

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

Y.2066

(06/2014)

Y系列：全球信息基础设施、互联网的协议问题、下一代网络、物联网和智慧城市

下一代网络 – 框架和功能性架构模型

物联网的共同要求

ITU-T Y.2066建议书

ITU-T



ITU-T Y系列建议书

Y系列：全球信息基础设施、互联网的协议问题、下一代网络、物联网和智慧城市

全球信息基础设施	
概要	Y.100 – Y.199
业务、应用和中间件	Y.200 – Y.299
网络方面	Y.300 – Y.399
接口和协议	Y.400 – Y.499
编号、寻址和命名	Y.500 – Y.599
运营、管理和维护	Y.600 – Y.699
安全	Y.700 – Y.799
性能	Y.800 – Y.899
互联网的协议问题	
概要	Y.1000 – Y.1099
业务和应用	Y.1100 – Y.1199
体系、接入、网络能力和资源管理	Y.1200 – Y.1299
传输	Y.1300 – Y.1399
互通	Y.1400 – Y.1499
服务质量和网络性能	Y.1500 – Y.1599
信令	Y.1600 – Y.1699
运营、管理和维护	Y.1700 – Y.1799
计费	Y.1800 – Y.1899
下一代网络上的IPTV	Y.1900 – Y.1999
下一代网络	
 框架和功能性架构模型	Y.2000 – Y.2099
服务质量和性能	Y.2100 – Y.2199
业务方面：业务能力和业务架构	Y.2200 – Y.2249
业务方面：下一代网络中服务和网络的互操作性	Y.2250 – Y.2299
下一代网络的增强	Y.2300 – Y.2399
网络管理	Y.2400 – Y.2499
网络控制架构和协议	Y.2500 – Y.2599
基于分组的网络	Y.2600 – Y.2699
安全	Y.2700 – Y.2799
通用移动性	Y.2800 – Y.2899
运营商级开放环境	Y.2900 – Y.2999
未来网络	Y.3000 – Y.3499
云计算	Y.3500 – Y.3999

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2066建议书

物联网的共同要求

摘要

ITU-T Y.2066建议书提供了物联网（IoT）的共同要求。这些要求基于IoT和IoT主体的一般用例，在ITU-T Y.2060建议书给出的IoT的定义的基础上发展而来。IoT的共同要求不依赖于任何具体的应用领域，如交通应用领域和健康应用领域等某一具体经济、商业、社会或管理范围内的知识或活动。

本建议书以IoT的概述（ITU-T Y.2060建议书）为基础，根据IoT和IoT主体的一般用例以及从要求角度需要考虑的重要领域制定了共同要求。本建议书还提供了从应用领域选取的一些有代表性的IoT的用例。本建议书规定的IoT共同要求分为非功能性要求、应用支持要求、业务要求、通信要求、设备要求、数据管理要求以及安全和隐私保护要求等类别。

沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T Y.2066	2014-06-22	13	11.1002/1000/12169

关键词

共同要求、功能性要求、物联网（IoT）、非功能性要求、用例。

* 访问此建议书，请在您的Web浏览器地址栏中输入网址<http://handle.itu.int/>，后接建议书的唯一识别码。例如<http://handle.itu.int/11.1002/1000/11830-en>。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2019

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
3.1	他处定义的术语	1
3.2	本建议书中定义的术语	2
4	缩写词和首字母缩略语	2
5	惯例	3
6	IoT和IoT主体的一般用例.....	3
6.1	一般用例	3
6.2	IoT主体	5
7	从要求角度需要考虑的重要领域	6
7.1	实施和操作问题	6
7.2	无处不在的连接	6
7.3	端到端智能	6
7.4	时间同步	6
7.5	人体连接	6
7.6	来自物的大量数据	6
7.7	与物相关的隐私保护	6
8	IoT的共同要求.....	6
8.1	IoT的共同要求类别	7
8.2	非功能性要求	7
8.3	应用支持要求	8
8.4	服务要求	8
8.5	通信要求	10
8.6	设备要求	10
8.7	数据管理要求	11
8.8	安全和隐私保护要求	12
	附件A – IoT的共同要求清单	13
	附录I – IoT的代表性用例.....	17
I.1	视频监控	17
I.2	紧急告警	17
I.3	数据获取	17
I.4	遥控	17
I.5	不同应用领域之间的事件传送	17

I.6	跨不同应用领域的数据共享	18
I.7	智慧城市综合运营中心	18
I.8	一个详细的用例：交通事故信息收集	18
	参考书目	19

物联网的共同要求

1 范围

本建议书提供了物联网（IoT）的共同要求。这些要求基于IoT和IoT主体的一般用例，在[ITU-T Y.2060]建议书给出的IoT的定义的基础上发展而来。IoT的共同要求不依赖于任何具体的应用领域，如交通应用领域和健康应用领域等某一具体经济、商业、社会或管理范围内的知识或活动。

本建议书以IoT的概述[ITU-T Y.2060]为基础，根据IoT和IoT主体的一般用例以及从要求角度需要考虑的重要领域制定了共同要求。本建议书规定的IoT共同要求分为非功能性要求、应用支持要求、业务要求、通信要求、设备要求、数据管理要求以及安全和隐私保护要求等类别。

本建议书的范围包括：

- IoT的一般用例；
- IoT主体；
- 从要求角度需要考虑的重要领域；
- IoT的共同要求。

IoT的共同要求的摘要和编号见附件A。

附录I提供了从应用领域选取的一些有代表性的IoT用例。

注 – 监管、法律和商业问题不在本建议书的范围之内。协议和接口相关要求（例如IoT的控制和管理问题）也不在本建议书的范围之内。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T Y.2060] ITU-T Y.2060建议书（2012），物联网概述。

