International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4122

(07/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Requirements and use cases

Requirements and capability framework of the edge-computing-enabled gateway in the Internet of things

Recommendation ITU-T Y.4122

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	**Y.4100–Y.4249**
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4122

Requirements and capability framework of the edge-computing-enabled gateway in the Internet of things

Summary

The gateway is an important component of Internet of things (IoT) systems, enabling IoT devices to connect to communication networks. Edge computing technologies can benefit the IoT, providing computation, storage, networking and intelligence in proximity to IoT devices.

Compared with the common gateway [ITU-T Y.4101], the edge-computing-enabled gateway in the IoT (EC-enabled IoT gateway) has additional capabilities supporting service layer interworking, and application layer interworking between IoT devices, IoT platforms and IoT application servers. In addition, the EC-enabled IoT gateway supports data transmission capabilities for IoT applications sensitive to time, latency, jitter and packet loss.

Based on the common requirements and capabilities of a gateway for IoT applications [ITU-T Y.4101] and IoT requirements for support of edge computing [ITU-T Y.4208], additional capabilities and capability framework of the edge-computing-enabled gateway in the IoT are specified. Examples of applicability of the edge-computing-enabled gateway in the IoT are also given.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4122	2021-07-14	20	11.1002/1000/14735

Keywords

Capability, capability framework, edge computing, gateway, internet of things, IoT, requirement.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4122

Requirements and capability framework of the edge-computing-enabled gateway in the Internet of things

1 Scope

Compared with the common gateway [ITU-T Y.4101], the edge-computing-enabled gateway in the Internet of things (IoT) – abbreviated as the EC-enabled IoT gateway – has additional capabilities supporting service layer interworking and application layer interworking between IoT devices, IoT platforms and IoT application servers. In addition, the EC-enabled IoT gateway supports data transmission capabilities for IoT applications sensitive to time, latency, jitter and packet loss.

Based on common requirements and capabilities of a gateway for IoT applications [ITU-T Y.4101] and IoT requirements for support of edge computing [ITU-T Y.4208], additional capabilities and a capability framework of the edge-computing-enabled gateway in the IoT are specified.

The scope of this Recommendation includes:

– The introduction of the EC-enabled IoT gateway;

– The requirements of the EC-enabled IoT gateway;

– The capabilities of the EC-enabled IoT gateway;

– The capability framework of the EC-enabled IoT gateway.

The appendix provides examples of applicability of the EC-enabled IoT gateway.

NOTE – Direct communication of the EC-enabled gateway with other gateways in the IoT is out of scope of this Recommendation.

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.4101] Recommendation ITU-T Y.4101/Y.2067 (2017), *Common Requirements and Capabilities of a Gateway for Internet of Things Applications*.

[ITU-T Y.4113] Recommendation ITU-T Y.4113 (2016), *Requirements of the Network for the Internet of Things.*

[ITU-T Y.4208] Recommendation ITU-T Y.4208 (2020), *Internet of Things Requirements for Support of Edge Computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T F.500]: Method of controlling access to information held in the directory either for retrieval, managing or updating purposes.

3.1.2 authentication [b-ITU-T Y.1271]: The act or method used to verify a claimed identity.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 gateway [ITU-T Y.4101]: A unit in the Internet of things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

3.1.5 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APP Application

CPU Central Processing Unit

EC Edge Computing

IoT Internet of Things

PLC Programmable Logic Controller

QoS Quality of Service

SS&AS Service Support and Application Support

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 document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need 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.

The expressions "edge-computing-enabled gateway in the Internet of things (IoT)" and "edge-computing (EC)-enabled IoT gateway" are used interchangeably.

6 Introduction of the edge-computing-enabled gateway in the IoT

The IoT is a global infrastructure that interconnects (physical and virtual) things and makes full use of things to offer services to all kinds of applications while ensuring security and privacy per corresponding requirements [ITU-T Y.4000].

To realize the vision of the IoT, the gateway is an important component to support the interconnection of devices which cannot connect to communication networks directly.

The EC-enabled IoT gateway is a kind of gateway with common gateway capabilities [ITU-T Y.4101] and additional capabilities for the support of edge computing.

