International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.748.0

(10/2014)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

Common requirements for Internet of things (IoT) applications

Recommendation ITU-T F.748.0

International Telecommunication Union

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
AUDIOVISUAL SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.748.0

Common requirements for Internet of things (IoT) applications

Summary

Recommendation ITU-T F.748.0 includes the common requirements for Internet of things (IoT) applications enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

The requirements defined in this Recommendation are general requirements, and can therefore be applied to many kinds of IoT applications regardless of their types and characteristics.

This Recommendation is based on the high-level requirements and the reference model defined in Recommendation ITU-T Y.2060.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.748.0	2014-10-14	16	11.1002/1000/12228

Keywords

Internet of things, IoT, things, ubiquitous computing.

---

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T F.748.0

Common requirements for Internet of things (IoT) applications

1 Scope

This Recommendation defines the common requirements for Internet of things (IoT) applications based on [ITU-T Y.2060].

This Recommendation covers the following from the application point of view:

– overview of the IoT applications;

– characteristics of the IoT applications;

– common requirements for the IoT applications.

NOTE – This Recommendation mainly focuses on the viewpoint of the IoT applications. The network layer aspect of 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.2060] Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things.*

[ISO/IEC 29182-1] ISO/IEC 29182-1 (2013), *Sensor networks: Sensor Network Reference Architecture (SNRA) – Part 1: General overview and requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 data fusion [ISO/IEC 29182-1]: Deriving information by processing data from various sources.

3.1.2 Internet of things (IoT) [ITU-T Y.2060]: 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 broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3 thing [ITU-T Y.2060]: With regard to the Internet of things, this is an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IoT Internet of Things

M2M Machine-to-Machine

MOC Machine Oriented Communication

MTC Machine-Type Communication

QoS Quality of Service

RFID Radio Frequency Identification

SOA Service Oriented Architecture

USN Ubiquitous Sensor Network

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.

6 Characteristics of things in the IoT

[ITU-T Y.2060] explains the concept of the Internet of things (IoT) as a vision with technological and social implications. In addition, the IoT can be viewed as 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.

Things in the IoT can be characterized using five criteria: fundamental, common, social, autonomy and capability of self-replication or control [b-CERP-IoT].

6.1 Fundamental characteristics

Fundamentally, things have characteristics as follows:

– Things can be "real world entities" or "virtual entities";

– Things have identity and there are means for identifying (automatically or manually) them, for example barcode and radio frequency identification (RFID);

– Things and their associated information (their virtual representations) respect the privacy, security and safety of other things or people with which they interact;

– Association (or relation) among things (both physical and virtual) and the related information is as important as the things and the information in IoT application; and

– Things communicate with each other via the infrastructure or the infrastructure-less communications means.

6.2 Common characteristics

There are common characteristics in things as follows:

– Things can use services that act as interfaces to things;

– Things could be competing with other things for resources, services and subject to selective pressures;

– Things may have embedded or attached sensors (and/or actuators), thus they can interact with their environment;

– Things use protocols to communicate with each other and the infrastructure; and

– Things are environmentally safe, where things are devices for identification, sense or communication, etc.

6.3 Social characteristics

Things have the following social characteristics towards other things or people:

– Things can communicate with other things, computing devices and with people;

– Things can collaborate to create groups or networks;

– Things can initiate communication without human intervention;

– Things can create, manage and destroy other things; and

– Things can respect the privacy, security and safety of other things or people with which they interact.

6.4 Autonomy of things

Autonomy is an important feature of the IoT. The followings are characteristics of autonomous things:

– Things can do many tasks autonomously;

– Things can negotiate, understand and adapt to their environment;

– Things can extract patterns from the environment or to learn from other things;

– Things can take decisions through their reasoning capabilities; and

– Things can selectively transform or evolve and propagate information.

6.5 Capability of self-replication or control

Autonomous things tend to have a capability of self-replication or control under specific conditions.

– Things can create, manage and destroy other things.

7 Characteristics of IoT applications

NOTE – Characteristics given in clauses 7.1 to 7.5 refer to [ITU-T Y.2060] and characteristics given in clauses 7.6 to 7.10 refer to [ISO/IEC 29182-1].