[ITU-T Y.2091] ITU-T Y.2091建议书（2011），下一代网络的术语和定义。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 应用 (application) [ITU-T Y.2091]: 一个结构化的能力集, 这些能力在一个或多个业务的支撑下提供增值功能, 它可以由API提供支撑。

3.1.2 消费者 (customer) [ITU-T Y.2091]: 消费者从企业购买或免费获得产品和服务。消费者可以是个人, 也可以是企业。

注1 – 每一个消费者中可能有多个用户。

3.1.3 设备 (device) [ITU-T Y.2060]: 在物联网中, 指具有强制性通信能力和选择性感知、激励、数据捕获、数据存储和数据处理能力的设备。

3.1.4 物联网 (Internet of Things) (IoT) [ITU-T Y.2060]: 信息社会的一种全球基础设施, 基于现有的和正在出现的、可互操作的信息和通信技术, 实现 (物理和虚拟) 之物的相互连接, 以提供先进的服务。

注1 – 通过使用识别、数据捕获、处理和通信能力, IoT充分利用物体向各种各样的应用提供服务, 同时确保满足安全和隐私要求。

注2 – 从广义而言, IoT可被视为具有技术和社会影响的一个愿景。

3.1.5 服务 (service) [ITU-T Y.2091]: 由提供商向用户提供的一系列功能与设施。

3.1.6 物 (thing) [ITU-T Y.2060]: 在物联网中, “物”指物理世界 (物理事物) 或信息世界 (虚拟事物) 中的一个对象, 它可被识别并整合进通信网络中。

3.2 本建议书中定义的术语

本建议书定义了下列术语:

3.2.1 应用领域 (application domain): 某一具体经济、商业、社会或管理范围内的知识或活动区域。

注 – 应用领域的示例包括交通应用领域、健康应用领域和政府应用领域。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语:

2G	第二代
3G	第三代
API	应用程序接口
CAN	控制器局域网
DSL	数字用户线
IoT	物联网
ITS	智能交通系统
LTE	长期演进
M2M	机器对机器
MOC	面向机器的通信
SDP	业务交付平台

SLA	业务水平协议
UML	统一建模语言
WiFi	无线保真

5 惯例

在本建议书中：

关键词“**须**”（**is required to**）指必须严格遵守的要求，如果宣称符合本文件，就不得违反。

关键词“**建议**”（**is recommended**）指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“**选择性的**”（**optionally**）和“**可能**”（**may**）指允许的选择性的要求、但并非建议遵守。该术语并非意在要求供应商实施该选项，网络运营商/服务提供商可选择性提供该功能。这意味着供应商可选择性地提供特性，并且仍然声称符合规范。

6 IoT和IoT主体的一般用例

本节描述了IoT和IoT主体的一般用例，以及一般用例和IoT主体之间的关系。本建议书规定的IoT主体指的是除IoT之外的、与IoT互动的实体。

6.1 一般用例

一般用例是在[ITU-T Y.2060]建议书给出的IoT的定义的基础上发展而来的。

根据[ITU-T Y.2060]给出的IoT的定义，IoT使“（通过物理和虚拟手段）将基于现有和正在出现的、可互操作信息和通信技术的东西相互连接实现高级服务”成为可能。这意味着IoT将物互联起来，以感知或激励它们，并提供高级服务，从而导出“IoT感知或激励”和“IoT服务提供”的一般用例。

根据[ITU-T Y.2060]给出的IoT的定义，“通过使用标识、数据捕获、处理和通信能力，IoT充分利用物体向各项应用提供服务，同时确保满足安全和隐私要求”。这意味着数据捕获和处理能力可与数据管理能力归为一组，并确保隐私保护，从而导出“IoT数据管理”和“IoT隐私保护”的一般用例。

图6-1展示了IoT一般用例模型，通过通用建模语言（UML）进行描述，更多信息见[b-UML]。这一模型由四个一般用例构成：IoT感知或激励、IoT数据管理、IoT服务提供和IoT隐私保护。

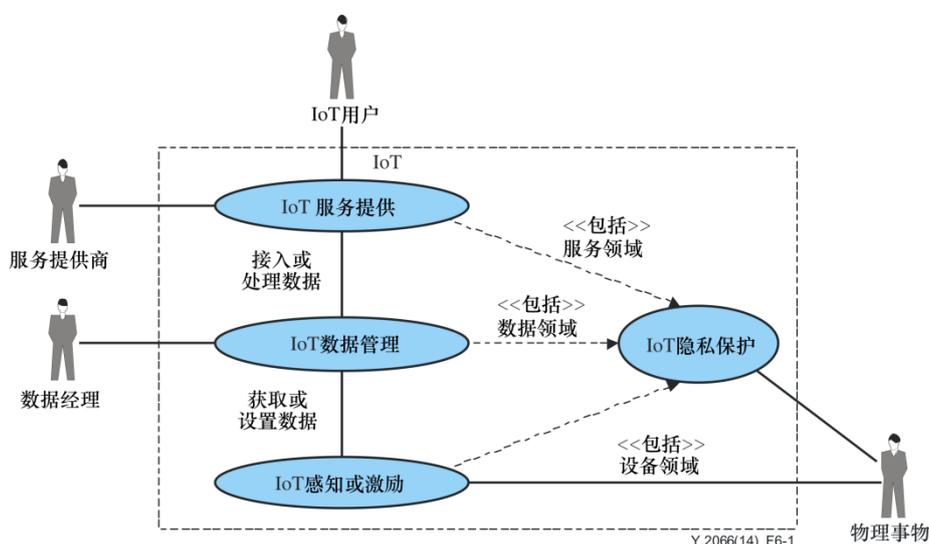


图6-1 – IoT一般用例模型

注1 – 在[b-UML]中，用例被定义为一个系统中有意义的工作的单独单元，可提供供系统外部实体观察的行为视图。用例可被用于捕获系统要求。用例模型（工作的各单独单元的组合）能够展示系统和系统外的实体之间的互动。在UML中，这些外部实体被称为“主体”。从这个角度来看，IoT变成正在由UML塑造的系统，而“IoT主体”成为IoT外的一个实体，并与IoT互动。