Compared with the common requirements and capabilities of a gateway in the IoT [ITU-T Y.4101], the EC-enabled IoT gateway can provide flexible capabilities and can cooperate efficiently with IoT technical components (e.g., IoT device, IoT platform, application server, IoT area network, access network [ITU-T Y.4113]).

The EC-enabled IoT gateway can efficiently make usage of the capabilities of IoT application servers, IoT platforms and IoT devices, and this enables the gateway's self-configuration in order to fulfil the service requirements identified in [ITU-T Y.4208].

IoT applications may be sensitive to time synchronization, latency, jitter, packet loss and other network quality of service (QoS) parameters. The EC-enabled IoT gateway can provide computation, storage, networking and intelligence in proximity to IoT devices, reducing network resource consumption (for example, spectrum and bandwidth resources) while meeting IoT application requirements at the same time.

7 Requirements of the edge-computing-enabled gateway in the IoT

The EC-enabled IoT gateway supports common requirements of the gateway specified in [ITU-T Y.4101]. The additional requirements of the gateway for the support of edge computing are a key target of this Recommendation.

Referring to the IoT reference model [ITU-T Y.4000] and the basic model of the network for the IoT [ITU-T Y.4113], the EC-enabled IoT gateway and the technical components interworking with it are shown in Figure 1.

NOTE 1 – The service support and application support (SS&AS) layer is optional for some IoT devices.

NOTE 2 – The IoT area network and the access network provide the underlying network connectivity for the EC-enabled IoT gateway and its interworking with other IoT technical components.

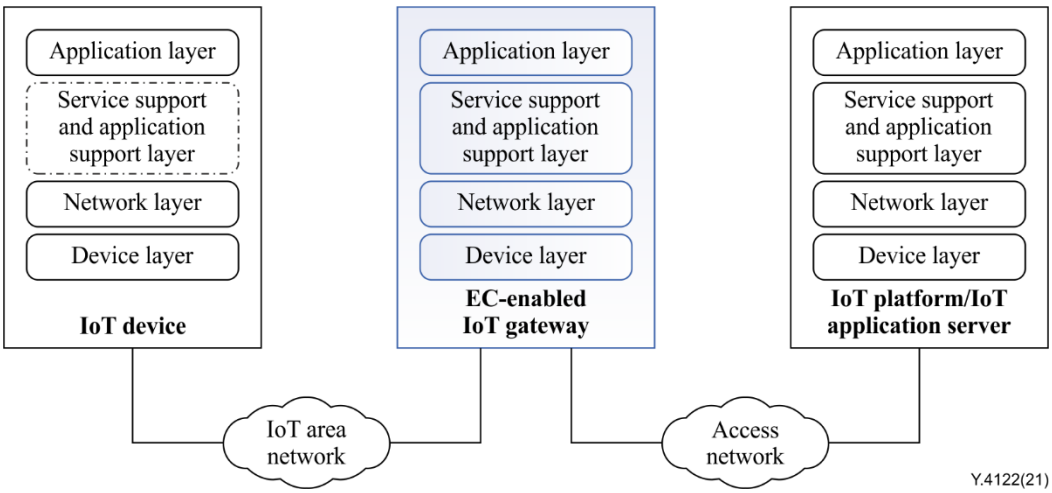

Figure 1 – EC-enabled IoT gateway and its interworking with other IoT technical components

7.1 Service layer interworking

Compared with the gateway [ITU-T Y.4101], the EC-enabled IoT gateway is required to additionally support service layer interworking in order to enable collaboration between IoT devices, IoT platforms and IoT application servers.

NOTE – As an example, the EC-enabled IoT gateway can support time-sensitive tasks on behalf of IoT devices.

7.2 Application layer interworking

Compared with the gateway [ITU-T Y.4101], it is recommended that the EC-enabled IoT gateway additionally support application layer interworking with IoT devices, IoT platforms and IoT application servers in order to enable application collaboration across these components.

7.3 Network QoS and time sensitiveness

Based on clauses 7.2.3 and 8.3.2 of [ITU-T Y.4208], "Internet of Things Requirements for Support of Edge Computing", compared with the common requirements of the gateway in the IoT [ITU-T Y.4101], it is recommended that the EC-enabled IoT gateway additionally support networking with bounded network QoS, including bounded latency, bounded jitter and bounded packet loss, between the EC-enabled IoT gateway and other IoT technical components.