7.1 Interconnectivity

In the IoT, anything will be inter-connected with the global information and communication infrastructure.

7.2 Things-related services

The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in the physical world and information world will change.

7.3 Heterogeneity

The devices in the IoT are heterogeneous and based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

7.4 Dynamic changes

The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices involved can change dynamically.

7.5 Enormous scale

The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

7.6 Data gathering and processing by things

IoT devices gather data from the real world and pre-process the data. Then IoT services are provided to the user, either directly from IoT devices or via a service provider.

NOTE – As seen in the definition of the IoT, sensor network technology is one of the key enablers for IoT services. [ISO/IEC 29182-1] describes the characteristics and defines the requirements of sensor networks. This clause rephrases the characteristics described in [ISO/IEC 29182-1] for reflecting the characteristics of the IoT.

7.7 Collaborative data processing

In IoT applications, IoT devices may collaborate to solve complex sensing problems such as the detection, classification and tracking of objects in the physical world. The data from an IoT device may be pre-processed and refined at the IoT device acquiring the data or at another IoT device.

Depending on the application, intermediate data, such as features or estimated parameters, may be extracted from the captured data during pre-processing. The results from this pre-processing may be shared among IoT devices. Once shared, the intermediate data from the multiple IoT devices can be transformed into context data and situation information by data fusion.

NOTE – As seen in the definition of the IoT, sensor network technology is one of the key enablers for IoT services. [ISO/IEC 29182-1] describes the characteristics and defines the requirements of sensor networks. This clause rephrases the characteristics described in [ISO/IEC 29182-1] for reflecting the characteristics of the IoT.

7.8 Maintenance-free operation

IoT devices may have to operate for long periods of time without maintenance or technical support to resolve problems. Provision of remote diagnostics and resolution may be required.

NOTE – As seen in the definition of the IoT, sensor network technology is one of the key enablers for IoT services. [ISO/IEC 29182-1] describes the characteristics and defines the requirements of sensor networks.

This clause rephrases the characteristics described in [ISO/IEC 29182-1] for reflecting the characteristics of the IoT.

7.9 Self-adaptation

IoT devices may self-adapt to accommodate changing operating conditions, to support robustness and reliability and to optimize resource management and functionality.

NOTE – As seen in the definition of the IoT, sensor network technology is one of the key enablers for IoT services. [ISO/IEC 29182-1] describes the characteristics and defines the requirements of sensor networks. This clause rephrases the characteristics described in [ISO/IEC 29182-1] for reflecting the characteristics of the IoT.

7.10 Energy efficiency and operating lifetime

Energy management is important in many IoT devices where the IoT device is battery-operated and it is desirable for the device to be operational for as long as possible. Energy harvesting technologies may help with energy management and extending the device lifetime.

NOTE – As seen in the definition of the IoT, sensor network technology is one of the key enablers for IoT services. [ISO/IEC 29182-1] describes the characteristics and defines the requirements of sensor networks. This clause rephrases the characteristics described in [ISO/IEC 29182-1] for reflecting the characteristics of the IoT.

7.11 Embedded intelligence

Embedded intelligence can be defined as the capability of things to collect information of the surroundings and analyse it to learn the state of the real world, possibly interacting with other widely deployed things. Smart things (or intelligent objects [b-SPRINGER-TRON]) are things with embedded intelligence that can interoperate with each other and can act independently if necessary.

Embedded intelligence (sometimes called ambient intelligence) and autonomous control will be integrated into IoT devices. The IoT is a large non-deterministic and open network in which auto-organized or intelligent entities (web services, service oriented architecture (SOA) components), and virtual objects will interoperate with each other, and shall be able to act independently depending on the context, circumstances or environments.

7.12 Location considerations

The precise geographic location of a thing and its precise geometrical dimensions will be critical (i.e., some things in the IoT will be sensor nodes in sensor networks. Sensor node location is important for many applications.)

It is desirable to provide the location context to the things and, if appropriate, to IoT applications in order to take full of advantage of the IoT.