注2 – 一些取自IoT应用（代表性的用例见附录I的描述）的用例可被分解为第6.1.1到6.1.4条描述的一般用例，以协助生成与IoT主体对应的功能性要求。例如，附录I.1中描述的“视频监控”用例可被分解为视频捕获（IoT感知或激励）、视频传输和存储（IoT数据管理）和视频重放及分析（IoT服务提供）用例。这些用例可用于生成视频监控的不同主体的功能性要求，例如支持实时视频传输的时间同步，以及支持摄影机源源不断生成的大量视频的存储的虚拟存储。

6.1.1 “IoT感知或激励”用例

“IoT感知或激励”用例是一个可被应用于多个应用领域的一般用例。这一用例涉及与物理事物连接、感知物理事物的状态或激励物理事物的活动。

6.1.2 “IoT数据管理”用例

“IoT数据管理”用例是一个可被应用于多个应用领域的一般用例。这一用例涉及物理事物的数据的捕获、转移、存储和处理活动。

6.1.3 “IoT服务提供”用例

“IoT服务提供”用例是一个可被应用于多个应用领域的一般用例。这一用例涉及服务提供商提供服务 and IoT用户使用服务的活动。

6.1.4 “IoT隐私保护”用例

“IoT隐私保护”用例是一个可被应用于多个应用领域的一般用例。这一用例涉及保护和隐藏物理事物的隐私信息的活动。

6.1.5 一般用例之间的关系

图6-1展示了被标识的一般用例之间的关系。“IoT数据管理”用例与“IoT感知或激励”用例和“IoT服务提供”用例二者相关。“IoT隐私保护”用例与所有其他用例相关。

6.2 IoT主体

用例被用于捕获系统要求（见[b-UML]）。每个用例都包括用例中涉及的主体的功能性要求。

根据图6-1介绍的IoT一般用例模型，共有四个IoT主体：“物理事物”主体、“数据经理”主体、“服务提供商”主体和“IoT用户”主体。本条描述的这四个IoT主体都被定义为IoT之外的实体，并从要求的角度做出了规定。它们与[ITU-T Y.2060]建议书附录I描述的业务职能不同。业务职能是从业务角度做出的规定。

注1 – 本建议书中描述的“物理事物”主体对应[ITU-T Y.2060]建议书中描述的物理事物。根据IoT一般用例模型，本建议书不考虑对应[ITU-T Y.2060]建议书中描述的虚拟事物的主体，因为虚拟事物本身即为IoT的一个实体。

注2 – 以下提供了本建议书描述的IoT主体和[ITU-T Y.2060]建议书附录I描述的职能之间的适用映射：

- “IoT用户”主体对应应用客户职能。
- “服务提供商”主体对应应用提供商、平台提供商和网络提供商职能。
- “数据经理”主体对应应用提供商职能（在提供的应用涉及一些数据管理功能的情况下），也可能对应设备提供商职能（在提供的设备涉及一些数据管理功能的情况下）。

6.2.1 “物理事物”主体

“物理事物”主体是一个在物理世界拥有独特标识符的IoT主体。“物理事物”通过感知或激励活动与IoT互动。

注 – “物理事物”主体可进一步例化为“人造事物”和“自然事物”。人造事物是由人类生产，并能够被产品序列号识别的物理事物。自然事物是在自然中生成，并能够通过生成时间、位置及其种类等被识别的物理事物。感知自然事物是IoT发展面临的挑战。

要注意，在本建议书的以下条款中，“物”一词指的是“物理事物”。

6.2.2 “数据经理”主体

“数据经理”主体是负责管理捕获、存储、传送和处理IoT数据，以满足IoT服务提供需求的IoT主体。

注 – “数据经理”可进一步例化为人类“数据经理”和机器“数据管理器”主体。人类“数据经理”主体手动进行IoT数据管理，而机器“数据管理器”以自动方式执行这一功能。这两个“数据经理”主体的实例与IoT数据管理的不同用例相关。

6.2.3 “服务提供商”主体

“服务提供商”主体是提供与物相关的所有可能的服务（例如监控、位置跟踪和服务发现等）的IoT主体。

注 – “服务提供商”主体可进一步例化为提供不依赖于特定应用领域服务的通用“服务提供商”和提供基于特定应用领域应用的应用“服务提供商”。

6.2.4 “IoT用户”主体

“IoT用户”主体是使用与物相关的所有可能的服务（例如监控、位置跟踪和服务发现等）的IoT主体。

7 从要求角度需要考虑的重要领域

对于IoT要求的规格，有若干重要领域需要关注。基于[ITU-T Y.2060]建议书中包含的IoT特性和高层要求，以及IoT相关的公共和学术研究结果（例如[b-IoT-A D6.2]），以下条款描述了从要求角度需要考虑的重要领域。