It is also recommended that the EC-enabled IoT gateway additionally support time-sensitive data transmission in order to ensure low latency and time synchronization between the EC-enabled IoT gateway and other IoT technical components.

8 Capabilities of the edge-computing-enabled gateway in the IoT

The EC-enabled IoT gateway supports the common capabilities of the gateway specified in [ITU-T Y.4101]. The additional capabilities of the gateway with support of edge computing are a key target of this document.

Based on IoT requirements for the support of edge computing [ITU-T Y.4208], the functional framework and capabilities of the IoT [ITU-T Y.4401] and common capabilities of the gateway in the IoT [ITU-T Y.4101], the capabilities of the EC-enabled IoT gateway (for simplicity, "the gateway" in the following clauses) can be classified into the following categories: protocol translation capabilities, data processing capabilities, remote updating capabilities, network support capabilities and management capabilities.

8.1 Protocol translation capabilities

Compared with the communication protocol translation capabilities specified in clause 8.2 of [ITU-T Y.4101], the gateway provides additional protocol translation capabilities in the SS&AS layer and/or application layer.

The gateway is required to provide SS&AS layer protocol translation to support the generic support capabilities of the SS&AS layer.

NOTE 1 – The generic support capabilities of the SS&AS layer are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may also be invoked by specific support capabilities, e.g., to build other specific support capabilities [ITU-T Y.4000].

Since computation, storage and intelligence may migrate from the IoT platforms and IoT application servers to the gateway, it is recommended that the gateway provide application layer protocol translation to support application layer interworking with IoT platforms and IoT application servers. Based on the protocol translation capabilities in the application layer, the gateway can cooperate with IoT platforms and IoT application servers with heterogeneous application layer protocols.

It is recommended that the gateway provide application layer protocol translation to support application layer interworking with the IoT devices. Based on the protocol translation capabilities in the application layer, the gateway can manage IoT devices with heterogeneous application layer protocols.

NOTE 2 – Refer to clause 8.3 of [ITU-T Y.4101] for more details.

8.2 Data processing capabilities

The data processing capabilities of the gateway include data collecting capability, data storage capability, data analysis capability and data delivery capability.

It is recommended that the gateway provide data processing capabilities to IoT platforms and IoT application servers so that IoT platforms and IoT application servers can deploy some data operations at the edge of the network. With respect to data operations in the IoT platforms and IoT application servers, due to shortened data transmission path and data processing capabilities provided by the gateway, processing speed may be increased.

It is recommended that the gateway allocate or reserve data processing related resources (e.g., memory, central processing unit (CPU), data flow priority, bandwidth) according to requests from IoT platforms and IoT application servers in preset mode and/or dynamic mode.

It is recommended that the gateway provide IoT devices with data storage, data analysis and data delivery capabilities in order to, on behalf of the IoT devices, collaborate with other IoT devices, IoT platforms and IoT application servers.

NOTE – For example, the deployment of the data analysis capability in the gateway may allow the reduction of transmission latency and jitter against the deployment of the data analysis capability in remote IoT platforms and IoT application servers.

8.3 Remote updating capabilities

To support service layer interworking and application layer interworking, it is recommended that the gateway provide remote updating capabilities, periodically or based on event triggering.

The remote updating capabilities are required to enable software loading, starting, stopping, updating and unloading, as well as application (APP) hosting and other operations according to commands from IoT platforms and IoT application servers.

8.4 Network support capabilities

In order to satisfy bounded network QoS, low latency and time synchronization requirements, the gateway is required to support time-sensitive data transmission capabilities (enabling technologies

include, but are not limited to, frame pre-emption [b-IEEE 802.1Q], traffic scheduling and time synchronization [b-IEEE 802.1AS]).

8.5 Management capabilities

8.5.1 Network access management

The gateway is required to support network access management and related protocols.

The gateway is required to have self-healing ability in order to ensure normal connection and reconnection to the IoT area network and access network after normal restart and abnormal power failure.

8.5.2 Log management

The gateway is required to support log recording, including recording of system log, access log, firewall log, alarm log and other logs, which enables, for example, monitoring of login operations and gateway configuration operations, as well as of access operations that violate preset rules or policies (such as illegal attack, access to some Internet sites, etc.).