7.13 Auto-configuring reliable information transmission over ubiquitous networks

According to the diversity of IoT services, the services information categories become much richer and differentiation of quality of service (QoS) in each category becomes more complicated than in existing networks. Information service, rather than connection service, will be a basic operation feature of the networks used in the IoT. As an infrastructure and support environment for a ubiquitous information society, ubiquitous networks will be an important feature in the IoT service environment. Reliable transmission technologies that are easy to set up or are auto-configuring are required in existing and/or evolving networks to provide ubiquitous and intelligent services and provide people with rich real-world information.

7.14 Security

In the IoT, all things are connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.

7.15 Privacy

Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. Unlike ordinary desktop and other legacy applications, in the IoT data may be collected by a ubiquitous sensor network (USN) without human users being aware of such collection.

7.16 Infrastructure-less versus infrastructure-based application

Some IoT applications, such as machine-to-machine (M2M), machine-type communications (MTC), machine oriented communications (MOC) or USN-based applications, require network infrastructure (for example, Internet or mobile telecommunication networks as a delivery/backbone network). In contrast, some applications used in smart home or smart office may not require network infrastructure. These two types of application will have different requirements. Still, it is required that these two types of applications be able to talk to each other through proper gateways.

7.17 Observation and/or actuation vs. data exchanges

Typically, things with embedded sensors observe physical environments and acquire information about surroundings. Based on this information, some devices are actuated (actuators) and physical surrounding can be controlled. Some applications, such as RFID applications for example, use data exchanges between things. In this type of application, data that the thing acquires from outside and/or holds inside are essential to provide the IoT services.

7.18 Application domains

IoT applications can be deployed in many domains. Table 7-1 lists typical application domains. This list is not exhaustive.

In the IoT, inter-domain applications will also be very common.

For example, a pre-planning of an outdoor outing by a family or a group of friends can use the following services.

– Information provided about transportation: train timetable and its operation status, expressway congestion, etc.
– Weather services of regions to be visited.
– Information about the environmental conditions of natural habitats such as mountains, rivers, lakes, marshes, etc. of the area to be visited.
– If the outing is overnight, information related to reservations (for example, hotel, camping sites or restaurants).
– If someone in the group is physically challenged, information on accessibility.

Table 7-1 – Example of IoT application domains

Domains	Description	Examples
Industry	Activities involving financial or commercial transactions among companies, organizations and other entities: These include business to business (B2B) and business to customers (B2Cs)	Manufacturing, logistics, service sector, banking, financial governmental authorities, intermediaries, etc.
Environment	Activities regarding the protection, monitoring and development of all natural resources	Agriculture and breeding, recycling, environmental management services, energy management, etc.
Society	Activities/initiatives regarding the development and inclusion of societies, cities and people	Governmental services towards citizens and other society structures (e-participation), e-inclusion (e.g., elderly, disabled people), public transportation, etc.
Home	Activities concerning individual and family members	Health monitoring for oneself (weight, sleeping hours, etc.), nutrition care by monitoring of diet taken by family members using Cloud database.

8 Common requirements for IoT applications

NOTE – Requirements given in clauses 8.2 to 8.10 refer to [ITU-T Y.2060]. The requirements of the IoT as a whole and the requirement for a single IoT application need to be considered separately. The requirements for IoT applications are defined here.

8.1 Identification

For communication between things, unique identification of the thing to communicate is required before communication. Many identification schemes may be used, depending on the application (e.g., RFID applications, sensor network applications and M2M applications).

8.2 Identification-based connectivity

IoT applications are required to support the establishment of connectivity between a thing and the IoT based on the thing's identifier.

A common approach is required for handling the possible assignment of heterogeneous identifiers to different types of things (see clause 7.16).

8.3 Interoperability

Interoperability is required to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services (see clauses 7.1 and 7.3). Proper gateways are required to be provided if infrastructure-less and infrastructure-based applications are mixed.

8.4 Autonomic networking

Autonomic networking (such as self-management, self-configuring, self-healing, self-optimizing, and self-protecting techniques and/or mechanisms; see clause 7.13) may be supported in networking control functions of the IoT in order to adapt to different application domains (see clause 7.18), different communication environments (see clauses 7.1, 7.3 and 7.16) and large numbers and types of devices (see clause 7.5).

8.5 Autonomic services provisioning

The services may be provided by capturing, communicating and processing automatically the data of things based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and data mining. Some things may be equipped with actuators to act on the surrounding environment.

