-ITU-T E.800] guarantees.

The industrial SDN is used throughout the device layer, the network layer and the service support and application support layer. The industrial SDN network is composed of terminal equipment in the device layer, programmable industrial SDN devices in the network layer and industrial SDN controllers in the service support and application support layer. A terminal equipment submits the data flow characteristics and transmission requirements to the appropriate industrial SDN controller(s) through the northbound interface. The industrial SDN controller(s) generates the forwarding rules of the industrial SDN network according to the received data flow characteristics and transmission requirements, and the forwarding rules are implemented in the programmable industrial SDN devices through the standardized southbound interface.

NOTE – The industrial SDN may support one or multiple network controllers. There are different types of northbound interfaces [b-ONF TR-523] and southbound interfaces of the network controllers, those network controllers controlling the networking devices via southbound interfaces (using protocols such as network configuration protocol (NETCONF) [b-IETF RFC 6241], yet another next generation (YANG) [b-IETF RFC 6020], border gateway protocol – link state (BGP-LS) [b-IETF RFC 9085], BGP flow specification (BGP Flowspec) [b-IETF RFC 8955], segment routing (SR) [b-IETF RFC 8402] and path computation element communication protocol (PCEP) [b-IETF RFC 5440]). Due to different types or manufacturers of the networking devices (such as industrial switches, routers, gateways, firewalls, IPSs, virtual switches, industrial PON and OTN), it may be complex to handle multiple protocols of northbound and southbound interfaces by a single network controller to achieve interoperability, so multiple network controllers may be used, which can be categorized as domain controllers and super controller. Each domain controller is intended to handle a part of the network (a domain), while the super controller is intended to control all the domain controllers, in order to realize cross domain management and coordination of the networking devices.

The IT network and the OT network in the enterprise are traditionally operated independently of each other, the topologies of both networks are rigid, and the cross-network information interaction and management are very difficult. The industrial SDN enables the deep integration of the IT network and the OT network in order to build a flexible and agile industrial network. The equipment and traffic in the IT network and the OT network can be uniformly monitored and managed.

## **6.5 Identification facilities**

As one of the components of the IIoT infrastructure for smart manufacturing, the identification facilities provide identification capabilities for identification of physical and logical resources.

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

## **6.6 Security and information protection facilities**

The security and information protection facilities provide security and information protection capabilities for the different enterprise functions, including device authentication and authorization, physical security, functional security and information security.

Those facilities are mainly used to protect various physical or virtual industrial resources, data analysis services, development kits, industrial applications, etc. They run through all the three layers of the IIoT infrastructure and address the different dimensions of security, including reliability, confidentiality, integrity, availability and information protection.

## **7 Common characteristics and requirements of IIoT infrastructure for smart manufacturing**

### **7.1 Common characteristics**

The common characteristics of the IIoT infrastructure for support of smart manufacturing include:

#### **7.1.1 Integration**

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

The common integration characteristics of the IIoT infrastructure are as follows:

- The IIoT infrastructure is based on ubiquitous perception, comprehensive connection and deep integration.
- The IIoT infrastructure supports the collaboration of different businesses such as research and development (R&D), production and management inside the enterprise.
- The IIoT infrastructure explores the optimal operation efficiency of the enterprise.
- The IIoT infrastructure supports the collaboration of production resources and social resources outside the enterprise.
- The IIoT infrastructure explores the optimal industrial resource allocation efficiency, and finally enables the capabilities of global collaboration.

#### **7.1.2 Compatibility**

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

NOTE 1 – The overlay mode is overlaying a new network and related equipment supporting the new business processes on the existing facilities to build another system other than the original system (e.g., deploying new monitoring equipment, sensing equipment and execution equipment on the existing industrial infrastructure to realize safety monitoring, data acquisition, analysis and optimization).

NOTE 2 – The upgrading mode is upgrading the existing industrial facilities, network equipment and platform to realize the upgrading of system technologies and capabilities (e.g., at the process manufacturing site, original analog instruments can be upgraded and replaced with intelligent instruments supporting 4G/5G, in order to realize the intelligent collection and aggregation of on-site data and the unmanned operation of dangerous sites).

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

The network of the IIoT infrastructure supports the capability of upgrading to, and to be compatible with networks enabling advanced technologies such as time-sensitive networking (TSN) [b-IEEE 802.1 TSN] and SDN.

#### **7.1.3 Scalability**

The IIoT infrastructure supports the flexibility and scalability capabilities of computing, storage, and network resources. Those IIoT resources can be automatically scaled according to the business load,

in order to adapt to the continuous evolution of functional modules, data resources and application capabilities.

#### **7.1.4 Efficiency and high performance**

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

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

#### **7.1.5 Heterogeneous connectivity**

The IIoT infrastructure meets the heterogeneous capabilities of the facilities in different layers of IIoT infrastructure in Figure 1, such as data collection and control devices in the device layer, diverse network type connectivity in the network layer and diverse computing and storage resources in the service support and application support layer, in order to provide services and capabilities across heterogeneous systems.

#### **7.1.6 Interoperability**

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

#### **7.1.7 Operational safety and reliability**

The IIoT infrastructure supports operational safety capabilities such as endpoint protection, communication and connection protection, operational safety monitoring, analysis, configuration and management, and data protection.

NOTE 1 – Operational safety refers to the aspects of safety that relate to the correct operation of a system or that are provided by the system itself [ITU-T Y.4003].

The IIoT infrastructure can realize high reliability of the hardware and software facilities. When a single hardware or software facility fails, it can ensure business continuity.

NOTE 2 – Reliability refers to the probability that the system operates correctly for a given period of time in a given environment [ITU-T Y.4003].

#### **7.1.8 Security and sensitive information protection**

The IIoT infrastructure supports capabilities to ensure security of facilities, control, network, applications and data. It supports comprehensive security capabilities such as system connection, system collaboration, data sharing and business cooperation.

The IIoT infrastructure supports capabilities to prevent production facilities and products from misuse and unauthorised access [ITU-T Y.4003].

The IIoT infrastructure supports capabilities of protection of IIoT users' personal information and protection of enterprises' sensitive information.

#### **7.1.9 Flexible and secure identification management and communication**

An ID-based network can be leveraged to run through facilities in all the three layers of the IIoT infrastructure as shown in Figure 1, forming an ID registration and resolution system (such as the object identifier (OID) resolution system (ORS) [b-ITU-T X.672], the GS1 identification system [b-GS1] and the Handle System [b-IETF RFC 3650]), in order to identify and resolve diverse IDs of physical and logical resources. The common characteristics of this system are as follows:

- The ID registration and resolution system supports the unified operation, administration and maintenance (OAM) of diverse identifiers.

NOTE – The identifiers of the ID registration and resolution system can uniquely identify physical and logical resources for smart manufacturing. The physical resources include, but are not limited to, materials, machines and products, while the logical resources include, but are not limited to, production processes, software, digital models and data.

- The ID registration and resolution system supports the registration and resolution of diverse identifiers.