The gateway is required to support the querying and clearing of log records.

The gateway is required to support the time stamping of log records.

The gateway is required to support a lack of loss of log records in case of power failure.

It is recommended that the gateway support detection of abnormal log records.

8.5.3 Power management

It is recommended that the gateway have power management to manage the power status of the IoT devices which are connected to the gateway.

NOTE – The management of the power status includes, but is not limited to, start, shutdown and restart of the power.

It is recommended that the gateway provide IoT platforms and IoT application servers with power management to start, shutdown and restart the power of the gateway.

8.5.4 Firmware management

The gateway is required to support firmware management from the IoT platforms and IoT application servers, including, but not limited to, firmware update and firmware fall-back.

9 Capability framework of the edge-computing-enabled gateway in the IoT

The capability framework of EC-enabled gateway in the IoT is shown in Figure 2.

The **application layer capabilities** provide application-dependent capabilities to applications of the EC-enabled IoT gateway in order to support application layer interworking between IoT devices, IoT platforms and IoT application servers. Application protocol translation, metadata management and service provisioning are basic capabilities.

The **SS&AS layer capabilities** provide application-independent capabilities in order to support applications deployed in the EC-enabled IoT gateway. SS&AS layer protocol translation, hardware virtualization and scheduling are basic capabilities.

The **network layer capabilities** include network quality monitoring and time-sensitive data transmission support, which are basic capabilities to support application layer interworking and service layer interworking.

The **device layer capabilities** include interface and functionality support, which is a basic capability to support upper layer capabilities.

The **management capabilities** include maintenance support, power management and firmware management.

The **security capabilities** include authentication, authorization, encryption support and access control.

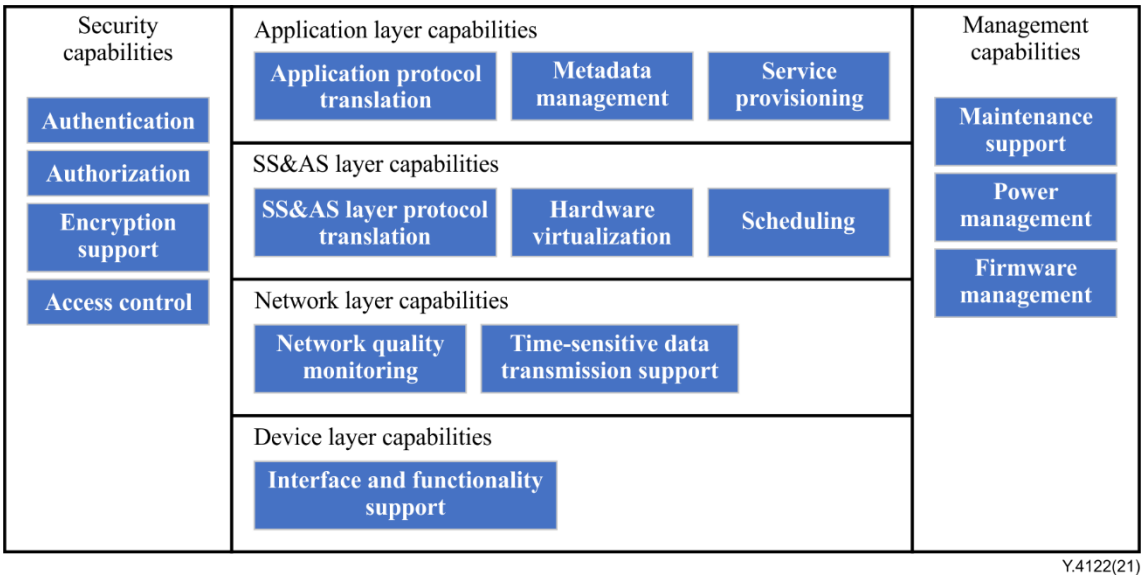

Figure 2 – Capability framework of EC-enabled IoT gateway

9.1 Application layer capabilities

9.1.1 Application protocol translation

According to clause 8.1, it is recommended that the gateway provide application protocol translation capability in order to support heterogeneous protocols at the application layer between IoT devices, IoT platforms and IoT application servers.

9.1.2 Metadata management

According to clause 8.1, the gateway has the capability of protocol identification. Protocol related metadata is required to be managed.