8.6 Location-based capabilities

The IoT as a whole supports location-based services. Location-based capabilities may be optionally supported by IoT applications. Certain types of communications and services will depend on the location information of things and/or users. It is required to sense and track the location information automatically, unless security and/or privacy concerns dictate otherwise, when location information is necessary for an IoT application.

8.7 Security

Generally accepted measures for providing confidentiality, authenticity and integrity of data are required to be provided to the things and servers after a proper threat-analysis is performed. The proper threat-analysis is required to pay attention the characteristics of an IoT application in particular (see clause 7.14)

8.8 Privacy protection

Privacy protection is required to be supported in the IoT. IoT applications are required to support privacy protection during data transmission, aggregation, storage, mining and processing. Privacy protection is recommended to strike a balance and not to impose an undue a barrier to data source authentication provided by the authentication requirement.

8.9 Plug and play

Plug and play capability is an important feature to be supported in the IoT in order to enable on-the-fly generation for seamless integration and cooperation of interconnected things with applications, and for improving responsiveness of things to application requirements. IoT applications are recommended to support plug and play features (see clauses 7.8 and 7.13).

8.10 Manageability

Manageability is required to be supported in the IoT in order to ensure normal network operations. IoT applications usually work automatically without people's participation, but their whole operation process should be manageable by the relevant parties.

8.11 Compliance with laws and regulations

Communications and services may be constrained by laws and regulations. Such constraints are often found in location-based services (see clause 8.6), and services related to human body.

Often security and privacy requirements are imposed by laws and regulations (see clauses 8.7 and 8.8). These are required to be obeyed in a global manner and IoT applications must meet local requirements as well.

8.12 Awareness of service

Even though IoT services are generally available without human intervention, humans (the users of IoT services) may need to be aware of IoT services surrounding them. When IoT services are provided to a user, it is recommended that the user be able to notice (discover) their presence. This has implication for security and privacy protection (for example surveillance, see clauses 8.7 and 8.8) [b-EC-PRIVACY].

8.13 Mobility support

IoT devices can be either mobile or static. When an IoT device moves from place to place, it is necessary to support mobility at the application level (such as service mobility between different service providers) as well as the network level. Therefore, IoT applications are recommended to support mobility of IoT devices.

8.14 Scalability support

As stated in clause 7.5, the scale of the network of IoT devices may be huge. IoT applications are recommended to support scalability, including the number of devices, the volume of data traffic that needs to be communicated, etc.

8.15 Robustness against dynamic changes

Clause 7.4 describes dynamic change of status of an IoT device. Therefore, IoT applications are recommended to provide robustness, e.g., seamless continuity and sustainability, against dynamic transformation and change of IoT devices.

8.16 Self-organization (re-organization) and self-healing

IoT devices may provide maintenance-free operation and may be self-adaptable as described in clauses 7.8 and 7.9. For coping with these characteristics, IoT applications are recommended to support self-organization (re-organization) and self-healing of the application and the network on the IoT device to recover from failure or mal-function. This requirement is related to robustness against dynamic transformation and changes in clause 8.15.

8.17 Energy efficient operation

IoT applications are recommended to operate IoT thing devices in a way that minimizes the necessary energy for operation. This will ensure longer battery life, if the devices are battery-operated (see clause 7.10), and longer maintenance-free operation (see clause 7.8). This will also help reduction of carbon gas emissions.

8.18 Common data format for collaborative data processing

IoT applications are recommended to adopt common data formats (see clause 7.7). This is to facilitate the mixing and mashing of data gathered by many IoT applications (which adds value to the collected data as a whole) as well as to facilitate data exchange.

Bibliography

[b-CERP-IoT] *Vision and Challenges for Realizing the Internet of Things*, CERP-IoT (Cluster of European Research Projects on the Internet of things), Publication Office of The European Union, March 2010, ISBN 978-92-79-15088-3. Also available online at http://bookshop.europa.eu/en/vision-and-challenges-for-realising-the-internet-of-things-pbKK3110323/

[b-EC-PRIVACY] *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 2011. Available online at http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[b-SPRINGER-TRON] *TRON Project 1987 Open Architecture Computer Systems*, Proceedings of the Third TRON Project Symposium, Springer Verlag, 1987, ISBN 978-4431700272.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015