In order to provide flexible, efficient and trusted networking and communication capabilities, the IIoT infrastructure provides capabilities to support multiple network technology types (such as virtual local area network (VLAN) [b-IEEE 802.1Q] and virtual extensible local area network (VXLAN) [b-IETF RFC 7348]), multiple encryption security protocols (such as transport layer security (TLS) [b-IETF RFC 8446] and datagram transport layer security (DTLS) [b-IETF RFC 9147]), multiple tunnelling protocols (such as Internet protocol security (IPsec) [b-IETF RFC 4301], layer 2 tunnelling protocol (L2TP) [b-IETF RFC 3931], generic routing encapsulation (GRE) [b-IETF RFC 2784], software-defined wide area network (SD-WAN) [b-ITU-T Q.3741] and multiprotocol label switching virtual private network (MPLS VPN) [b-IETF RFC 4364]), and Internet protocol version 4 (IPv4) [b-IETF RFC 791] / Internet protocol version 6 (IPv6) [b-IETF RFC 8200] dual stack.

#### **7.1.10 Customized application support**

The IIoT infrastructure mainly focuses on the upstream and downstream cooperation within the industrial chain, the common characteristics for customized application support are as follows:

- The IIoT infrastructure provides reusable services.
- The IIoT infrastructure supports a digital catalogue of reusable services and mechanisms for discovery of services and service access endpoints.
- The IIoT infrastructure supports an access control policy management system that enables creation and management of policies related to access of services by different users and privileges.
- The IIoT infrastructure supports the production and operation activities facing the whole industrial chain (such as R&D, production and manufacturing, supply chain, logistics and product operation and maintenance).
- The IIoT infrastructure carries out the transaction of data and services throughout supply and demand, in order to realize information sharing and service collaboration within and among enterprises.

## **7.2 High-level requirements**

The high-level requirements of the IIoT infrastructure for support of smart manufacturing are as follows.

### **7.2.1 Requirements for integration capabilities**

The IIoT infrastructure is required to support capabilities of integration - including collaboration - as opposed to an isolated and silo-based approach of system development and deployment.

The IIoT infrastructure is required to have the ability to support an ecosystem that includes all relevant stakeholders in the manufacturing value chain.

### **7.2.2 Requirements for compatibility**

The IIoT infrastructure is required to be compatible with existing facilities to interact with.

This includes identification capabilities compatible with heterogeneous identification systems.

### **7.2.3 Requirements for scalability**

The IIoT infrastructure is required to be upgradable and expandable (diversity and number of devices, facilities, capabilities) according to the changing requirements of applications without significant impact on operational performances such as real-time, non real-time and high reliability performances, for continuous easy to use and maintain.

#### **7.2.4 Requirements for efficiency and high performance**

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

The IIoT infrastructure is required to be efficient in terms of operations (data and functions).

#### **7.2.5 Requirements for heterogeneous connectivity**

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

#### **7.2.6 Requirements for interoperability**

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

#### **7.2.7 Requirements for operational safety and reliability**

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

#### **7.2.8 Requirements for security and sensitive information protection**

The IIoT infrastructure is required to support protection of production facilities and products from impermissible physical influences, e.g., protection against the entry into a room from unauthorized persons [ITU-T Y.4003].

The IIoT infrastructure is required to support protection of the information and communication technology capabilities from impermissible influences via the communication interfaces of production facilities [ITU-T Y.4003].

The IIoT infrastructure is required to support protection of information from loss and misuse, insurance of its timely provision to entitled users and maintenance of its integrity and confidentiality [ITU-T Y.4003].

The IIoT infrastructure is required to provide protection of sensitive information. This includes protection of identities in the different identity management activities.

#### **7.2.9 Requirements for flexible and secure identification management and communication**

The IIoT infrastructure is required to support flexible and secure identification management and communication according to the diversity of applications and facilities.

The encoding and resolution mechanism of the ID registration and resolution system is required to be compatible with the encoding and resolution mechanisms of existing ID registration and resolution systems.

ID-based network communication is required to enable various security functions (such as authentication, authorization and access control) and protect sensitive information of the communication objects.

#### **7.2.10 Requirements for customized application support**

The IIoT infrastructure is required to provide application developers with development support environment, operation support environment, service invocation and orchestration support, service operation management, multiple tenant management and other support functions.

Customized applications can obtain data, analysis and processing capabilities provided by the IIoT infrastructure through unified interfaces (such as application programming interfaces (APIs) and web services).

### **7.3 Layer level requirements**

The following sub-clauses identify the layer level requirements of the IIoT infrastructure for support of smart manufacturing.

#### **7.3.1 Device requirements**

The device layer facilities provide the bottom layer I/O interfaces for communication and interaction between and among smart manufacturing facilities and upper layer facilities of the IIoT infrastructure. The device layer facilities include basic functions (such as data perception, data identification, device control and execution) and specific smart manufacturing support functions (such as massive industrial data access, data conversion, data pre-processing and edge analysis).

The device layer facilities are required to have the ability to support a variety of software and hardware methods for data collection. Collected data include assets properties, status and behaviour, e.g., temperature change data collected by temperature sensors during motor operation.

The device layer facilities are required to set up linkage between data and assets to define the objects represented by data. For example, it is necessary to clearly identify which sensor data represents the temperature information of a specific motor.

The device layer facilities are required to have the ability to convert the expected target action into control signals. For example, the motions of the industrial robotic arm are converted into the rotation angle command signals of the motors.

The device layer facilities are recommended to have the ability to change the asset status in the physical environment according to the control signals, including changing the mechanical and electrical status of industrial equipment, as well as changing the operational processes for personnel and supply chains.

The device layer facilities are required to have the ability to access massive industrial data, including data access capabilities for industrial equipment (such as robotics, machine tools and blast furnaces) and information systems (such as MES and ERP), in order to realize large-scale and comprehensive collection and interconnection of various industrial data.

The device layer facilities are recommended to have the ability to unify the format, and parse the semantics, of multi-source heterogeneous collected data, and conduct data cleaning, compression, caching and other operations before transmitting them to the upper layer facilities.

The device layer facilities are recommended to cope with real-time application scenarios, carry out real-time analysis and feedback control signals at the edge, and provide capabilities (such as resource scheduling, operation, maintenance, development and debugging) for edge application development.

#### **7.3.2 Network requirements**

As described in clause 6, the network (part) of the IIoT infrastructure can be divided into factory internal network and factory external network.

The factory internal network can be further divided into IT network and OT network. The OT network consists of different levels and at each level different network technologies may be used. For instance, at the field level, various proprietary fieldbus and industrial Ethernet technologies are used to build manufacturing cells, a kind of small-scale local network, in order to support dedicated industrial control functions. As those proprietary protocols are not compatible among each other, the field level inter-connection and communication are not straightforward and can bring extra complexity to the management of the overall industrial system.