According to clause 8.2, the gateway provides data processing capabilities to IoT devices, IoT platforms and IoT application servers. The gateway is required to provide metadata management to enable these capabilities.

The gateway is required to provide metadata management capability to support application layer interworking between IoT devices, IoT platforms and IoT application servers.

Metadata addition, deletion, modification and lookup are four basic operations that metadata management is required to provide.

9.1.3 Service provisioning

According to clause 8.2, the gateway is required to provide service provisioning capability to support application layer interworking between IoT devices, IoT platforms and IoT application servers. Via service provisioning capability, IoT platforms and IoT application servers can, for example, activate and deactivate the gateway (fully or partially, i.e., with only some specific capabilities).

9.2 Service support and application support layer capabilities

9.2.1 SS&AS layer protocol translation

According to clause 8.1, in order to support the interworking of IoT devices with IoT platforms and IoT application servers, the gateway adapts the protocols between the IoT devices, IoT platforms and IoT application servers.

According to clause 8.1, the gateway is required to provide a protocol translation capability in the SS&AS layer to support SS&AS layer interworking between IoT devices, IoT platforms and IoT application servers.

9.2.2 Hardware virtualization

According to clause 8.2, it is recommended that the gateway provide hardware virtualization capability in the SS&AS layer in order to support application software independence from the gateway's hardware.

NOTE – Hardware virtualization aims to abstract the functionalities of the hardware and cover up the differences of the hardware in order to, for example, simplify the hardware development.

9.2.3 Scheduling

According to clause 8.2, the gateway is required to provide resource scheduling capability (for example, network priority scheduling of different application data flows), in order to support application layer interworking and SS&AS layer interworking.

9.3 Network layer capabilities

9.3.1 Network quality monitoring

According to clause 8.2, it is recommended that the gateway provide network quality monitoring capability as this is critical to effectively support interworking between the gateway, IoT platforms and IoT application servers, and make good usage of the network resources.

It is recommended that the network quality monitoring capability collect network quality related data in order to support network quality analysis and network problem diagnosis (for example, data associated with wireless signal strength).

It is recommended that the network quality monitoring capability report the network quality related data to IoT platforms and IoT application servers so that IoT platforms and IoT application servers can adjust their network strategy (e.g., traffic priorities, spectrum allocation) according to the network status, as appropriate.

9.3.2 Time-sensitive data transmission support

According to clause 8.4, the gateway is required to support time-sensitive data transmission capabilities.

9.4 Device layer capabilities

9.4.1 Interface and functionality support

According to clause 8.4, the gateway is required to support network interfaces and corresponding functionalities to ensure time-sensitive data transmission with the IoT area network as well as the access network.

9.5 Management capabilities

9.5.1 Maintenance support

According to clause 8.5.2, the gateway is required to provide maintenance capability to support recovery from errors, and restoration from previous backups.

9.5.2 Power management

According to clause 8.5.3, it is recommended that the gateway provide power management capability in order to enable the IoT platforms and IoT application servers to manage the power of the gateway.

NOTE – The IoT platforms and IoT application servers can invoke the power management capability provided by the gateway, for example, to lower the energy consumption of the gateway.

According to clause 8.5.3, it is recommended that the gateway provide the IoT platforms and IoT application servers with power management capability in order to manage the power of the IoT devices connected with the gateway on their behalf.

9.5.3 Firmware management

According to clause 8.5.4, the gateway is required to provide firmware management capability, including, but not limited to, firmware release, firmware update and firmware fall-back, in order to enable interworking with IoT devices, IoT platforms and IoT application servers as appropriate.

9.6 Security capabilities

9.6.1 Authentication

According to clauses 8.1, 8.2, 8.3 and 8.5, the gateway interworks with IoT platforms, IoT application servers and IoT devices.

It is recommended that the gateway provide authentication capability, e.g., to verify the identity of the gateway's access requester. The access requester may include IoT devices, IoT platforms and IoT application servers.

9.6.2 Authorization

According to clauses 8.1, 8.2, 8.3 and 8.4, the gateway interworks with IoT platforms, IoT application servers and IoT devices. Authorization is necessary for the gateway to ensure that interworking operations work under proper rights.

It is recommended that the gateway provide authorization capability, e.g., to grant the corresponding access rights to the access requester.