7.1 实施和操作问题

IoT的实施和操作问题是需要应对的重要领域，例如，要实现异构IoT实施之间的互操作性，获得用于支持大量互联互通设备的足够的可扩展性，以及用于支持IoT中的自动操作的高可用性。

7.2 无处不在的连接

为实现物与IoT之间的互联互通，必须考虑无处不在的连接。连接能力需要独立于特定应用领域，并支持异构通信技术之间的集成。

7.3 端到端智能

需要考虑端到端智能，尤其是关于“通信智能”和“服务智能”，例如，在无人类干预的情况下提供服务。这包括思考基于位置的通信和基于情境的通信（可被视为智能通信）、内容感知服务和情境感知服务（可被视为智能服务），以及自配置、自修复、自优化和自我保护服务（可被视为另一种智能服务，整体被称为自主服务（[ITU-T Y.2060]建议书））。

7.4 时间同步

在使用通信和服务能力时，为保持互联物之间行动的时间同步性，需要考虑时间同步。

7.5 人体连接

为在法律法规范围内提供与人体相关的通信能力，必须仔细考虑人体连接的要求。需要规定特殊服务质量（QoS），量化可靠性，并保护隐私。

7.6 来自物的大量数据

由于将有大量设备与IoT互联，将会产生大量从物向IoT传输的数据 – “大数据”一词被专门用于表示数据的大容量、多种类和高速度。为了在IoT用户或应用要求的时间内对大数据进行分类、传输、存储、处理、验证和查询，应考虑到通信带宽、存储和处理能力等资源可扩展性。

7.7 与物相关的隐私保护

来自物的数据可能包含与物的所有者或用户相关的隐私信息。数据可被用于定位或跟踪物的所有者或用户，侵犯他们的隐私。在捕获、传送、存储、验证和处理来自物的数据的过程中，应考虑隐私保护。隐私保护不得被用于阻碍对来自物的数据的验证。

8 IoT的共同要求

本建议书规定的IoT的共同要求为技术要求，不依赖于任何具体的应用领域。协议和接口相关的要求（例如，IoT的控制和管理问题）不在本建议书的范围之内。

8.1 IoT的共同要求类别

在本建议书中，IoT的共同要求被分为非功能性要求和功能性要求。

IoT非功能性要求指与IoT本身的实施和操作相关的要求。

IoT功能性要求指与IoT主体（例如，IoT外部与IoT互动的实体）相关的要求。本建议书规定的IoT功能性要求进行如下分类：

- 应用支持要求；
- 服务要求；
- 通信要求；
- 设备要求；
- 数据管理要求；
- 安全和隐私保护要求。

附件A列出了以下条款描述的全部要求并已编号。在以下条款中，每个描述相应要求的段落的末尾均插入了方括号“[]”，方括号内为附件A所示的要求的编号。

8.2 非功能性要求

此类别的要求与任何IoT主体无关，因为这些要求并非从第6条描述的IoT一般用例导出。

8.2.1 互操作性

需要确保异构IoT实施之间的互操作性[N1]。

注 – 为支持IoT的互操作性，需要标准化IoT的架构参考模型。

8.2.2 可扩展性

需要确保IoT支持扩展性，以应对大量设备、应用和用户[N2]。

注1 – 处理大量设备的可扩展性要求意味着处理IoT中大量数据（大数据）的要求。

注2 – 处理大量应用和用户的可扩展性要求意味着要求具备大量处理和存储资源。可通过在IoT中整合云计算技术来支持这一要求。

注3 – 应考虑在处理大量设备、应用和用户时的公平性。

8.2.3 可靠性

IoT能力的可靠性（例如IoT通信、服务和数据管理能力）是必需的[N3]。

注 – 应考虑用于支持可靠性的恢复能力。

8.2.4 高可用性

IoT的服务提供、数据管理、通信、物的感知和激励需要高可用性[N4]。

8.2.5 适应性

需要IoT对未来兴起的新兴信息技术的适应性[N5]。

注 – IoT使用的技术标准应对新技术的适应性造成最小限制。

8.2.6 可管理性

IoT应支持可管理性，以确保正常操作。IoT操作通常可自动执行，无需人员干预，但操作过程应可管理[N6]。

注1 – 应考虑IoT的设备管理，例如设备状态管理、设备连接管理、功耗管理等。设备管理应考虑设备资源的限制，例如能源、内存和带宽。

注2 – 应考虑IoT的自动故障管理，例如主动故障申报、故障诊断、故障恢复等。

注3 – 应考虑IoT的自动配置管理，例如设备参数的自动配置。

8.3 应用支持要求

应用支持要求指开发不同应用领域的IoT应用的功能性要求。这些要求仅与“服务提供商”主体相关。

8.3.1 可编程接口

需要标准化的可编程接口，以提供对于应用支持能力的开放接入[A1]。

注 – 可编程接口允许以可编程方式支持IoT。

8.3.2 组管理

IoT需要支持组管理，包括IoT组的显示、创建、修改、删除和IoT组成员的显示、添加、修改和删除[A2]。

注 – IoT组可包含IoT用户和/或者设备。

8.3.3 时间同步

需要可靠的时间同步，以在IoT中支持全球时戳[A3]。

注 – 时戳允许安全可信的时间关键型服务的提供。

8.3.4 协作

目的相同的接入IoT应用的服务或设备之间需要协作，以便IoT能够启动此类服务或设备之间的自主目标驱动协作[A4]。

注 – 接入IoT应用的设备之间的协作需要由设备本身激活，以便IoT能够通过此类设备中的分布式控制支持可扩展协作。

8.3.5 用户管理

需要用户管理，包括IoT用户的创建、认证、授权和计费[A5]。

8.3.6 资源使用结算

需要按照每个应用的情况进行IoT资源使用情况计费[A6]。

8.4 服务要求

这些要求与服务提供商、IoT用户和物主体相关。

注 – 根据“服务”的一般定义，即提供商向用户提供的一系列功能和设施[ITU-T Y.2091]，服务要求与IoT用户和服务提供商主体均有关系。不排除直接向物主体提供服务的情况。

