International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2066

(06/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Common requirements of the Internet of things

Recommendation ITU-T Y.2066

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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
Network control architectures and protocols	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.3999

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

Recommendation ITU-T Y.2066

Common requirements of the Internet of things

Summary

Recommendation ITU-T Y.2066 provides the common requirements of the Internet of things (IoT). These requirements are based on general use cases of the IoT and IoT actors, which are built from the definition of IoT contained in Recommendation ITU-T Y.2060. The common requirements of the IoT are independent of any specific application domain, which refer to the areas of knowledge or activity applied for one specific economic, commercial, social or administrative scope, such as transport application domain and health application domain.

This Recommendation builds on the overview of IoT (Recommendation ITU-T Y.2060), developing the common requirements based on general use cases of the IoT and the IoT actors and taking into account important areas of consideration from a requirement perspective. Some representative use cases of the IoT, which are abstracted from application domains, are also provided. The common requirements of the IoT specified in this Recommendation are classified into the categories of non-functional requirements, application support requirements, service requirements, communication requirements, device requirements, data management requirements and security and privacy protection requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2066	2014-06-22	13	11.1002/1000/12169

Keywords

Common requirements, functional requirements, Internet of things (IoT), non-functional requirements, use cases.

* 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 Y.2066

Common requirements of the Internet of things

1 Scope

This Recommendation provides the common requirements of the Internet of things (IoT). These requirements are based on general use cases of the IoT and IoT actors, which are built from the definition of IoT contained in [ITU-T Y.2060]. The common requirements of the IoT are independent of any specific application domain, which refer to the areas of knowledge or activity applied for one specific economic, commercial, social or administrative scope, such as transport application domain and health application domain.

This Recommendation builds on the overview of IoT [ITU-T Y.2060], developing the common requirements based on general use cases of the IoT and IoT actors and taking into account important areas of consideration from a requirement perspective. The common requirements of the IoT specified in this Recommendation are classified into the categories of non-functional requirements, application support requirements, service requirements, communication requirements, device requirements, data management requirements and security and privacy protection requirements.

The scope of this Recommendation includes:

- general use cases of the IoT
- IoT actors
- important areas of consideration from a requirement perspective
- common requirements of the IoT.

The common requirements of the IoT are summarized and numbered in Annex A.

Some representative use cases of the IoT, which are abstracted from application domains, are provided in Appendix I.

NOTE – Regulatory, legal and business aspects are outside the scope of this Recommendation. Protocol and interface related requirements (e.g., for the control and management aspects of IoT) are also outside the 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 Internet of things*.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 customer [ITU-T Y.2091]: The customer buys products and services from the enterprise or receives free offers or services. A customer may be a person or a business.

NOTE – There can be many users per customer.

3.1.3 device [ITU-T Y.2060]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.4 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 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 service [ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 application domain: An area of knowledge or activity applied for one specific economic, commercial, social or administrative scope.

NOTE – Transport application domain, health application domain and government application domain are examples of application domains.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G Second Generation

3G Third Generation

API Application Programming Interface

CAN Controller Area Network

DSL Digital Subscriber Line

IoT Internet of Things

ITS Intelligent Transport Systems

LTE Long Term Evolution

M2M Machine-to-Machine

MOC Machine Oriented Communication

SDP Service Delivery Platform

SLA Service Level Agreement

UML Unified Modelling Language

WiFi Wireless Fidelity

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 General use cases of the IoT and IoT actors

This clause describes general use cases of the IoT and IoT actors and the relations among general use cases and IoT actors. An IoT actor specified in this Recommendation refers to an entity that is external to the IoT and that interacts with the IoT.

6.1 General use cases

The general use cases are built from the definition of IoT contained in [ITU-T Y.2060].

According to the definition of IoT, given in [ITU-T Y.2060], IoT enables "advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". This implies that the IoT interconnects things to sense or actuate things and to provide advanced services, so the general use cases of "IoT sensing or actuating" and "IoT service provision" can be derived.

According to the definition of IoT, as given in [ITU-T Y.2060], "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". This implies that data capture and processing capabilities can be grouped as data management capabilities and privacy protection should be guaranteed. So the general use cases of "IoT data management" and "IoT privacy protection" can be derived.

Figure 6-1 shows the general use case model of the IoT, which is described via unified modelling language (UML), for more information see [b-UML]. This model consists of four general use cases: IoT sensing or actuating, IoT data management, IoT service provision and IoT privacy protection.