9.6.3 Encryption support

According to clauses 8.1, 8.2, 8.3 and 8.4, the gateway interworks with IoT platforms, IoT application servers and IoT devices. Some sensitive data may be transmitted: as an example, the data for power management of the production devices in a factory is critical to production safety.

It is recommended that the gateway provide encryption support capability, including but not limited to support of encryption for storage and communication.

NOTE – Communication encryption may be used between the gateway and other IoT technical components such as IoT devices, IoT platforms and IoT application servers.

9.6.4 Access control

According to clause 8.1, it is recommended that the gateway provide access control capability, e.g., to prevent access to information stored in the gateway itself in case no access right is granted to the requester.

Appendix I

Examples of applicability of the edge-computing-enabled gateway in the IoT

(This appendix does not form an integral part of this Recommendation.)

I.1 EC-enabled IoT gateway in crane control

In factories, the EC-enabled IoT gateway can be used to support interworking between the IoT platform and IoT devices in industrial deployments.

Figure I.1 is an example of EC-enabled IoT gateway usage in crane control.

Industrial cranes are large mechanical pieces of equipment which are composed of mechanical structures, sensors and actuators. Remote control of industrial cranes is usually used in large-scale factories, harbours and mines.

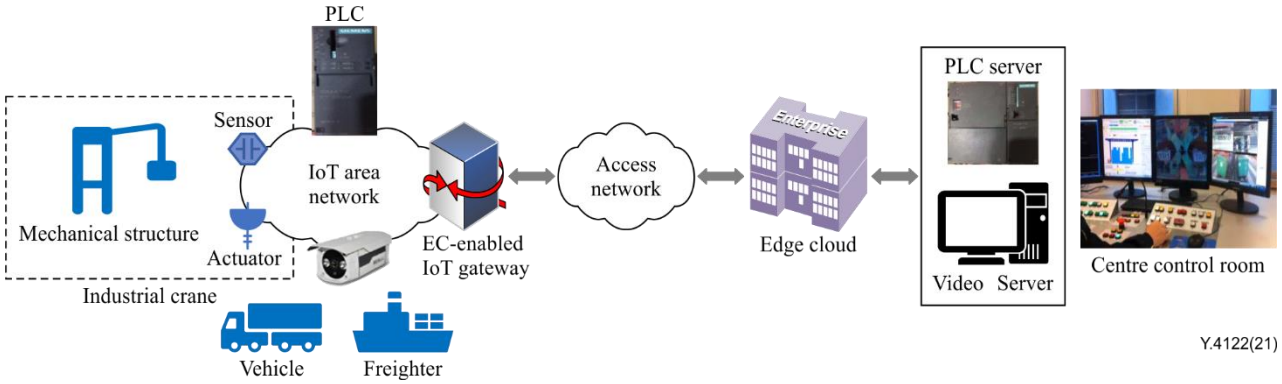

Figure I.1 – Example of EC-enabled IoT gateway usage in crane control (PLC – programmable logic controller)

Figure I.2 shows typical crane control before the introduction of EC-enabled gateway usage.

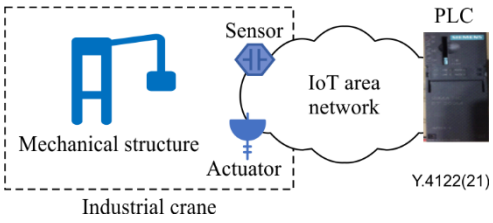

Figure I.2 – Typical crane control before the introduction of EC-enabled gateway usage

With respect to Figure I.2, the basic process of crane control is as follows:

1. The crane sensors collect status information relating to the crane;
2. The crane sensors send this status information to the programmable logic controllers (PLCs);
3. Based on the status provided by the crane sensors, the PLCs make decisions and send control commands to the crane actuators;
4. The crane actuators execute the received commands;
5. Based on the execution of the actuators, the crane performs the actions.

The limitation of crane control without EC-enabled gateway usage is that when there is more than one PLC, these PLCs cannot make decisions collaboratively and efficiently.

Compared with typical crane control before the introduction of EC-enabled gateway usage, the EC-enabled IoT gateway can provide resources, for example, computation, storage and network, to support the collaborative decision making of multiple PLCs, and can support interworking between the servers deployed at the central control room and the PLCs deployed on the field.