8.4.1 服务优先级

需要服务优先级，以满足IoT用户不同组的不同服务要求[S1]。

注 – 需要支持差异化服务，以便IoT能够提供不同的服务水平协议（SLA）。

8.4.2 基于句法的服务

IoT需要基于句法的服务，以支持自动服务提供。实施基于句法的服务的机制包括服务句法标注、服务句法接入和服务间的句法交换[S2]。

注 – 服务句法标注能够允许服务的句法描述。服务句法接入可被用于通过句法接口接入服务。服务间的句法交换可启用服务间的句法提供和交流，以支持自动创建新服务。

8.4.3 服务组合

需要服务组合以支持在IoT中创建灵活的服务[S3]。

注1 – 初级服务是一系列无法直接满足IoT应用的某些要求的基本操作。服务组合是其中一种服务创建方式，可基于初级服务自动创建更加复杂的服务，以满足IoT应用的所有多样化要求。

注2 – 现有的灵活服务提供技术，例如服务提供平台（SDP）等，能够支持服务组合的要求。

8.4.4 移动性服务

需要移动性服务，从而使IoT能够从服务提供的角度支持服务移动性、用户移动性和设备移动性，例如，当支持服务移动性时，服务提供不受服务接入位置的约束[S4]。

8.4.5 可靠和安全的人体连接服务

在提供人体连接服务时，需要保障高可靠性和安全性[S5]。

注 – 不同国家对于这些服务可能有不同的法律和法规要求。

8.4.6 自主服务

需要自主服务，从而使IoT能够基于服务提供商配置的或IoT用户定制的规则自主捕获、通信和处理物数据[S6]。

注 – 需要支持自主服务的集中和分散控制，从而使IoT能够启用集中或分散的自动化活动。

需要基于位置的和情境感知服务，从而使IoT能够基于位置信息以及物和/或者用户的相关情境启动灵活、用户定制和自主服务[S7]。

8.4.7 服务管理

需要服务管理，以便能够以高可用性和高可靠性的方式支持服务提供[S8]。

注 – 服务管理包括服务生命周期管理和服务完整性检测等。服务生命周期管理有助于提高服务可用性，服务完整性检测有助于提高服务可靠性。

8.4.8 发现服务

需要发现服务，从而使IoT用户、服务、设备和物数据能够被服务提供商或者IoT用户发现[S9]。

注 – 服务提供商或IoT用户可根据不同标准，例如地理位置信息、设备类型等发现特定IoT用户、服务、设备和物数据。

8.4.9 服务订阅支持

需要服务订阅支持，从而使IoT能够提供允许IoT用户订阅所需服务和相关的物数据的方式[S10]。

8.4.10 命名和寻址

需要标准化的物和服务的命名和寻址[S11]。

8.4.11 虚拟存储和处理

需要虚拟存储和处理能力，以便存储和处理大量数据（大数据）[S12]。

8.5 通信要求

通信要求指与IoT用户、服务供应商、数据经理和物主体之间的信息交换相关的功能性要求。这些要求与所有IoT主体相关。

8.5.1 通信模式

需要支持设备之间或IoT用户之间的基于事件的定期和自动通信模式[C1]。

需要支持单播通信模式（例如，IoT用户或设备之间的通信）。需要支持组播、广播和任播通信模式，从而使IoT能够在一组IoT用户或设备内部提供各类通信服务（例如，支持IoT用户或设备之间的协作）[C2]。

注 – 建议支持设备之间或IoT用户之间的基于事件的定期自动通信模式，同时在避免业务流量拥挤的可能性的机制支持下，维持网络性能。

需要支持设备发起的通信，以满足自动通信的需要[C3]。

8.5.2 通信控制

需要支持通信差错控制，从而使IoT能够，例如，应对设备间的干扰[C4]。

需要支持关键时间通信，从而使IoT能够处理和交付关键时间信息[C5]。

8.5.3 智能通信

智能通信的要求包括自动网络化[ITU-T Y.2060]、内容感知通信和基于位置的通信的要求。

IoT需要自动网络化，以支持网络化层面的自我配置、自愈、自优化和自我保护能力，从而适应不同的应用域、不同的通信环境和大量不同类型的设备[C6]。

需要内容感知通信，从而，例如，使IoT能够基于内容进行路径选择和通信路由[C7]。

需要基于位置的通信，从而使IoT能够支持IoT主体之间基于位置的互动[C8]。

注 – 需要自动捕获和追踪位置信息。

8.5.4 异构通信支持

在设备层（见[ITU-T Y.2060]），通信可通过各类有线或无线技术，例如控制器局域网（CAN）总线、无线个域网（ZigBee）、蓝牙、WiFi等技术进行。需要支持异构设备相关的通信技术[C9]。

在网络层（见[ITU-T Y.2060]），通信可通过各种技术，例如第二代或第三代（2G或3G）网络、长期演进（LTE）、以太网、或数字用户线路（DSL）等进行。