In fact, the IIoT demands the IT-OT convergence [b-ITU-T Y.2623] [b-ISO/IEC TR 30166] [b-IIRA] [b-Cigref] in order to make the manufacturing systems more flexible and intelligent. This allows traditional manufacturing equipment to communicate beyond their own manufacturing cells and even the geographical boundaries of enterprises or other industrial installations, thus enabling the remote monitoring, analysis and control of physical devices. To enable the “true” IT-OT convergence by breaking the barriers of the proprietary protocols and the interoperability by facilitating the communication among factory internal network and factory external network, a unified large scale industrial network (ULSIN) is required as the network part of the IIoT infrastructure for support of smart manufacturing.

The ULSIN is required to interconnect the factory internal network with the factory external network by industrial firewalls and gateways, in order to control appropriately the shared information from the factory internal network and protect against the threats from the factory external network.

The ULSIN is required to support different network technologies, in order to provide comprehensive connectivity for the interconnection of the smart manufacturing ecosystem entities.

The ULSIN is recommended to integrate all different devices, including drives, I/O modules, machines, servers, robot arms and others, into one network and support seamless communication among them. Comparing with isolated manufacturing cells, each device in the IIoT infrastructure for manufacturing is recommended to be uniquely identified and reachable within the ULSIN. Among others, this can greatly increase the flexibility of the industrial control application design and enable the communication among different production units, which is hard to achieve in existing manufacturing systems.

The ULSIN is recommended to support the interoperability of the existing industrial infrastructure and devices. Since the existing industrial networks using diverse proprietary protocols are typically working in the physical and data-link layers, the ULSIN provides the capabilities required by the IIoT infrastructure in the network layer, thus avoiding the direct conflict with the existing industrial networks. This enables integration of the existing industrial network technologies, such as fieldbuses, industrial Ethernet and wireless communication technologies, into the ULSIN without or with minimum adaptation, as well as seamless connectivity with other networks (located inside or outside the IIoT infrastructure borders).

NOTE 1 – The ULSIN supports the interoperability with the existing industrial infrastructure and devices by providing common network layer capabilities, avoiding the need for gateways which are typically non-scalable. The application-level communication interoperability doesn’t fall into the scope of ULSIN, being related to the upper layers of the network layer.

The ULSIN is recommended to provide high performance in terms of bandwidth, latency and jitter, in order to support a large diversity of industrial services and applications: industrial services and applications usually don’t demand high bandwidth, but are sensitive to latency; motion control applications typically run at a cycle time of sub-milliseconds, while other real time industrial applications do it at a cycle time from 1ms to 100ms; although non real time applications don’t demand low latency, they may require time deterministic transmission, similarly to other industrial applications.

The ULSIN is recommended to be capable of supporting real time industrial applications at the network layer. For motion control applications, whose control functions typically run at a cycle time of sub-milliseconds, it is recommended to leverage data link layer technologies like TSN. And the ULSIN is recommended to support motion control applications by bridging TSN networks.

The ULSIN is recommended to provide high reliability of the network level communications, according to the requirements of a large diversity of industrial services and applications. Differently from a network for residential users, an industrial system typically requires high reliability (from 99.999% to 99.99999%), including for the industrial network part, as unexpected or unintended

service interruptions caused by network level failures could lead to huge loss in terms of production and business value.

NOTE 2 – The packet duplication and elimination (PDE) technology specified in the TSN standards [b-IEEE 802.1 TSN] can be used to improve the reliability of the system at the expense of hardware infrastructure duplication. The Protection Switching technology specified in the ITU-T G.8031 standard [b-ITU-T G.8031] is another candidate, although the current specification doesn't meet the requirements of real-time industrial applications while it can be used for non real-time industrial application like automated guided vehicle (AGV).

### **7.3.3 Service support and application support requirements**

The service support and application support layer facilities provide support capabilities of integration, interconnection and information fusion to fulfil the requirements of industrial digital transformation.

NOTE – These facilities also integrate technologies such as edge-cloud collaboration, big data, artificial intelligence (AI) and microservices, in order to provide support for services and applications.

The service support and application support layer facilities are required to provide high quality data resources for modelling and analysis.

The service support and application support layer facilities are required to support system integration capabilities, in order to facilitate intensive utilization of data from different sources.

The service support and application support layer facilities are recommended to support human-computer interaction, in order to enhance user experience.

The service support and application support layer facilities are required to provide resource management capabilities including resource scheduling, operation and maintenance management.

The service support and application support layer facilities are required to provide industrial data and model management capabilities (such as data governance, data sharing and data visualization).

The service support and application support layer facilities are required to provide management capabilities for conducting retrieval, classification and identification of industrial data and models.

The service support and application support layer facilities are recommended to integrate industrial modelling methods (such as application simulation analysis and service processes) and data science modelling methods (such as statistical analysis, data modelling based on big data and AI technologies), in order to realize in-depth mining and analysis of industrial data value.

The service support and application support layer facilities are recommended to integrate tools for R&D, design, production management and operation management, as well as other tools (such as computer aided design (CAD), computer aided engineering (CAE), MES and ERP).

The service support and application support layer facilities are recommended to adopt low code development, graphical programming and other technologies to facilitate development, which can support application personnel for carrying out efficient and flexible industrial application innovation.

### **7.3.4 Industrial SDN requirements**

The industrial SDN provides support capabilities for the network layer of IIoT infrastructure. It is used for agile and flexible OAM of network, and provides network services of high reliability and comprehensive interconnection.

The industrial SDN is recommended to adopt a simplified network architecture, in order to enable flexible and simple network management.

The industrial SDN is required to support the comprehensive connection of devices with different communication protocols, including devices that apply standard IP and Ethernet protocols, devices that apply industrial Ethernet protocols and devices that apply other communication protocols. The

industrial SDN is required to identify and classify these protocols by programmable network devices, and forward data according to these protocols.

The industrial SDN is required to support flexible networking of network devices.

NOTE 1 – When communication relationships among network devices change, industrial SDN uses software-defined methods to modify forwarding rules, in order to quickly adapt to new networking modes and communication relationships.

The industrial SDN is required to meet the transmission requirements of IT network services (such as control, collection and connection services) and OT network services (such as office automation (OA), Internet, fixed phone, video/audio conferencing and internal systems interconnections) at the same time, such as IT network services with high bandwidth requirements and OT network services with real-time and high reliability requirements.

NOTE 2 – The industrial SDN centralized controller allocates network resources according to different transmission requirements, and manages them through bandwidth limitation, priority configuration and other OAM methods.

The industrial SDN controller is required to detect connection of the network devices, analyze network failures and improve network security through traffic tracking and abnormal traffic monitoring.

NOTE 3 – This is in order to provide unified capabilities for the IT-OT converged network, such as management of topologies, alarms, performances, audits and reports.

The industrial SDN is recommended to support management visualization of the network.

### **7.3.5 Identification requirements**

The ID registration and resolution system, which is introduced in clause 7.1.9, is required to provide capabilities of ID data collection, ID management, ID registration, ID resolution and ID data processing.