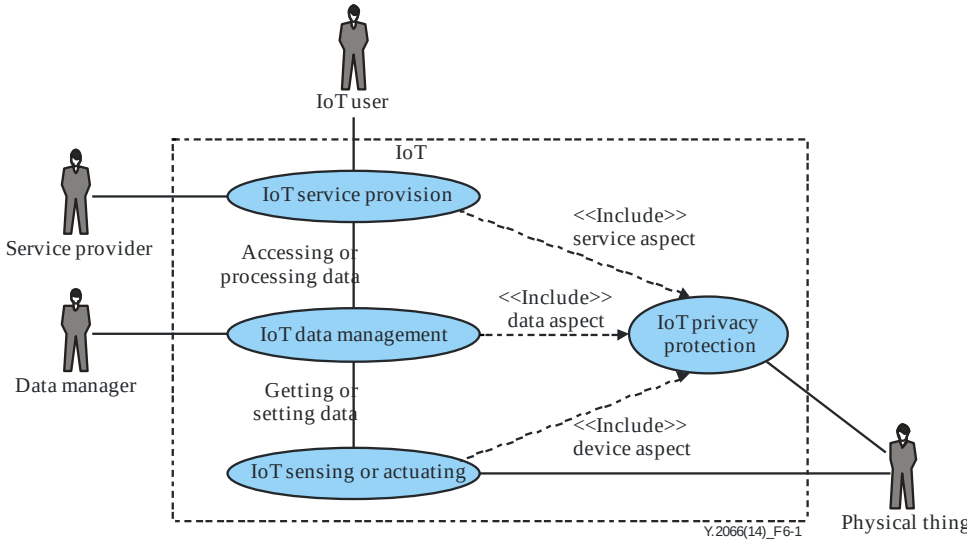

Figure 6-1 – The general use case model of the IoT

NOTE 1 – In [b-UML], a use case is defined as a single unit of meaningful work in a system. It may provide a view of behaviour observable by entities outside the system. The use cases can be used to capture the requirements of a system. A use case model (combination of single units of work) can show the interaction between the system and entities external to the system. These external entities are referred to as "actors" in UML. In this perspective, the IoT becomes the system being modelled with UML while an "IoT actor" is an entity that is outside the IoT, and interacts with the IoT.

NOTE 2 – Some use cases abstracted from IoT applications (the representative use cases described in Appendix I) can be decomposed into the general use cases described in clauses 6.1.1 to 6.1.4, to facilitate the generation of the functional requirements corresponding to the IoT actors. For example, the "video surveillance" use case described in Appendix I.1 can be decomposed into video capturing (IoT sensing or actuating), video transmission and storage (IoT data management) and video replay and analysis (IoT service provision) use cases. These use cases can be used to generate the functional requirements from different actors of video surveillance, such as time synchronization to support real-time video transmission and virtual storage to support storage of a large amount of video continuously generated by video cameras.

6.1.1 "IoT sensing or actuating" use case

"IoT sensing or actuating" use case is a general use case that can be applicable to multiple application domains. This use case involves the activities of connecting with physical things, sensing the states of physical things or actuating the physical things.

6.1.2 "IoT data management" use case

"IoT data management" use case is a general use case that can be applicable to multiple application domains. This use case involves the activities of capturing, transferring, storing and processing the data of physical things.

6.1.3 "IoT service provision" use case

"IoT service provision" use case is a general use case that can be applicable to multiple application domains. This use case involves the activities of providing services by the service provider and using services by the IoT user.

6.1.4 "IoT privacy protection" use case

"IoT privacy protection" use case is a general use case that can be applicable to multiple application domains. This use case involves the activities of securing and hiding the private information of the physical things.

6.1.5 The relationships among the general use cases

The relationships among the identified general use cases are shown in Figure 6-1. The "IoT data management" use case is related to both the "IoT sensing or actuating" use case and the "IoT service provision" use case. The "IoT privacy protection" use case is related to all other use cases.

6.2 The IoT actors

The use cases are used to capture the requirements of a system (see [b-UML]). Each use case includes the functional requirements of the actors involved in the use case.

According to the general use case model of IoT illustrated in Figure 6-1, there are four IoT actors: the "Physical thing" actor, the "Data manager" actor, the "Service provider" actor and the "IoT user" actor. These four IoT actors, described in this clause, are entities defined outside the IoT and specified from a requirement viewpoint. They are different from the business roles described in Appendix I of [ITU-T Y.2060], which are specified from a business viewpoint.

NOTE 1 – The "Physical thing" actor described in this Recommendation corresponds to physical thing as described in [ITU-T Y.2060]. According to the general use case model of IoT, the actor that would correspond to virtual thing as described in [ITU-T Y.2060] is not considered in this Recommendation since a virtual thing is an entity of the IoT itself.

NOTE 2 – The following provides the applicable mappings between the IoT actors described in this Recommendation and the roles described in Appendix I of [ITU-T Y.2060]:

- The "IoT user" actor corresponds to the application customer role.
- The "Service provider" actor corresponds to application provider, platform provider and network provider roles.
- The "Data manager" actor corresponds to the application provider role in the case where the provided applications involve some data management functionalities and it may also correspond to the device provider role in the case where the provided devices involve some data management functionalities.

6.2.1 "Physical thing" actor

The "Physical thing" actor is an IoT actor that has a unique identifier in the physical world. "Physical thing" interacts with the IoT via sensing or actuating activities.