需要支持异构网络相关通信技术[C10]。

8.6 设备要求

设备要求指对于与物相连的设备的功能性要求。这些要求与IoT用户和物主体相关。

8.6.1 物连接

IoT需要支持在物标识符的基础上建立物与IoT之间的连接[D1]。

注 – 需要以统一方式处理物的异构标识符（见[ITU-T Y.2060]）。

8.6.2 设备控制和配置

需要支持设备远程监测、控制和配置，从而提高IoT的设备可管理性[D2]。

IoT需支持即插即用功能，以支持即时生成、构成或获取基于句法的配置，从而将物与应用无缝集成和合作，对应用要求做出响应（见[ITU-T Y.2060]）[D3]。

8.6.3 物监测

需要自动通知物状态及其变更，以便及时监测物[D4]。

8.6.4 设备移动性

需要设备移动性，从而使IoT能够支持与设备相连接的物的移动性[D5]。

8.6.5 设备完整性检测

需要设备完整性检测，以帮助支持设备的高可用性[D6]。

8.7 数据管理要求

数据管理要求指IoT数据的存储、集总、传送和处理等功能性要求。这些要求与数据经理和IoT用户主体相关。

8.7.1 数据存储

需要支持基于预定义的规则和策略的物数据存储[DM1]。

8.7.2 数据处理

需要支持基于预定义的规则和策略的数据融合和采集[DM2]。

8.7.3 数据查询

需要支持查询存储的物的历史数据，从而使IoT能够提供关于物的历史信息[DM3]。

8.7.4 数据访问控制

IoT需要支持其所有者对数据的访问控制，以便IoT用户能够控制他们的数据如何向其他IoT用户公开[DM4]。

8.7.5 数据交换

需要支持与IoT外的实体的数据交换，从而使IoT能够提供对外部数据资源的访问，例如IoT外的健康数据库[DM5]。

8.7.6 数据验证

需要支持物数据的完整性检测和生命周期管理，从而使IoT能够提供物数据的高可用性和可靠性[DM6]。

8.7.7 句法注释和物数据访问

需要物数据的句法注释。需要句法访问物数据，从而支持物的自动查询[DM7]。

8.7.8 物数据的句法存储、传送和集总

需要物数据的句法存储、传送和集总，从而使物数据的句法存储、传送和集总能够根据IoT用户或应用的要求自动执行[DM8]。

8.8 安全和隐私保护要求

安全和隐私保护要求是指在捕获、存储、传送、集总和处理物数据以及提供涉及物的服务期间的功能性要求。这些要求与IoT的所有主体有关。

8.8.1 通信安全

需要安全、可信和隐私保护的通信能力，以禁止对数据进行未经授权的访问，保证数据的完整性，并在IoT中传输或传送数据期间可以保护与隐私相关的数据内容[SP1]。

8.8.2 数据管理安全

需要安全、可信和隐私保护的数据管理能力，以禁止对数据进行未经授权的访问，保证数据的完整性，并在IoT中存储或处理数据时可以保护与隐私相关的数据内容[SP2]。

8.8.3 服务提供安全

需要安全、可信和隐私保护的服务提供能力，以禁止未经授权的服务访问和欺诈性的服务提供，并可以保护与IoT用户相关的隐私信息[SP3]。

8.8.4 安全策略和技术的整合

需要整合不同安全策略和技术的能力，以确保对IoT中各种设备和用户网络执行一致的安全控制[SP4]。

8.8.5 相互认证和授权

在设备（或IoT用户）可以接入IoT之前，需要根据预定义的安全策略执行设备（或IoT用户）与IoT之间的相互认证和授权[SP5]。

8.8.6 安全审计

IoT需要支持安全审计。任何数据访问或企图接入IoT应用都需要根据适当的法律法规使之完全透明、可追溯和可重现。特别地，IoT需要支持有关数据传输、存储、处理和应用访问的安全审计[SP6]。

附件A

IoT的共同要求清单

(此附件为本建议书不可分割的组成部分。)

下表列出了第8条“IoT的共同要求”中描述的要求，并编号。

要求编号	要求种类	要求描述	要求摘要	
N1	非功能性	需要确保异构IoT实施之间的互操作性。	需要互操作性。	
N2	非功能性	IoT需要支持可扩展性，以处理大量设备、应用和用户。	需要可扩展性。	
N3	非功能性	需要IoT能力（例如IoT通信、服务和数据管理能力）的可靠性。	需要可靠性。	
N4	非功能性	IoT需要在服务提供、数据管理、通信、物的感知和激励中提供高可用性。	需要高可用性。	
N5	非功能性	IoT需要适应未来出现的新技术。	需要适应性。	
N6	非功能性	IoT应支持可管理性，以确保正常操作。	需要可管理性。	
A1	应用支持	需要标准化的可编程接口，以为应用支持能力提供开放接入。	需要标准化的可编程接口。	
A2	应用支持	IoT需要支持组管理，包括IoT组的显示、创建、修改、删除和IoT组成员的显示、添加、修改和删除。	需要组管理。	
A3	应用支持	需要可靠的时间同步，以在IoT中支持全球时戳。	需要可靠的时间同步。	
A4	应用支持	需要在服务之间或具有相同目标的设备之间进行协作，以访问IoT应用程序。	需要协作。	
A5	应用支持	需要用户管理，包括IoT用户的创建、认证、授权和计费。	需要用户管理。	
A6	应用支持	需要按照每个应用的情况进行IoT资源使用情况计费。	需要资源使用情况计费。	
S1	服务	需要服务优先级，以满足IoT用户不同组的不同服务要求。	需要服务优先级。	
S2	服务	IoT需要基于句法的服务，以支持自主服务提供。	需要基于句法的服务。	