### **7.3.6 Security and information protection requirements**

Security and information protection requirements of the IIoT infrastructure are in line with the security and information protection requirements of the IoT, which refer to the functional requirements during capturing, storing, transferring, aggregating and processing the data of things, as well as to the provision of services which involve things [ITU-T Y.4100].

The IIoT infrastructure is required to provide security and information protection capabilities at the different layers of the IIoT infrastructure framework. These capabilities include support of communication security, data management security, service provision security, integration of security policies and techniques, mutual authentication and authorization, and security audit [ITU-T Y.4100].

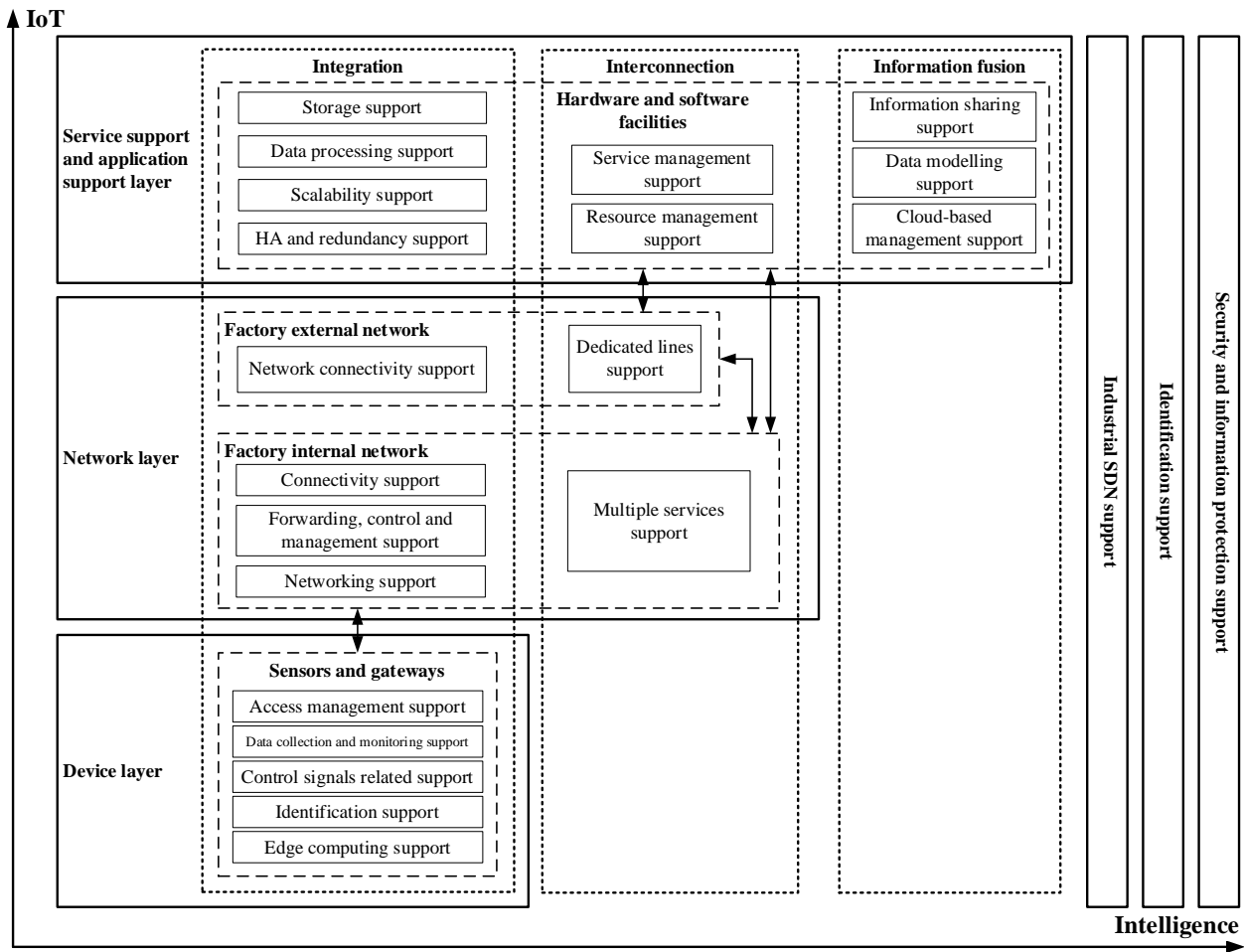
## **8 Reference framework of the IIoT infrastructure capabilities for smart manufacturing**

### **8.1 Reference framework**

This clause describes a reference framework of the IIoT infrastructure capabilities.

The reference framework integrates the intelligence enablement with the different layers of the IIoT infrastructure. This reference framework is built according to the two dimensions of intelligence [ITU-T Y.4003] and IoT [ITU-T Y.4000].

Figure 2 illustrates the reference framework of the IIoT infrastructure capabilities for smart manufacturing.



**Figure 2 – Reference framework of the capabilities of IIoT infrastructure for smart manufacturing**

The IoT dimension in Figure 2 concerns different layers of IIoT infrastructure, according to the IoT reference model [ITU-T Y.4000], providing capabilities to support industrial services and applications.

NOTE 1 – The industrial services and applications are not part of the IIoT infrastructure, they are supported by the IIoT infrastructure.

NOTE 2 – The management capabilities of IIoT infrastructure are not positioned as cross-layer management capabilities as in the IoT reference model [ITU-T Y.4000], but are distributed across the three layers of the IoT dimension in order to provide a clear representation with regards to the intelligence dimension.

The intelligence dimension in Figure 2 concerns the enablement of different layers of intelligence (smart capabilities) in the IIoT infrastructure, from intelligence at integration layer to intelligence at information fusion layer. By means of the IIoT infrastructure, those smart capabilities can be enabled for smart manufacturing.

NOTE 3 – In the reference model of smart manufacturing in the context of the industrial IoT [ITU-T Y.4003], apart from the smart manufacturing applications and resources layers which concern, respectively, diverse applications based on different enterprise characteristics and diverse resources without generic characteristics, the integration, interconnection and information fusion layers are directly related to the IIoT infrastructure.

NOTE 4 – The resources and smart manufacturing applications layers in the intelligence dimension of the smart manufacturing reference model focus, respectively, on the smart manufacturing resources

and innovative industrial application patterns, which are highly related to the specific production processes and industrial applications of smart manufacturing. The smart manufacturing resources and applications in different industrial environments may have totally different characteristics and capabilities, they do not constitute the general infrastructure of IIoT. On the other hand, the IIoT infrastructure concerns the digitalization of smart manufacturing resources and the application innovation with respect to the common requirements for support of general capabilities.

The following clauses describe the two dimensions of the reference framework.

### **8.1.1 IoT dimension**

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

- 1) The “device layer” represents devices, such as sensors and gateways. It is the physical foundation of the data collection facilities. It supports the basic level of intelligence in the integration layer of the intelligence dimension. It provides capabilities of access management support, data collection and monitoring support, control signals related support, identification support and edge computing support, which are provided respectively in clause 8.2.1.
- 2) The “network layer” represents the network infrastructure between the devices and the service support and application support layer facilities, and it is composed by the factory internal network and the factory external network.