NOTE – The "Physical thing" actor can be further instantiated into "artificial thing" and "natural thing". An artificial thing is a physical thing that is produced by mankind and can be identified by a product serial number. A natural thing is a physical thing that is generated in nature and can be identified, for example, by generated time, location and its category. Sensing natural things can constitute a challenge in the development of IoT.

Note that, in the following clauses of this Recommendation, the term "thing" refers to "physical thing".

6.2.2 "Data manager" actor

The "Data manager" actor is an IoT actor that is responsible for management of capturing, storing, transferring and processing IoT data to satisfy the IoT service provision requirements.

NOTE – The "Data manager" actor can be further instantiated into human "Data manager" and machine "Data manager" actors. A human "Data manager" actor performs the data management of IoT manually while a machine "Data manager" actor performs this in an automatic manner. These two instantiations of the "Data manager" actor are associated with different use cases of IoT data management.

6.2.3 "Service provider" actor

The "Service provider" actor is an IoT actor that provides all possible services related with things, such as monitoring, location tracking and service discovery.

NOTE – The "Service provider" actor can be further instantiated into a common "Service provider" actor that provides services which are independent of specific application domains and into an application "Service provider" actor that provides applications based on specific application domains.

6.2.4 "IoT user" actor

The "IoT user" actor is an IoT actor that uses all possible services related with things, such as monitoring, location tracking and service discovery.

7 Important areas for consideration from a requirement perspective

There are several important areas that need to be focused on for the specification of requirements of the IoT. Based on the IoT characteristics and high level requirements contained in [ITU-T Y.2060] as well as results of IoT related public and academic research (e.g., [b-IoT-A D6.2]), the following clauses describe important areas for consideration from a requirement perspective.

7.1 Implementation and operational aspects

The implementation and operational aspects of IoT are an important area to be addressed, e.g., in order to achieve interoperability among heterogeneous IoT implementations and to obtain the adequate scalability for the support of a large amount of connected devices and high availability for the support of automatic operations in IoT.

7.2 Ubiquitous connectivity

In order to realize connectivity between things and IoT, ubiquitous connectivity is required to be considered. Connectivity capabilities need to be independent of specific application domains and integration of heterogeneous communication technologies needs to be supported.

7.3 End-to-end intelligence

End-to-end intelligence is required to be considered, in particular with regard to the "intelligence of communications" and the "intelligence of services", e.g., in order to provide services without human intervention. This includes consideration of location based communications and context based communications (which may be regarded as intelligent communications), content-aware services and context-aware services (which may be regarded as intelligent services), as well as self-configuration, self-healing, self-optimization and self-protection services (which may be regarded as other intelligent services termed as a whole as autonomic services [ITU-T Y.2060]).

7.4 Time synchronization

In order to keep time synchronicity among the actions of interconnected things when using communication and service capabilities, time synchronization is required to be considered.

7.5 Human body connectivity

In order to provide communication capabilities related with the human body in compliance with regulation and laws, the requirements of human body connectivity are required to be carefully considered. Special quality of service (QoS) is required to be specified, reliability is required to be quantified, and privacy protection is required.

7.6 A large amount of data from things

As there will be a large number of devices connected with the IoT, there will be a large amount of data – the term "big data" is popularly used to signify large volume, variety and velocity of data – transmitted from things to the IoT. In order to classify, transfer, store, process, validate and query the big data within the time as required by IoT users or applications, resource scalability, such as communication bandwidth, storage and processing capacity, should be considered.

7.7 Privacy protection related with things

The data from things may contain private information related to the owners or users of things. The data may be used to locate or trace the owners or users of the things violating their privacy. Privacy protection during capturing, transferring, storing, validating and processing data of things should be considered. Privacy protection should not be used to hinder the validation of data of things.

8 Common requirements of the IoT

The common requirements of IoT specified in this Recommendation are technical requirements and are independent of any specific application domain. Protocol and interface related requirements (e.g., for the control and management aspects of IoT) are outside the scope of this Recommendation.

8.1 Categories of IoT common requirements

In this Recommendation, the IoT common requirements are divided into non-functional requirements and functional requirements.

The IoT non-functional requirements refer to the requirements related to the implementation and operation of the IoT itself.

The IoT functional requirements refer to the requirements related to the IoT actors, i.e., entities which are external to the IoT and that interact with the IoT. The IoT functional requirements specified in this Recommendation are categorized as follows:

– application support requirements
– service requirements
– communication requirements
– device requirements
– data management requirements
– security and privacy protection requirements.

All the requirements described in the following clauses are listed and numbered in Annex A. In the following clauses, the requirement numbers, as shown in Annex A, are put between square brackets "[ ]" and inserted at the end of each paragraph describing the corresponding requirement(s).

8.2 Non-functional requirements

The requirements of this category are not related to any IoT actors as they are not derived from the general use cases of IoT described in clause 6.

8.2.1 Interoperability

Interoperability is required to be ensured among heterogeneous IoT implementations [N1].

NOTE – In order to support interoperability in IoT, there is a need to standardize an architecture reference model of IoT.

8.2.2 Scalability

Scalability is required to be supported in IoT in order to handle a large number of devices, applications and users [N2].