要求编号	要求种类	要求描述	要求摘要	
S3	服务	需要服务组合以支持在IoT中创建灵活的服务。	需要服务组合。	
S4	服务	需要移动性服务，从而使IoT能够支持服务移动性、用户移动性和设备移动性	需要移动性服务。	
S5	服务	在提供人体连接服务时，需要高可靠性和安全性。	需要高可靠和安全的人体连接服务。	
S6	服务	需要自动服务，从而使IoT能够基于服务提供商配置的或IoT用户定制的规则自动捕获、通信和处理物数据。	需要自动服务。	
S7	服务	需要基于位置的和情境感知服务，从而使IoT能够基于位置信息以及物和/或者用户的相关情境启动灵活、用户定制和自主服务。	需要基于位置的和情境感知服务。	
S8	服务	需要服务管理，以便以高可用性和高可靠性的方式支持服务提供。	需要服务管理。	
S9	服务	需要发现服务，从而使IoT用户、服务、设备和物数据能够被服务提供商或者IoT用户发现。	需要发现服务。	
S10	服务	需要服务订阅支持，从而使IoT能够提供允许IoT用户订阅所需服务和相关的物数据的方式。	需要服务订阅支持。	
S11	服务	需要标准化的物和服务的命名和寻址。	需要标准化的命名和寻址。	
S12	服务	需要虚拟存储和处理能力，以便存储和处理大量数据（大数据）。	需要虚拟存储和处理能力。	
C1	通信	IoT需要支持设备之间或IoT用户之间的基于事件的定期和自动通信模式。	需要支持基于事件的定期和自动通信模式。	
C2	通信	需要支持单播通信模式（例如，IoT用户或设备之间的通信）。需要支持组播、广播和任播通信模式，从而使IoT能够在—组IoT用户或设备内部提供各类通信服务（例如，支持IoT用户或设备间的协作）。	需要支持单播、组播、广播和任播通信模式。	

要求编号	要求种类	要求描述	要求摘要	
C3	通信	需要支持设备发起的通信，以满足自动通信的需要。	需要支持设备发起的通信。	
C4	通信	需要支持通信差错控制，从而使IoT能够，例如，解决设备间的干扰。	需要支持通信差错控制。	
C5	通信	需要支持关键时间通信，从而使IoT能够处理和交付关键时间信息。	需要支持关键时间通信。	
C6	通信	IoT需要网络化层面的自我配置、自愈、自优化和自我保护能力。	需要自动网络化。	
C7	通信	需要内容感知通信，从而，例如，使IoT能够基于内容进行路径选择/和通信路由。	需要内容感知通信。	
C8	通信	IoT需要支持IoT主体之间基于位置的互动。	需要基于位置的通信。	
C9	通信	在设备层（见[ITU-T Y.2060]），通信可通过各类有线或无线技术，例如控制器局域网（CAN）总线、无线个域网（ZigBee）、蓝牙、WiFi等技术进行。	需要支持异构设备相关的通信技术。	
C10	通信	在网络层（见[ITU-T Y.2060]），通信可通过各种技术，例如第二代或第三代（2G或3G）网络、长期演进（LTE）、以太网、或数字用户线路（DSL）等进行。	需要支持异构网络相关的通信技术。	
D1	设备	IoT需要支持基于事物的标识符在物和IoT之间建立连接。	需要物与IoT之间基于标识符的连接。	
D2	设备	需要支持设备的远程监测、控制和配置，从而提高IoT设备的可管理性。	需要设备的远程监测、控制和配置。	
D3	设备	IoT需支持即插即用功能，以支持即时的基于句法的设备配置。	需要即插即用能力。	
D4	设备	需要自动通知物状态及其变更，从而及时监测物。	需要对物的即时监测。	
D5	设备	IoT需要支持物的移动性。	需要设备移动性。	
D6	设备	需要设备完整性检测，以支持设备的高可用性。	需要设备完整性监测。	

要求编号	要求种类	要求描述	要求摘要	
DM1	数据管理	IoT需要支持基于预定义的规则和策略的物数据存储。	需要支持物数据存储。	
DM2	数据管理	需要支持基于预定义的规则和策略的数据融合和采集。	需要支持物数据处理。	
DM3	数据管理	IoT需要提供关于物的历史信息。	需要支持查询物的历史信息。	
DM4	数据管理	IoT需要支持数据所有者对数据的访问控制，从而使IoT用户能够控制如何将他们的数据暴露给其他IoT用户。	需要数据所有者的数据访问控制。	
DM5	数据管理	需要提供对外部数据资源的访问，例如，IoT外的健康数据库。	需要支持与IoT外的实体的数据交换。	
DM6	数据管理	IoT需要提供物数据的完整性检测和生命周期管理，从而使IoT能够提供物数据的高可用性和可靠性。	需要物数据的完整性检测和生命周期管理。	
DM7	数据管理	需要物数据的句法注释。需要句法访问物数据，从而支持物的自动查询。	需要句法注释和句法访问物数据。	
DM8	数据管理	物数据的存储、传送和集总需要根据IoT用户或应用的要求自动执行。	需要物数据的句法存储、传送和集总。	
SP1	安全和隐私保护	IoT需要支持安全、可信和隐私保护的通信能力。	需要通信安全。	
SP2	安全和隐私保护	IoT需要提供安全、可信和隐私保护的数据管理能力。	需要数据管理安全。	
SP3	安全和隐私保护	IoT需要提供安全、可信和隐私保护的服务提供能力。	需要服务提供安全。	
SP4	安全和隐私保护	IoT需要整合与各类设备和用户网络相关的不同安全策略和技术。	需要整合不同安全策略和技术。	
SP5	安全和隐私保护	在设备（或IoT用户）可以接入物IoT之前，需要根据预定义的安全策略执行相互认证和授权。	需要相互认证和授权。	
SP6	安全和隐私保护	任何数据接入或企图接入IoT的应用都需要根据适当的法律法规使之完全透明、可追溯和可重现。	IoT需要支持安全审计。	