The factory internal network interconnects facilities in the device layer, the factory external network and the service support and application support layer. It supports the integration layer and the interconnection layer of the intelligence dimension. It provides capabilities of connectivity support, capabilities of forwarding, control and management support, and capabilities of networking support at the integration layer of the intelligence dimension, as well as capabilities of multiple services support at the interconnection layer of the intelligence dimension. These capabilities are provided respectively in clause 8.2.2.

In addition to the factory external network interconnection with the factory internal network, the factory external network also interconnects facilities of the service support and application support layer, and exchanges data with facilities of the factory internal network and the service support and application support layer. According to the different layers of the intelligence dimension, the capabilities of the factory external network include network connectivity support at the integration layer of the intelligence dimension, and dedicated lines support at the interconnection layer of the intelligence dimension. These capabilities are provided respectively in clause 8.2.3.

- 3) The “service support and application support layer” represents the infrastructure composed by the hardware and software facilities for supporting services and applications. According to the different layers of the intelligence dimension, the capabilities of the service support and application support layer include storage support, data processing support, scalability support, and high availability (HA) and redundancy support at the integration layer of the intelligence dimension. The capabilities of the service support and application support layer include service management support and resource management support at the interconnection layer of the intelligence dimension. The capabilities of the service support and application support layer include information sharing support, data modelling support and cloud-based management support for comprehensive information integration and fusion at the information fusion layer of the intelligence dimension. These capabilities are provided respectively in clause 8.2.4.

NOTE – Appropriate technologies such as cloud computing, big data, AI, digital twin, information security and other emerging information technologies are key enablers for the depth and breadth of information fusion, in order to achieve smart manufacturing.

The cross-layer capabilities include industrial SDN support and support of identification and security and information protection.

The industrial SDN support capabilities, which cross the network layer and the service support and application support layer, provide the support for uniform management of the network resources, and for facilitating the IT-OT convergence, in order to enable agile and flexible industrial network. These capabilities are provided in clause 8.2.5.

On the premise of identification and security and information protection, the IIoT infrastructure provides capabilities of identification support, and security and information protection support, throughout all the three layers of the IoT dimension. These capabilities are provided in clause 8.2.6 and 8.2.7.

### **8.1.2 Intelligence dimension**

The intelligence dimension concerns three layers: integration, interconnection and information fusion.

- 1) The “integration” layer enables the fundamental integration capabilities from data collection and data exchange to data storage and data management, with respect to the facilities of all layers in the IoT dimension.

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

In the network layer, via interconnection between the factory internal network and the factory external network, the integration layer realizes reliable transmission of data.

In the service support and application support layer, via comprehensive integration of the hardware and software facilities, the integration layer supports diverse services and applications.

- 2) The “interconnection” layer enables interconnection capabilities with respect to the network layer and the service support and application support layer in the IoT dimension.

In the network layer, the interconnection layer supports the interconnection of the entities of the smart manufacturing ecosystem.

In the service support and application support layer, the interconnection layer supports management capabilities for services and resources.

- 3) The “information fusion” layer enables information interconnection and coordination capabilities throughout enterprises, with respect to the service support and application support layer in the IoT dimension.

In the service support and application support layer, the information fusion layer supports information fusion for services and applications.

## **8.2 Details on the capabilities**

Details of the IIoT infrastructure capabilities are provided in this clause according to the IoT dimension layering of Figure 2.

### **8.2.1 Device capabilities**

- 1) Access management support

- support of access management with different security strategies, including, but not limited to, authentication, authorization, encryption and protection;

- support of necessary authentication and authorization processes of the connected objects, and interception of unauthorized access;

- support of access rights limitation;

NOTE 1 – Only data which has been pre-defined in terms of access rights can be accessed, and this is in order to prevent accessing and tampering restricted data.

- support of high bandwidth;

NOTE 2 – 1 to 10 Gbit/s bandwidth, even higher, is expected to be supported for video-based services and applications.

- support of data flow classification and priority differentiation;
- support of device management protocols, including, but not limited to, oneM2M [b-ITU-T Y.4500.x];
- support of remote operations, including, but not limited to, access isolation and control of online/offline status (such as shutdown and reboot);
- support of remote firmware management and remote configuration upgrading, especially for manageable devices such as sensors and gateways.

## 2) Data collection and monitoring support

- support of data collection via diverse protocols;

NOTE 3 – Examples of protocols include, but are not limited to, Ethernet, RS232 and RS485 for dedicated industrial devices and control systems, and message queuing telemetry transport (MQTT) [b-ISO/IEC 20922], enhanced device protocol (EDP) [b-EDP], hypertext transfer protocol (HTTP) [b-IETF RFC 9114], constrained application protocol (CoAP) [b-IETF RFC 7252] and short message peer-to-peer (SMPP) [b-SMPP].

- support of data collection with different data formats, including, but not limited to, data sets, logs and files;
- support of collection data conversion to unified data formats;
- support of local storage of collected data;
- support of submitting collected data upward to the hardware and software facilities for further analysis and storage;
- support of real-time monitoring of operational status, including, but not limited to, device status, start time, operating and idle time, faults, alarms, production parameters and operation parameters;
- support of status monitoring of network links, including, but not limited to, connection status, transmission delay status and routing status.

## 3) Control signals related support

- support of converting the expected target control actions into specific control signals;
- support of changing the asset status in the physical environment according to the control signals.

## 4) Identification support

- support of identification of physical and logical resources with unique identifiers, and their registration.

## 5) Edge computing support

- support of pre-processing data, including, but not limited to, data integrity and consistency checking, abnormal data identification and processing, missing data identification, redundant and useless data cleaning for further data modelling and analysis;
- support of detecting and locating fault scope and fault locations according to the monitoring information of operational status and network link status;

- support of determination and execution of emergency actions (such as emergency shutdown) according to the fault level;
- support of edge application development capabilities, including, but not limited to, resource scheduling, operation, maintenance, development and debugging.

### **8.2.2 Factory internal network capabilities**

#### 1) Connectivity support

- support of interconnection among diverse connected objects (such as sensors and gateways, smart manufacturing devices and other resources) and systems inside the enterprise;
- support of accessing industrial equipment via diverse technologies, including, but not limited to, industrial field buses, industrial Ethernet and industrial wireless networks.

#### 2) Forwarding, control and management support

- support of non real-time data and real-time data forwarding of collected data, control and management data;
- support of backwards compatibility and interoperability with the legacy industrial systems by applying techniques for cross communication, such as tunnelling techniques;
- support of network control, including, but not limited to, generation of routing and flow tables, path selection, interconnection of routing protocols, access control list (ACL) and QoS configurations;
- support of network management, including, but not limited to, management of QoS, network topology, network access, network resources.