As shown in Figure I.1, via the IoT area network, the gateway can support interworking between crane sensors, actuators, PLCs and other devices, for example, video cameras. Therefore, decision making can be based on statuses from multiple crane sensors and the control commands can be sent to multiple actuators. Cooperation between these actuators can then be achieved.

Additionally, via access network, the gateway can support interworking between PLCs, PLC servers and other devices (for example, video cameras) and those devices' servers (for example, video servers). Therefore, decision making can not only be based on statuses from multiple crane sensors but can also be based on information from multiple severs deployed in the centre control room. The crane control can then cooperate with other equipment, for example, vehicles and freighters.

In summary, the EC-enabled IoT gateway can help to improve the efficiency of crane control and broaden the scope of crane application.

I.2 EC-enabled IoT gateway in product inspection

The EC-enabled IoT gateway can be used in product inspection. In order to improve the yield rate of products, they must pass through a strict inspection. The inspection is often composed of a complex set of test items. The IoT platform can deliver the test items or inspection models to the gateway. With the help of the gateway, the product inspection can be carried out more easily and efficiently.

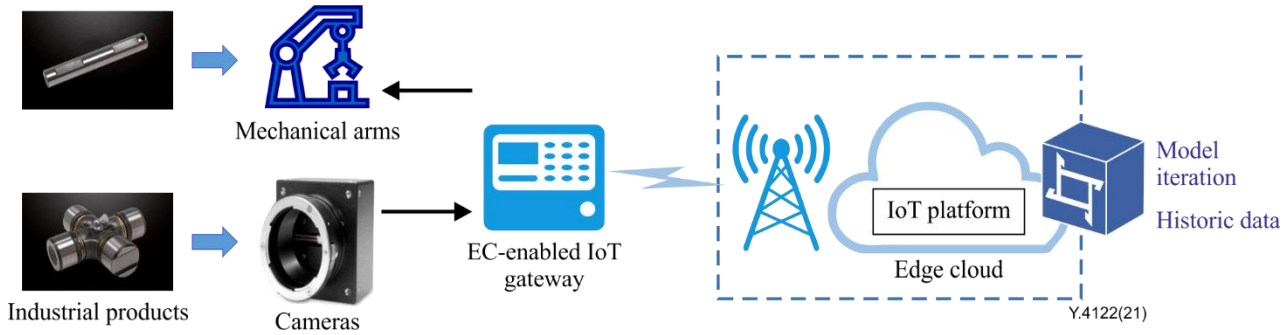

Figure I.3 – Example of EC-enabled IoT gateway usage in product inspection

As shown in Figure I.3, the gateway can be used in product inspection:

1. Cameras take photos of the industrial products;
2. Cameras send these photos to the gateway;
3. The gateway invokes a photo-based defect analysis program to inspect the defective products;
4. When a defective product is found, the gateway controls mechanical arms to remove the defective product.

To improve the accuracy of the analysis results of the photo-based defect analysis program, the edge cloud can keep a large amount of historical data from photos. Based on this historical data from photos, an inspection model for the photo-based defect analysis program can be iterated.

When the model is iterated, the iterated inspection model can be sent to the gateway. Then the gateway is updated, and the yield rate may consequently be improved.

The benefits of the EC-enabled IoT gateway in this use case include but are not limited to:

1. That the gateway can be configured by the IoT platform in the edge cloud in Figure I.3, so that the capabilities of the gateway can be iteratively enhanced.

2. That the gateway can support diverse IoT devices, for example, cameras and mechanical arms as shown in Figure I.3, so that cooperation between IoT devices can be achieved.
3. That the gateway can provide data processing at the edge near to the production line, which may reduce pressure on the transport network and IoT platform, and enable real-time operations, for example, the removal of defective products from the production line.

Bibliography

[b-ITU-T F.500] Recommendation ITU-T F.500 (1992), *International public directory services*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (2019) | ISO/IEC 9594-1:2019, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2014), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-IEEE 802.1AS] IEEE 802.1AS (2011), *Standard for Local and Metropolitan Area Networks – Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks*.

[b-IEEE 802.1Q] IEEE 802.1Q (2014), *Standard for Local and Metropolitan Area Networks —– Bridges and Bridged Networks*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021