附录I

IoT的代表性用例

(本附录非本建议书不可分割的组成部分。)

本附录描述了一些具有代表性的IoT用例，基于应用领域内或跨多个应用领域的用例选取和分类。

I.1 视频监控

视频监控是典型的存在于大量IoT应用中的用例类型。例如，在智慧城市应用中，出于保护城市安全的目的，视频监控被用于观察人们的行动。在污染监管中，视频监控被用于观察工厂是否排出污水。医院使用视频监控来远程观察病人状态。

视频监控通常需要大量资源，例如用于传送视频的高通信带宽、用于保存视频副本的大量存储资源和用于搜索和处理视频的强大的处理器。

I.2 紧急告警

紧急告警选取自大量用例，例如患者心脏病发作时的求救信息传输，车辆无法正常行驶之前或之后、发生交通事故时的告警信息传输，以及在血压超过阈值时的告警信息传输。

这类用例需要高优先级和可靠的数据传输、最小的时延，还需要设备具有发起通信的能力。

I.3 数据获取

此类用例数量繁多，例如燃气计量、用水计量和质量监测、电量计量、公共汽车票终端数据上传等等。在这些用例中，每隔一定时间发生一次数据通信。

这些用例要求定期数据传输机制。传输任务可根据给定策略自动激活。通常，在大多数案例中，数据传输的吞吐量很低。

I.4 遥控

此类用例包括大量应用领域中的用例，例如家庭自动化、制造和智能交通系统（ITS）。在这些用例中，IoT应用需要用户远程控制设备的能力。

对于这类用例来说，用于远程控制设备的数据通信非连续，并且不一定每隔一定的时间发生。这些用例需要一些机制来建立控制器和由控制器或设备启动的远程设备之间的连接，只有在需要数据传输时才需要。

I.5 不同应用领域之间的事件传送

在许多IoT应用（例如智慧城市和应急管理应用）中，在一个应用领域发生的事件会被传送到其他相关应用领域。在被传送到不同应用领域的事件的基础上，不同应用可协作工作，以提供比仅限于单独领域的应用更多的功能和服务。此类用例的例子包括道路和桥梁维护应用之间的事件传送，交通管理和驾驶应用之间的事件传送，以及天气预报和洪灾防范应用之间的事件传送等。

此类应用案例需要事件以标准化的格式进行描述，从而使不同的IoT应用能够理解内容。此外，事件需要被可靠、安全地传送。

I.6 跨不同应用领域的共享

一些数据不仅在收集这些数据的IoT应用中十分重要，在其他IoT应用中亦非常重要。此类数据包括地理位置数据、道路交通流量数据等。根据相关法律法规，数据可在不同应用领域之间共享，以提供更多功能和服务。例如，移动电话的与地理位置相关的数据可被应用于计算道路交通流量。

此类用例需要不同IoT应用领域之间的标准化的数据格式，从而使数据能够在不同应用领域之间共享。

I.7 智慧城市综合运营中心

基于IoT基础设施开发的智慧城市现在已成为全世界城市开发的新潮流。未来，城市需要具备智能“大脑”系统，以分析由IoT设备收集的不同类型的数据，并在所做的研究以及其他相关行动的基础上做出行动。此类城市大脑系统可被称为“智慧城市综合运行中心”。

这一综合运营中心基本需要跨多个应用领域的共享、集总和处理。例如，此类综合运营中心的实施通常需要整合城市实时运行状态信息与事件监控、数据分析、早期智能警报和信息传播、智慧决策和集成的命令与分派。

I.8 一个详细的用例：交通事故信息收集

直接涉及或路过一场事故的车辆中的ITS电台（ITS-S）探测到发生了一起车祸，自动启动事故报告处理流程。设备会尝试连接至IoT，之后向其发送事故报告。IoT收到并核实事故报告，并将分析结果推送至服务订户，例如警察局和急救中心。

服务订户可要求IoT收集更多关于事故的信息。IoT收到这些服务请求之后，会根据订户的请求，让ITS-S收集更多信息。事故地点附近的ITS-S接收、核实、解析并执行收到的命令，例如拍照、获取当前行进状态、生成报告、签署报告并上传署名报告至IoT。IoT累积并核实由ITS-S上传的报告，之后生成急救中心需要的包含关于事故现场的视觉信息的报告和关于车祸现场附近交通情况的报告。这些报告被分别再次推送给急救中心和警察局。

急救中心分析关于事故现场的报告，之后制定具体的救援方案。警察局分析关于交通状况的报告，制定具体的交通管制方案。

这一用例需要设备具有发起通信的能力，具有安全、可信的通信能力和不同应用间的事件驱动的协作。

参考书目

- [b-ITU-T Y.2061] ITU-T Y.2061建议书（2012），下一代网络（NGN）环境下支持面向机器的通信（MOC）应用的要求。
- [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*:
http://www.iso.org/iso/catalogue_detail.htm?csnumber=52854

ITU-T建议书系列

系列A	ITU-T工作的组织
系列D	通用资费原则
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	终端和主观及客观评估方法
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	数据网、开放系统通信和安全性
系列Y	Y系列：全球信息基础设施、互联网的协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题