NOTE 1 – The requirement in scalability for handling a large number of devices implies the requirement of handling a large amount of data (big data) in IoT.

NOTE 2 – The requirement in scalability for handling a large number of applications and users implies the requirement of having a large amount of processing and storage resources. Such a requirement may be supported via the integration of cloud computing technologies in IoT.

NOTE 3 – Fairness in handling a large number of devices, applications and users should be considered.

8.2.3 Reliability

Reliability in capabilities of IoT, such as reliability in communication, service and data management capabilities of IoT, is required [N3].

NOTE – Consideration should be given to resilience for support of reliability

8.2.4 High availability

High availability is required in service provisioning, data management, communication, sensing and actuating things of IoT [N4].

8.2.5 Adaptability

Adaptability to the new technologies emerging in the future is required in IoT [N5].

NOTE – The technical standards used in IoT should impose minimum constraints concerning the adaptability to new technologies.

8.2.6 Manageability

Manageability is required to be supported in IoT in order to ensure normal operations. IoT operations are usually performed automatically without people's intervention, but the operation process should be manageable [N6].

NOTE 1 – Consideration should be given to device management in IoT, e.g., device state management, device connectivity management, energy consumption management, etc. The constraints in device resources, such as energy, memory and bandwidth, should be considered in device management.

NOTE 2 – Consideration should be given to automatic fault management in IoT, e.g., proactive fault reporting, fault diagnosis, fault recovery, etc.

NOTE 3 – Consideration should be given to automatic configuration management in IoT, e.g., automatic configuration of device parameters.

8.3 Application support requirements

Application support requirements refer to the functional requirements from the development of IoT applications in different application domains. These requirements are only related to the "service provider" actor.

8.3.1 Programmable interfaces

Standardized programmable interfaces are required in order to provide open access to application support capabilities [A1].

NOTE – Programmable interfaces allow the support of IoT applications in a programmable way.

8.3.2 Group management

Group management, including display, creation, modification, deletion of IoT groups and display, addition, modification and deletion of IoT group members, is required to be supported in IoT [A2].

NOTE – An IoT group may contain IoT users and/or devices.

8.3.3 Time synchronization

Reliable time synchronization is required, in order to support global time stamping in IoT [A3].

NOTE – Time stamping allows the provision of secure and trusted time critical services.

8.3.4 Collaboration

Collaboration is required among services or among devices accessing, with the same goal, IoT applications, so that the IoT can enable autonomous goal-driven collaboration among such services or devices [A4].

NOTE – Collaboration among devices accessing IoT applications is expected to be activated by the devices themselves, so that the IoT can support scalable collaboration with distributed control among such devices.

8.3.5 User management

User management is required, including creation, authentication, authorization and accounting of IoT users [A5].

8.3.6 Resource usage accounting

Accounting of IoT resource usage is required on a per application basis [A6].

8.4 Service requirements

These requirements are related to the service provider, IoT user and thing actors.

NOTE – According to the general definition of "service" as a set of functions and facilities offered to a user by a provider [ITU-T Y.2091], the service requirements are related to both the IoT user and service provider actors. This does not exclude the case of a service offered directly to the thing actor.

8.4.1 Service prioritization

Prioritization of services is required to satisfy the different service requirements of different groups of IoT users [S1].

NOTE – Differentiated services are expected to be supported, so that the IoT can provide different service level agreements (SLAs).

8.4.2 Semantic based services

Semantic based services are required in IoT to support autonomic service provisioning. The mechanisms for implementing semantic based services include service semantic annotation, service semantic access and semantic exchange among services [S2].

NOTE – Service semantic annotation can allow the semantic description of services. Service semantic access can be used to access services through semantic interfaces. Semantic exchange among services can enable the provision and exchange of semantics between services in order to support automatic creation of new services.

8.4.3 Service composition

Service composition is required to support flexible service creation in IoT [S3].

NOTE 1 – The primary services are a set of basic operations that cannot directly satisfy some requirements of IoT applications. Service composition is one of the service creation methods that can be used to automatically create more complex services based on primary services in order to satisfy all of the various requirements of IoT applications.

NOTE 2 – Existing flexible service provisioning technologies, such as service delivery platform (SDP), can support, among others, the requirements of service composition.

8.4.4 Mobility services

Mobility services are required, so that the IoT can support service mobility, user mobility and device mobility in the service provisioning perspective, e.g., service provisioning is not constrained by the service access location when service mobility is supported [S4].

8.4.5 Reliable and secure human body connectivity services

High reliability and security are required when human body connectivity services are provided [S5].

NOTE – Different countries may have different legal and regulatory requirements on these services.

8.4.6 Autonomic services

Autonomic services are required, so that the IoT can enable automatic capture, communication and processing of data of things based on rules configured by service providers or customized by IoT users [S6].

NOTE – Support of both centralized and decentralized control of autonomic services is expected, so that the IoT can enable centralized or decentralized automated activities.

Location based and context-aware services are required, so that the IoT can enable flexible, user-customized and autonomic services based on the location information and related context of things and/or users. [S7].