#### 3) Networking support

- support of multiple labelling protocols, including, but not limited to, VLAN and VXLAN;
- support of multiple tunnelling protocols, including, but not limited to, IPsec, L2TP, GRE, SD-WAN and MPLS VPN;
- support of IPv4/IPv6 dual stack;
- support of capabilities enabling high performance networking, including, but not limited to, capabilities for support of high bandwidth, strict latency, high reliability, high frequency transmission, high capacity connectivity, high mobility, high data forwarding priority, long transmission distance and high communication anti-interference, according to the different service and application requirements;

NOTE 1 – As an example, remote control services require specific delay and bandwidth performances. E.g., video based remote control service normally requires delay not larger than 20ms, and the network should provide relative bandwidth guarantees (e.g., high-definition video surveillance normally requires gigabit-level of bandwidth, and automatic optical inspection system implemented on the production line normally requires bandwidth from 1 to 10 Gbit/s, or even higher) according to the specific remote control video resolution requirements.

NOTE 2 – As another example, control services require different low latency and low packet loss transmission performances. For motion control applications, the end-to-end (E2E) latency should be less than 100us. For real time industrial applications (non-motion control), the E2E latency should be less than 1-100ms. The packet loss ratio should range from 99.999% to 99.99999%.

NOTE 3 – As another example, connection services, such as wireless connected AGVs, require high frequency transmission, high capacity connectivity and high mobility.

NOTE 4 – As another example, considering poor anti-interference performance of copper cables, the industrial PON technology can be adopted to avoid electromagnetic interferences within optical fibre cables.

- support of load balancing and fault recovery;
- support of network physical isolation or logical isolation, providing strictly limited access control;
- support of open architectures and protocols to not prevent network expansion.

#### 4) Multiple services support

- support of OT network services, including, but not limited to, control, collection and connection services;

NOTE 5 – The control services include local and remote control services.

NOTE 6 – The collection services include, but are not limited to, information collection services, video detection and collection services.

NOTE 7 – The connection services include, but are not limited to, device program download service, production processing program download service, AGV navigation service, remote diagnosis and maintenance guidance service.

- support of IT network services, including, but not limited to, OA, Internet, fixed phone, video/audio conferencing and internal systems interconnections;

NOTE 8 – The internal systems interconnection services provide interconnection of internal systems, including, but not limited to, MES, ERP, PLM, CRM, SCM and safety protection systems.

- support of rapid deployment, adjustment and recycle of OT and IT network services.

### **8.2.3 Factory external network capabilities**

#### 1) Network connectivity support

- support of interconnection with the factory internal network by industrial firewalls and gateways;

NOTE 1 – As an example, the access from the factory external network to the factory internal network is controlled and filtered by industrial firewalls, and firewalls record the accessing operations and backtrack security audits.

- support of interconnection with industrial fixed networks, wireless networks, Internet and dedicated networks.

#### 2) Dedicated lines support

- support of dedicated lines among different networks with specific E2E SLAs according to the service and application requirements;

- support of Internet dedicated lines;

NOTE 2 – The Internet dedicated lines can be classified as general and dedicated Internet services. The general Internet service provides best-effort data transmission and forwarding capabilities for low requirements of delay, reliability and flexibility. The dedicated Internet service provides communication links for higher requirements.

- support of enterprise interconnection dedicated lines;

NOTE 3 – As examples, the enterprise interconnection dedicated lines can be provided by virtual dedicated lines (e.g., by using SD-WAN, IPsec and MPLS VPN), physically isolated dedicated lines (e.g., by using SDH and OTN), network slicing, etc.

- support of cloud dedicated lines;

NOTE 4 – As examples, the cloud dedicated lines may provide capabilities of fixed routing configuration, seamless resources expansion, exclusive utilization, high security and performance.

- support of rapid deployment, adjustment and recycle of the dedicated lines.

## 8.2.4 Service support and application support capabilities

### 1) HA support

- support of HA of application servers, edge computing nodes, storage and other hardware and software facilities;
- support of service or function migration;
- support of load balancing to prevent access and process overload;
- support of periodic full and incremental backup mechanism for rapid data disaster recovery.

### 2) Scalability support

- support of flexible scalability for hardware and software facilities, in order to adapt capability expansion and maintenance of data resources, functional modules and applications;
- support of dynamic adjustment of hardware and software resources according to the service and application loads and requirements.

### 3) Data processing support

- support of data conversion abilities, including, but not limited to, conversion of data format and data type according to the requirements of applications, such as system upgrade, data integration, data migration, data exchange, data cleaning, data standardization, data security, data compression and data model change;
- support of data organization according to unified service rules or functional modules;
- support of data access abilities, including, but not limited to, re-organizing, splitting and mapping;
- support of data quality monitoring automation;

NOTE 1 – As an example, the device operation log files can be analyzed and evaluated by personalized data quality monitoring rules, in order to generate periodic maintenance task, or find potential risks of the devices and raise warnings to perform predictive maintenance actions.

- support of human-computer interaction for enhanced user experience;
- support of integration capabilities for data. These capabilities include, but are not limited to, big data programming paradigms and executing engines;
- support of high concurrency and low latency of data processing;
- support of online and offline big data computing;
- support of big data computing modes, including, but not limited to, real-time computing (such as stream computing), non real-time computing (such as batch computing), graph-based computing and interactive computing;

NOTE 2 – The interactive computing mode is mainly used for real-time interactive query and data analysis, such as report generation of large data warehouses. The interactive computing mode needs processing performances of high concurrency and low latency with the characteristics of high query complexity.

- support of distributed computing frameworks, including, but not limited to, structured query language (SQL) [b-ISO/IEC 9075-x] and other big data computing frameworks;
- support of programming frameworks for relation-based data objects, in order to provide capabilities of intuitive and easy operation and management of data objects;
- support of seamless integration of big data computing frameworks.

### 4) Storage support

- support of rational databases such as SQL and non-rational databases such as not only SQL (NoSQL);
- support of centralized and distributed storage;
- support of high-speed writing and reading of data;
- support of dynamic expansion and contraction of storage capacity;
- support of data filtering, in order to store different types of data into different databases and data sheets, and filter error data and other abnormal data;
- support of data dictionary;

NOTE 3 – For user repacked irregular data, the storage can compare and analyze them using data dictionary, in order to acquire and store actual data.

- support of tiered data storage.

NOTE 4 – As an example, storing hot (real-time or high frequency accessed) data into database which have specific real-time performance, and storing other data into database for long-term data, with the real-time database synchronizing with the long-term database at an appropriate time interval.

#### 5) Resource management support

- support of resource management, including, but not limited to, management of homogeneous and heterogeneous computing, storage and network resources;
- support of status monitoring of computing, storage and network resources, and raising warnings or alarms while these resources are in abnormal status;
- support of industrial data and model management.

#### 6) Service management support

- support of centralized management of services (such as database services and load balancing services), as well as service lifecycle management;- support of flexible interaction (i.e., adopt service and application functional modular design) among different service modules;
- support of providing reusable services;
- support of resources orchestration and collaboration of multiple services for service resource expansion and rapid service deployment;
- support of industrial processes and tools integration, and adoption of low code development, graphical programming and other technologies for efficient and flexible service and application innovation.