8.4.7 Service management

Service management is required so that service provisioning can be supported in a highly available and reliable way [S8].

NOTE – Service management includes, among others, service lifecycle management and service integrity checking. Service lifecycle management can help to increase service availability and service integrity checking can help to increase service reliability.

8.4.8 Discovery services

Discovery services are required, so that the IoT users, services, devices and data of things can be discovered by service providers or IoT users [S9].

NOTE – The service provider or IoT user can discover specific IoT users, services, devices and data of things according to different criteria, such as geographic location information, type of device, etc.

8.4.9 Service subscription support

Service subscription support is required, so that the IoT can provide a means to allow the IoT user to subscribe to the needed services and associated data of things [S10].

8.4.10 Naming and addressing

Standardized naming and addressing of things and services is required [S11].

8.4.11 Virtual storage and processing

Virtual storage and processing capabilities are required in order to store and process a large amount of data (big data) [S12].

8.5 Communication requirements

Communication requirements refer to the functional requirements related to message exchange among the IoT user, service provider, data manager and thing actors. These requirements are related to all the IoT actors.

8.5.1 Communication modes

Event-based, periodic and automatic communication modes between devices or between IoT users are required to be supported [C1].

The support of the unicast communication mode is required (e.g., for communications between IoT users or devices). The support of the multicast, broadcast and anycast communication modes is required, so that the IoT can provide various communication services within a group of IoT users or devices (e.g., to support the collaboration among IoT users or devices) [C2].

NOTE – It is recommended to support event-based, periodic and automatic communication modes between devices or between IoT users, while preserving network performance by the support of mechanisms for avoiding the possibility of traffic congestion.

The support of device initiated communications is required so as to satisfy the requirements of automatic communications [C3].

8.5.2 Communication control

Error control for communications is required to be supported, so that the IoT is able, for example, to cope with interferences between devices [C4].

Time-critical communications are required to be supported, so that the IoT can provide time-critical message handling and delivery [C5].

8.5.3 Intelligent communication

The requirements of intelligent communication include requirements of autonomic networking [ITU-T Y.2060], content-aware communication and location based communication.

Autonomic networking is required in IoT to support self-configuring, self-healing, self-optimizing and self-protecting capabilities at the networking level, in order to adapt to different application domains, different communication environments and large numbers and varied types of devices [C6].

Content-aware communication is required, so that, for example, the IoT can provide a support for path selection and routing of communications based on content [C7].

Location based communication is required, so that the IoT can support location based interactions among IoT actors [C8].

NOTE – Location information is expected to be captured and traced automatically.

8.5.4 Heterogeneous communication support

Communications can take place in the device layer (see [ITU-T Y.2060]) through various kinds of wired or wireless technologies, such as controller area network (CAN) bus, ZigBee, Bluetooth, WiFi, etc. Support for heterogeneous device related communication technologies is required [C9].

Communications can take place in the network layer (see [ITU-T Y.2060]) through various kinds of technologies, such as second generation/third generation (2G/3G), long term evolution (LTE), Ethernet, digital subscriber line (DSL), etc.

Support for heterogeneous network related communication technologies is required [C10].

8.6 Device requirements

Device requirements refer to the functional requirements from the piece of equipment connected with things. These requirements are related to the IoT user and thing actors.

8.6.1 Connectivity of things

The IoT is required to support the establishment of the connectivity between a thing and the IoT based on the identifier of the thing [D1].

NOTE – Heterogeneous identifiers of things are expected to be processed in a unified way, (see [ITU-T Y.2060]).

8.6.2 Device control and configuration

Support of remote monitoring, control and configuration of devices is required so that device manageability in IoT is increased [D2].

Plug and play capability is required to be supported in IoT in order to enable on-the-fly generation, composition or acquisition of semantic-based configurations for seamless integration and cooperation of things with applications and responsiveness to application requirements, (see [ITU-T Y.2060]) [D3].

8.6.3 Monitoring of things

Automatic notification of the status of things and its changes is required in order to monitor things in timely manner [D4].

8.6.4 Device mobility

Device mobility is required, so that the IoT can support mobility of things connected with devices [D5].

8.6.5 Device integrity checking

Device integrity checking is required, in order help to support high availability of devices [D6].

8.7 Data management requirements

Data management requirements refer to the functional requirements from storing, aggregating, transferring and processing the data of the IoT. These requirements are related to the data manager and IoT user actors.

8.7.1 Data storage

Storing data of things based on predefined rules and policies is required to be supported [DM1].

8.7.2 Data processing

Data fusion and mining based on predefined rules and policies are required to be supported [DM2].

8.7.3 Data query

Querying stored historical data of things is required to be supported, so that the IoT can provide historical information about things [DM3].

8.7.4 Data access control

Access control of data by their owner is required to be supported in IoT, so that IoT users can have the ability to control how their data are exposed to other IoT users [DM4].

8.7.5 Data exchange

Data exchange with entities outside the IoT is required to be supported, so that the IoT is able to provide access to external data sources, e.g., health databases outside the IoT [DM5].