#### 7) Cloud-based management support

- support of management of virtualized resources, including, but not limited to, virtualized computing, storage and network resources;
- support of management of private cloud, public cloud and hybrid cloud;
- support of management of cloud services, including, but not limited to, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

#### 8) Data modelling support

- support of data modelling;

NOTE 5 – As an example, creating device object models based on abstracting the device objects, in order to rapidly create different device model instances.

NOTE 6 – As another example, creating different production process models, in order to realize collaboration mechanism among different production processes.

- support of multi-type and multi-dimension semantics and models, in order to build generic semantic and model libraries for the support of data modelling from different industrial services and applications.

#### 9) Information sharing support

- support of information sharing among different services and applications;
- support of information sharing via different application layer communication modes, including, but not limited to, request/response mode and publish/subscribe mode;
- support of distributed ledger technologies such as blockchain, in order to leverage their characteristics for information sharing. Those characteristics include, but are not limited to, consensus, smart contract, immutability, data sharing, decentralization and tamper-resistance [b-ITU-T X.1409].

### 8.2.5 Industrial SDN capabilities

- support of NFV for specific purposes. These specific purposes include, but are not limited to, network isolation and support of multiple services;
- support of rapid deployment, adjustment and recycle of network services with different SLAs;
- support of control and adjustment of network resources, in order to improve operation and maintenance efficiency;
- support of providing comprehensive and unified authentication and authorization mechanisms to enhance the protection ability against threats and to protect sensitive information;
- support of comprehensive visualization of network traffic and providing full path fault detection capability, in order to reduce the cost of network OAM;
- support of unified network configuration policy, in order to ensure the seamless access and consistent experience of legitimate users in different network environments;

NOTE – Network environments refer to the diversity of networks in terms of geographic distribution, organizational structure, technological implementation and service requirements.

- support of multiple communication protocols, including, but not limited to, IP, Ethernet and industrial Ethernet;
- support of unified management protocols, including, but not limited to, NETCONF, YANG and simple network management protocol (SNMP) [b-IETF RFC 3411].

### 8.2.6 Identification capabilities

- support of ID data collection via different communication technologies, including, but not limited to, wireline and wireless technologies;
- support of management of diverse IDs;
- support of registration and resolution of diverse IDs using the encoding and resolution mechanism, compatible with existing ID registration and resolution systems and platforms;
- support of processing of ID data.

### 8.2.7 Security and information protection capabilities

The security capabilities of the IIoT infrastructure include generic security capabilities and specific security capabilities [ITU-T Y.4003].

Generic security capabilities are in line with the basic security capabilities of IoT [ITU-T Y.4401], including capabilities of communication security, data management security, service provision security, security integration, mutual authentication and authorization, and security audit, which are independent of industrial applications.

Specific security capabilities are closely coupled with application-specific requirements [ITU-T Y.4000], e.g., production material management security requirements and enterprise management security requirements.

The information protection capabilities of the IIoT infrastructure include protection of IIoT users' personal information and protection of enterprises' sensitive information, involving protection of identities during the different identity management activities.

## **9 Security considerations**

In order to mitigate security threats such as network attacks faced by IIoT, the IIoT infrastructure should comprehensively consider information and communication security. Best practices should be adopted when using IIoT in industrial environments.

Furthermore, IIoT infrastructure security and information protection should facilitate security of other IIoT-related industrial resources, such as IIoT infrastructure connected manufacturing resources, and industrial applications like smart manufacturing applications, throughout the three dimensions of the smart manufacturing reference model [ITU-T Y.4003].

## Bibliography

- [b-ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.
- [b-ITU-T G.671] Recommendation ITU-T G.671 (2019), *Transmission characteristics of optical components and subsystems*.
- [b-ITU-T G.803] Recommendation ITU-T G.803 (2000), *Architecture of transport networks based on the synchronous digital hierarchy (SDH)*.
- [b-ITU-T G.872] Recommendation ITU-T G.872 (2019), *Architecture of optical transport networks*.
- [b-ITU-T G.8031] Recommendation ITU-T G.8031 (2015), *Ethernet Linear Protection Switching*.
- [b-ITU-T H.320] Recommendation ITU-T H.320 (2004), *Narrow-band visual telephone systems and terminal equipment*.
- [b-ITU-T M.1301] Recommendation ITU-T M.1301 (2001), *General description and operational procedures for international SDH leased circuits*.
- [b-ITU-T Q.3741] Recommendation ITU-T Q.3741 (2019), *Signalling requirements for SD-WAN service*.
- [b-ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.
- [b-ITU-T X.672] Recommendation ITU-T X.672 (2022) | ISO/IEC 29168-1:2023, *Information technology – Open systems interconnection – Object identifier resolution system*.
- [b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.
- [b-ITU-T X.1409] Recommendation ITU-T X.1409 (2022), *Security services based on distributed ledger technology*.
- [b-ITU-T Y.2623] Recommendation ITU-T Y.2623 (2021), *Requirements and framework of industrial Internet networking based on future packet based network evolution*.
- [b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.
- [b-ITU-T Y.4500.x] Recommendation ITU-T Y.4500.x-series (2018), *oneM2M Recommendation series*.
- [b-ISO/IEC 9075-x] ISO/IEC 9075-x-series:2023, *Information technology — Database languages SQL*.
- [b-ISO/IEC 20922] ISO/IEC 20922:2016, *Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1*.
- [b-ISO/IEC TR 23188] ISO/IEC TR 23188:2020, *Information technology — Cloud computing — Edge computing landscape*.
- [b-ISO/IEC TR 30166] ISO/IEC TR 30166:2020, *Internet of things (IoT) – Industrial IoT*.

- [b-IEC 61158-1] IEC 61158-1 ED3 (2023), *Industrial communication networks – Fieldbus specifications – Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series.*
- [b-IEC 61784-2-3] IEC 61784-2-3 ED1 (2023), *Industrial networks – Profiles – Part 2-3: Additional real-time fieldbus profiles based on ISO/IEC/IEEE 8802-3 – CPF 3.*
- [b-IEC 62601] IEC 62601 ED2 (2015), *Industrial networks – Wireless communication network and communication profiles – WIA-PA.*
- [b-IEC 62948] IEC 62948 ED1 (2017), *Industrial networks – Wireless communication network and communication profiles – WIA-FA.*
- [b-IEC PAS 63088] IEC PAS 63088 ED1 (2017), *Smart manufacturing - Reference architecture model industry 4.0 (RAMI4.0).*
- [b-3GPP TS 36.300] 3GPP TS 36.300 V17.5.0 (2023), *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 17).*  
[https://www.3gpp.org/ftp/Specs/latest/Rel-17/36\\_series](https://www.3gpp.org/ftp/Specs/latest/Rel-17/36_series)
- [b-Bluetooth] Bluetooth SIG – Bluetooth Core Specification 5.3, July 2021.  
[https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc\\_id=521059](https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=521059)
- [b-Cigref] Cigref report, December 2019, *IT/OT convergence: A fruitful integration of information systems and operational systems.*  
<https://www.cigref.fr/cigref-report-it-ot-convergence-a-fruitful-integration-of-information-systems-and-operational-systems>
- [b-EDP] China Mobile – Device Terminal Access Protocol – EDP V1.6, February 2017, *Enhanced Device Protocol (EDP).*  
<https://open.iot.10086.cn/en/doc/book/device-develop/multipro/EDP/introduce.html>
- [b-ETSI GR F5G 007] ETSI GR F5G 007 v1.1.1 (2023-01), *Fifth Generation Fixed Network (F5G); F5G Industrial PON.*  
[https://www.etsi.org/deliver/etsi\\_gr/F5G/001\\_099/007/01.01.01\\_60/gr\\_F5G007v010101p.pdf](https://www.etsi.org/deliver/etsi_gr/F5G/001_099/007/01.01.01_60/gr_F5G007v010101p.pdf)
- [b-ETSI NFV] ETSI ISG NFV, *Network Functions Virtualisation (NFV).*  
<https://www.etsi.org/technologies/nfv>
- [b-GS1] GS1 General Specifications Release 23.0, Jan 2023, *GS1 General Specifications Standard.*  
<https://ref.gs1.org/standards/genspecs/>
- [b-IEEE 802.1 TSN] Janos Farkas, et. Al, *Time-Sensitive Networking Standards.*  
<https://ieeexplore.ieee.org/document/8412457>
- [b-IEEE 802.1Q] ISO/IEC/IEEE 8802-1Q:2020, *Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks — Part 1Q: Bridges and bridged networks.*
- [b-IEEE 802.3] IEEE 802.3-2022, *IEEE Standard for Ethernet.*  
<https://standards.ieee.org/ieee/802.3/10422/>
- [b-IEEE 802.11] ISO/IEC/IEEE 8802-11:2022, *Telecommunications and information exchange between systems — Specific requirements for local and metropolitan area networks — Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.*
- [b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol.*  
<https://www.rfc-editor.org/rfc/rfc791>
- [b-IETF RFC 1180] IETF RFC 1180 (1991), *A TCP/IP Tutorial.*  
<https://www.rfc-editor.org/rfc/rfc1180>

- [b-IETF RFC 2784] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.  
<https://www.rfc-editor.org/rfc/rfc2784>
- [b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.  
<https://www.rfc-editor.org/rfc/rfc3931>
- [b-IETF RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*.  
<https://www.rfc-editor.org/rfc/rfc3650>
- [b-IETF RFC 3931] IETF RFC 3931 (2005), *Layer Two Tunneling Protocol – Version 3 (L2TPv3)*.  
<https://www.rfc-editor.org/rfc/rfc3931>
- [b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.  
<https://www.rfc-editor.org/rfc/rfc4301>
- [b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.  
<https://www.rfc-editor.org/rfc/rfc4364>
- [b-IETF RFC 5440] IETF RFC 5440 (2009), *Path Computation Element (PCE) Communication Protocol (PCEP)*.  
<https://www.rfc-editor.org/rfc/rfc5440>
- [b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF)*.  
<https://www.rfc-editor.org/rfc/rfc6020>
- [b-IETF RFC 6241] IETF RFC 6241 (2011), *Network Configuration Protocol (NETCONF)*.  
<https://www.rfc-editor.org/rfc/rfc6241>
- [b-IETF RFC 7252] IETF RFC 7252 (2014), *The Constrained Application Protocol (CoAP)*.  
<https://www.rfc-editor.org/rfc/rfc7252>
- [b-IETF RFC 7348] IETF RFC 7348 (2014), *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*.  
<https://www.rfc-editor.org/rfc/rfc7348>
- [b-IETF RFC 8200] IETF RFC 8200 (2017), *Internet Protocol, Version 6 (IPv6) Specification*.  
<https://www.rfc-editor.org/rfc/rfc8200>
- [b-IETF RFC 8402] IETF RFC 8402 (2018), *Segment Routing Architecture*.  
<https://www.rfc-editor.org/rfc/rfc8402>
- [b-IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.  
<https://www.rfc-editor.org/rfc/rfc8446>
- [b-IETF RFC 8955] IETF RFC 8955 (2020), *Dissemination of Flow Specification Rules*.  
<https://www.rfc-editor.org/rfc/rfc8955>
- [b-IETF RFC 9085] IETF RFC 9085 (2021), *Border Gateway Protocol – Link State (BGP-LS) Extensions for Segment Routing*.  
<https://www.rfc-editor.org/rfc/rfc9085>
- [b-IETF RFC 9114] IETF RFC 9114 (2022), *HTTP/3*.  
<https://www.rfc-editor.org/rfc/rfc9114>
- [b-IETF RFC 9147] IETF RFC 9147 (2022), *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*.  
<https://www.rfc-editor.org/rfc/rfc9147>
- [b-IIRA] Industry IoT Consortium (IIC) technical report, December 2022, *The Industrial Internet Reference Architecture, Version 1.10*.  
<https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf>
- [b-ISA-100.11a] ANSI/ISA-100.11a-2011, *Wireless systems for industrial automation: Process control and related applications*.  
<https://www.isa.org/products/ansi-isa-100-11a-2011-wireless-systems-for-industr>

- [b-ONF TR-523] ONF TR-523, October 2016, *Intent NBI – Definition and Principles*.  
[https://opennetworking.org/wp-content/uploads/2014/10/TR-523\\_Intent\\_Definition\\_Principles.pdf](https://opennetworking.org/wp-content/uploads/2014/10/TR-523_Intent_Definition_Principles.pdf)
- [b-SCADA] ISA112, SCADA Systems standards committee.  
<https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112>
- [b-SMPP] SMS Forum – Short Message Peer-to-Peer Protocol Specification Version 5.0, February 2003.  
[https://smpp.org/SMPP\\_v5.pdf](https://smpp.org/SMPP_v5.pdf)
- [b-TIA-232] TIA-232 Revision F, October 1997, *Interface Between Data Terminal Equipment and Data Circuit- Terminating Equipment Employing Serial Binary Data Interchange*.  
[https://global.ihs.com/doc\\_detail.cfm?&csf=TIA&item\\_s\\_key=00125234&item\\_key\\_date=870024&input\\_doc\\_number=232&input\\_doc\\_title=&org\\_code=TIA](https://global.ihs.com/doc_detail.cfm?&csf=TIA&item_s_key=00125234&item_key_date=870024&input_doc_number=232&input_doc_title=&org_code=TIA)
- [b-TIA-485] TIA-485-A, March 1998, *Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems*.  
[https://global.ihs.com/doc\\_detail.cfm?&csf=TIA&item\\_s\\_key=00032964&item\\_key\\_date=870024&input\\_doc\\_number=485&input\\_doc\\_title=&org\\_code=TIA](https://global.ihs.com/doc_detail.cfm?&csf=TIA&item_s_key=00032964&item_key_date=870024&input_doc_number=485&input_doc_title=&org_code=TIA)
-