8.7.6 Data validation

Integrity checking and life cycle management of data of things are required to be supported, so that the IoT is able to provide high availability and reliability of data of things [DM6].

8.7.7 Semantic annotation and access to data of things

Semantic annotation of data of things is required. Semantic access to data of things is required, so that automatic querying of things can be supported [DM7].

8.7.8 Semantic storage, transfer and aggregation of data of things

Semantic storage, transfer and aggregation of data of things are required, so that storage, transfer and aggregation of data of things can be performed automatically according to the requirements of IoT users or applications [DM8].

8.8 Security and privacy protection requirements

Security and privacy protection requirements 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. These requirements are related to all the IoT actors.

8.8.1 Communication security

Secure, trusted and privacy protected communication capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected during data transmission or transfer in IoT [SP1].

8.8.2 Data management security

Secure, trusted and privacy protected data management capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected when storing or processing data in IoT [SP2].

8.8.3 Service provision security

Secure, trusted and privacy protected service provision capability is required, so that unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected [SP3].

8.8.4 Integration of security policies and techniques

The ability to integrate different security policies and techniques is required, so as to ensure a consistent security control over the variety of devices and user networks in IoT [SP4].

8.8.5 Mutual authentication and authorization

Before a device (or an IoT user) can access the IoT, mutual authentication and authorization between the device (or the IoT user) and IoT is required to be performed according to predefined security policies [SP5].

8.8.6 Security audit

Security audit is required to be supported in IoT. Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws. In particular, IoT is required to support security audit for data transmission, storage, processing and application access [SP6].

Annex A

The IoT common requirements list

(This annex forms an integral part of this Recommendation.)

The following table lists and numbers the requirements described in clause 8 "Common requirements of the IoT".

Requirement number	Requirement category	Requirement description	Summary of the requirement	
N1	Non-functional	Interoperability is required to be ensured among heterogeneous IoT implementations.	Interoperability is required.	
N2	Non-functional	Scalability is required to be supported in IoT in order to handle a large amount of devices, applications and users.	Scalability is required.	
N3	Non-functional	Reliability in capabilities of IoT, such as reliability in communication, service and data management capabilities of IoT, is required	Reliability is required.	
N4	Non-functional	The IoT is required to provide high availability in service provisioning, data management, communication, sensing and actuating things.	High availability is required.	
N5	Non-functional	Adaptability to the new technologies emerging in the future is required in IoT	Adaptability is required.	
N6	Non-functional	Manageability is required to be supported in IoT in order to ensure normal operations.	Manageability is required.	
A1	Application support	Programmable interfaces are required to be standardized to provide open access to application support capabilities.	Standardized programmable interfaces are required.	
A2	Application Support	Group management, including display, creation, modification, deletion of IoT groups and display, addition, modification, deletion of IoT group members, is required to be supported in IoT.	Group management is required.	
A3	Application Support	In order to support global time stamping in IoT, reliable time synchronization is required.	Reliable time synchronization is required.	
A4	Application Support	Collaboration among services or among devices with the same goal accessing IoT applications is required.	Collaboration is required.	

Requirement number	Requirement category	Requirement description	Summary of the requirement	
A5	Application support	User management is required, including creation, authentication, authorization and accounting of IoT users.	User management is required.	
A6	Application support	Accounting of IoT resource usage is required on a per application basis.	Resource usage accounting is required.	
S1	Service	Prioritization of services is required to satisfy the different service requirements of different groups of IoT users.	Prioritization of services is required.	
S2	Service	Semantic based services are required in IoT to support autonomic service provisioning.	Semantic based services are required.	
S3	Service	Service composition is required to support flexible service creation in IoT.	Service composition is required.	
S4	Service	Mobility services are required, so that the IoT can support service mobility, user mobility and device mobility.	Mobility services are required.	
S5	Service	High reliability and security are required when human body connectivity services are provided.	Highly reliable and secure human body connectivity services are required.	
S6	Service	Autonomic services are required, so that the IoT can enable automatic capture, communication and processing of data of things based on rules configured by service providers or customized by IoT users.	Autonomic services are required.	
S7	Service	Location based and context-aware services are required, so that the IoT can enable flexible, user-customized and autonomic services based on the location information and related context of things and/or users.	Location based and context-aware services are required.	
S8	Service	Service management is required so that service provisioning can be supported in highly available and reliable way.	Service management is required.	
S9	Service	Discovery services are required, so that the IoT users, services, devices and data of things can be discovered by service providers or IoT users.	Discovery services are required.	

Requirement number	Requirement category	Requirement description	Summary of the requirement	
S10	Service	Service subscription support is required, so that the IoT can provide a means to allow the IoT user to subscribe to the needed services and associated data of things.	Service subscription support is required.	
S11	Service	Standardized naming and addressing of services and things is required.	Standardized naming and addressing is required.	
S12	Service	In order to store and process a large amount of data (big data), virtual storage and processing capabilities are required.	Virtual storage and processing capabilities are required.	
C1	Communication	The IoT is required to support event-based, periodic and automatic communications between devices or between IoT users.	Event-based, periodic, and automatic communication modes are required to be supported.	
C2	Communication	The support of the unicast communication mode is required (e.g., for communications between IoT users or devices). The support of the multicast, broadcast and anycast communication modes is required, so that the IoT can provide various communication services within a group of IoT users or devices (e.g., to support the collaboration among IoT users or devices).	The support of the unicast, multicast, broadcast and anycast communication modes is required.	
C3	Communication	The support of device initiated communications is required so as to satisfy the requirements of automatic communications.	The support of device initiated communications is required.	
C4	Communication	Error control for communications is required, so that the IoT is able, for example, to cope with interferences between devices.	Error control for communications is required to be supported.	
C5	Communication	The IoT is required to provide time-critical message handling and delivery.	Time-critical communications are required to be supported.	
C6	Communication	Self-configuring, self-healing, self-optimizing and self-protecting capabilities at the networking level are required in IoT.	Autonomic networking is required.	

Requirement number	Requirement category	Requirement description	Summary of the requirement	
C7	Communication	Content-aware communication is required, so that, for example, the IoT can provide a support for path selection / and routing of communications based on content.	Content-aware communication is required.	
C8	Communication	The IoT is required to support location based interactions among IoT actors.	Location based communication is required.	
C9	Communication	Communications can take place in the device layer [ITU-T Y.2060] through various kinds of wired or wireless technologies, such as controller area network (CAN) bus, ZigBee, Bluetooth, WiFi, etc.	Support for heterogeneous device related communication technologies is required.	
C10	Communication	Communications can take place in the network layer [ITU-T Y.2060] through various kinds of technologies, such as second generation /third generation (2G/3G), long term evolution (LTE), Ethernet, digital subscriber line (DSL), etc.	Support for heterogeneous network related communication technologies is required.	
D1	Device	The IoT is required to support the establishment of the connectivity between a thing and the IoT based on the identifier of the thing.	Identification-based connectivity between a thing and the IoT is required.	
D2	Device	Support of remote monitoring, control and configuration of devices is required so that device manageability in IoT is increased.	Remote monitoring, control and configuration of devices are required.	
D3	Device	Plug and play capability is required to be supported in IoT in order to enable on-the-fly semantic-based configurations of devices.	Plug and play capability is required.	
D4	Device	Automatic notification of the status of things and its changes is required in order to monitor things in a timely manner.	Monitoring things in a timely manner is required.	
D5	Device	The IoT is required to support mobility of things.	Device mobility is required.	
D6	Device	Device integrity checking is required, in order to support high availability of devices.	Device integrity checking is required.	

Requirement number	Requirement category	Requirement description	Summary of the requirement	
DM1	Data management	The IoT is required to support storing data of things based on predefined rules and policies.	Storing data of things is required to be supported.	
DM2	Data management	Data fusion and mining based on predefined rules and policies are required to be supported.	Processing data of things is required to be supported.	
DM3	Data management	The IoT is required to provide historical information about things	Querying historical data of things is required to be supported.	
DM4	Data management	Access control of data by their owner is required to be supported in IoT, so that IoT users can have the ability to control how their data are exposed to other IoT users	Data access control by the data owners is required.	
DM5	Data management	The IoT is required to provide access to external data sources, e.g., health databases outside the IoT.	Data exchange with entities outside the IoT is required to be supported.	
DM6	Data management	The IoT is required to provide integrity checking and life cycle management of data of things, so that the IoT is able to provide high availability and reliability of data of things.	Integrity checking and life cycle management of data of things is required.	
DM7	Data management	Semantic annotation of data of things is required. Semantic access to data of things is required, so that automatic querying of things can be supported.	Semantic annotation and semantic access to data of things are required.	
DM8	Data management	Storage, transfer and aggregation of data of things are required to be performed automatically according to the requirements of IoT users or applications.	Semantic storage, transfer and aggregation of data of things are required.	
SP1	Security and privacy protection	The IoT is required to support secure, trusted and privacy protected communication capability.	Communication security is required.	
SP2	Security and privacy protection	The IoT is required to provide secure, trusted and privacy protected data management capability.	Data management security is required.	
SP3	Security and privacy protection	The IoT is required to provide secure, trusted and privacy protected service provision capability.	Service provision security is required.	

Requirement number	Requirement category	Requirement description	Summary of the requirement	
SP4	Security and privacy protection	Integration of different security policies and techniques related to the variety of devices and user networks in IoT is required.	Integration of different security policies and techniques is required.	
SP5	Security and privacy protection	Before a device (or an IoT user) can access the IoT, mutual authentication and authorization is required according to predefined security policies.	Mutual authentication and authorization is required.	
SP6	Security and privacy protection	Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws.	Security audit is required to be supported in IoT.	

Appendix I

Representative use cases of the IoT

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

This appendix describes some representative use cases of the IoT, which are abstracted and classified based on application use cases within application domains or across multiple application domains.

I.1 Video surveillance

Video surveillance is a typical class of use cases present in numerous IoT applications. For example, in smart city applications, video cameras are used to watch people's movements for city safety purposes. In pollution supervision, video surveillance is used to watch whether polluted water flows out of a factory. Hospitals use video surveillance to watch the status of a patient remotely.

Video surveillance typically requires a large number of resources, such as high communication bandwidth for transferring video, a large amount of storage resources for keeping copies of video and powerful processors for searching and processing video.

I.2 Emergency alerting

Emergency alerting is abstracted from a large number of use cases, such as rescue message transmission when a patient heart disease occurs, alerting message transmission before a vehicle fails to work normally or after that, when a traffic accident happens, and alerting message transmission when blood pressure exceeds a threshold value.

Such use cases require high priority and reliable data transport with minimized time delay and also require device-initiated communication capabilities.

I.3 Data acquisition

This class of use cases includes a number of use cases, such as gas metering, water metering and quality monitoring, electricity metering, bus ticket terminal data uploading, etc. In these use cases, data communications happen at regular time intervals.

These use cases require mechanisms for periodical data transmission. The transmission task may be activated automatically under a given policy. Normally, in most of these use cases, the throughput of data transmission is low.

I.4 Remote control

This class of use cases includes use cases within a number of application domains, such as home automation, manufacturing and intelligent transport systems (ITS). In these use cases, the IoT application requires the capability for the user to control devices remotely.

For this class of use cases, data communications for controlling remote devices are not continuous and do not necessarily happen at regular time intervals. These use cases require mechanisms to establish connectivity between controllers and remote devices initiated by controllers or devices only when data transmission is required.

I.5 Transfer of events across different application domains

In many IoT applications such as smart city and emergency management applications, events that happen in one application domain are transferred to other relevant application domains. Based on events transferred across different application domains, different applications can work collaboratively so that more functions and services can be provided than those specific to a single application domain. Examples of such use cases include events transferred between road and bridge maintenance applications, between traffic management and driving applications, between weather forecast and flood prevention applications, etc.

Such use cases need that the events be described in a standardized format so the different IoT applications can understand them. Furthermore, the events should be transferred reliably and securely.

I.6 Data sharing across different application domains

Some data are of importance not only in the IoT application where such data are collected, but also in other IoT applications. Such data includes geographic position data, road traffic data, etc. In accordance with appropriate regulation and laws, data may also be shared across different application domains thus allowing for more functions and services to be provided. For example, data related to the geographic position of mobile phones might be used for calculating the road traffic.

Such use cases need standardized data formats among the different IoT application domains so that data can be shared across different application domains.

I.7 Integrated operating centre for smart city

Smart cities developed based on IoT infrastructure are becoming a new trend in city development all over the world. In the future, cities will need to have an intelligent "brain" system to analyse different kinds of data collected by IoT devices and to act upon their analysis and other related actions. Such a city brain system may be referred to as an "integrated operating centre for a smart city".

This integrated operating centre basically requires data sharing, aggregation and processing across multiple application domains. For example, implementations of such an integrated operating centre usually require the integration of urban real-time operational status information with event monitoring, data analysis, intelligent early warning and information dissemination, intelligent decision-making and integrated command and dispatching.

I.8 One detailed use case: traffic accident information collection

An ITS-station (ITS-S) inside a vehicle that is directly involved in or is passing by an accident detects that a crash has happened and starts an accident reporting process automatically. It tries to connect to the IoT and then sends the accident report to it. The IoT receives and verifies the accident report and the analysis result is pushed to the service subscribers, i.e., a Police Station and a Rescue Centre.

The service subscribers can ask the IoT to collect more information about the accident. The IoT receives these service requests and then asks the ITS-Ss to collect some more information according to the requests of the subscribers. The ITS-Ss in proximity to the accident site receive, verify, parse and execute the received commands, i.e., take pictures, get current travel status, generate reports, sign the reports and upload signed reports to the IoT. The IoT accumulates and verifies the reports uploaded by the ITS-Ss and then generates a report containing visual information about the accident scene for the Rescue Centre and a report about the traffic situation near the accident site. These reports are again pushed to the Rescue Centre and Police Station respectively.

The rescue centre analyses the report about the accident scene and then formulates a specific rescue plan. The police station analyses the report about traffic situation and formulates a specific traffic control plan.

This use case requires device-initiated communication capability, secure and trust communication capability and event-driven collaboration among different applications.

Bibliography

[b-ITU-T Y.2061] Recommendation ITU-T Y.2061 (2012), *Requirements for the support of machine-oriented communication applications in the next generation network environment.*

[b-IoT-A D6.2] The Internet of Things Architecture – IoT-A (2011), *Project Deliverable D6.2 – Updated Requirements List*.
http://www.iot-a.eu/public/public-documents/documents-1

[b-UML] ISO/IEC 19505-2:2012, *Information technology – Object Management Group Unified Modeling Language (OMG UML) – Part 2: Superstructure*.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=52854

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, 2014