**ISO/IEC JTC 1/WG 10**
**Internet of Things**
**Convenorship: KATS (Korea, Republic of)**

| | |
|---|---|
| **Document type:** | Working Draft Text |
| **Title:** | WD of ISO/IEC 30141, Information technology — Internet of Things Reference Architecture (IoT RA) |
| **Status:** | As per the ISO/IEC JTC 1/WG 10 Ottawa Recommendation 39, this WD is circulated to WG 10 members and its liaison organizations for comments using the ISO commenting template. |
| **Date of document:** | 2015-10-10 |
| **Source:** | Project Editors |
| **Expected action:** | COMM |
| **Action due date:** | 2015-12-18 |
| **No. of pages:** | 107 |
| **Email of secretary:** | |
| **Committee URL:** | http://isotc.iso.org/livelink/livelink/open/jtc1wg10 |

**ISO/IEC 30141:####(X)**

ISO/IEC JTC 1/WG 10

Secretariat: KSA

# Information technology — Internet of Things Reference Architecture (IoT RA)

# WD stage

**Warning for WDs and CDs**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland.

# Contents



 

 

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1/WG 10.

ADD INFORMATION ABOUT REPLACED STANDARDS AND OTHER PARTS AS NECESSARY

# Introduction

**Editors' Note** from the comments received on "Introduction" section: The paragraphs in this introduction clause will be revised as the contents of this document is stabilized.

Internet of Things (IoT) has been studied for many years, and it has been gaining more momentum over the last few years as system development and implementation for various applications and services have been adopting and adapting IoT technology. Then, the IoT is an enabling technology, and it is not a system or system of systems by itself, and it consist of many other supporting technologies, for example, many different type of communication and data network technology, networking technology, information technology, sensing and control technologies, software technology, device/hardware technology, and so on. The IoT technology can be used for developing and implementing a system of systems applications and services, resulting in IoT-based or -applied systems (hereafter "IoT Systems") which include, but not limited to, smart city, smart grid, smart home/building, smart factory, digital agriculture, manufacturing, intelligent transportation and traffic, logistics and asset/inventory management, retail transactions, e-Health, public safety, e-Learning, environment monitoring. These applications and services are built upon primarily interconnecting smart objects and essential supporting objects such as actuators, middleware, data and communication networks, various software/algorithms and data composing IoT services. The smartness in IoT comes from various aspects and levels: (1) device level (e.g., sensing and actuating devices with smart algorithms); (2) middleware level which has various types of embedded smart and supporting functions; (3) application software level which provides various types of services using various types of software (e.g., data mining, data fusion, etc.); and (4) network level where data/information exchanges and other interactions (e.g., command and control, etc.) occur among complex interconnectedness of devices, middleware functions, and application software.

**Editors' Note** from the comments received on "physical and virtual objects" in the paragraph below: The contributions for the definitions of "thing," "physical object," and "virtual object" are requested from the WG 10 experts in Clause 4 "Terms and Definitions" section.

In designing and developing IoT Systems, three main aspects and technologies should be considered: (1) physical aspect and technology; (2) communications aspect and technology; and (3) data/information aspect and technology. In a different perspective, IoT Systems are composed of physical objects and virtual objects where both objects together mean "things" in "Internet of Things." The physical and virtual objects together collect, process, extract, and/or exchange data/information. They also can decide, and/or act/react to environments autonomously or upon user's request. The data and information generated by IoT Systems are likely sensitive in nature; yet, data and information exchange is an essential and imperative process of IoT Systems that provide various applications and services. Therefore, data/information security and user privacy is the other major technology area of importance to be considered for by the developer of IoT Systems. Security and privacy in IoT Systems are also associated and dictated by international and national legislations, and IoT Systems should comply with the local security/privacy laws. Additionally, reliability, dependability, and data validation and associated requirements are the other areas that the developers of IoT Systems should consider.

In this IoT RA International Standard (IS), the IoT RA is described from the aforementioned three main technology areas in this international standard (IS):

— IoT Systems Reference Architecture (SRA): Describes the IoT Systems from system perspective

 

- IoT Communications Reference Architecture (CRA): Describes the IoT Systems from communication technology perspective

- IoT Information Reference Architecture (IRA): Describes the IoT Systems from information technology perspective

- The architecture entities defined in the SRA, CRA, and IRA are coincident and related across these three IoT reference architectures. Describing the IoT RA using the three different perspectives will benefit not only the IoT standard developers but also the IoT Systems developers. For example, developing IoT Security Architecture or implementing IoT security, the developers can do their work in accordance to the three perspectives describing physical security, communication security, and information security. Other requirements can also be described from these three architecture perspectives.

The ISO/IEC 30141 of International Standard (IS) are to:

- provide guidance to facilitate the design and development of IoT Systems,

- promote open and common guiding architecture leading to seamless interoperability of IoT Systems, and

- make IoT Systems' components plug-and-play, so that it becomes easy to add/remove IoT Systems components to/from the IoT Systems.

 

# Information technology — Internet of Things Reference Architecture (IoT RA)

## 1 Scope

This International Standard specifies IoT conceptual ~~reference~~ model and reference architecture from different architectural views, common entities, and interfaces between IoT domains.

**Editors' Note**: The "conceptual model" is being deleted from the original NWIP scope, but "conceptual model" is expected be described the "conceptual reference model" clause whose text will be recommended by SRG 5.

**Editor's Note**: The scope should be modified since the "conceptual reference model" is changed into "conceptual model" in WG10 meeting in Ottawa, and it should be discussed in next WG10 meeting.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO #####-#:20##, *General title — Part #: Title of part*

**Editors' Note**: Any document that is vital to understand this IS will be added as normative references.

## 3 Terms and definitions

**3.1**
**actuator**
An Actuator is a Component which conveys digital information to effect a change of some property of a physical entity [IoT-A]++

**Editor's Note:** This term and definition was deleted from Clause 3 in the Ottawa meeting, but added from the SRG 5 CM Contribution. The original definition in Clause 3 for actuator which was deleted in the Ottawa meeting: "device that provides a physical output in response to an input signal in predetermined way."

**3.2**
**architecture framework**
conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders

[SOURCE: ISO/IEC 42010:2011]

**3.3**
**architecture view**
work product expressing the architecture of a system from the perspective of specific system concerns

[SOURCE: ISO/IEC 42010:2011]

 

**3.4**
**characteristics**
a distinctive mark, trait, or feature that may serve for identification; a distinguishing or essential peculiarity or quality

[Source: Oxford English Dictionary Online]

**3.5**
**component**
modular, deployable, and replaceable part of a system that encapsulates implementation and exposes a set of interfaces

[SOURCE: ISO/TS 19104:2008]

A modular, deployable, and replaceable part of a system that encapsulates implementations [ISO/TS 19104:2008 ++]

Note 1 to entry: a component may expose or use interfaces (local or on a network) to interact with other entities. A Component which exposes or uses network interfaces is called an Endpoint.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.6**
**concept**
text of the definition

Action item – Use OED definition? – Contribution from WG 10 experts requested on the use of OED definition for this term. Provide the contribution as (1) Use of OED definition is sufficient for this IS; or (2) Use of OED definition is not sufficient for this IS. In case (2), the contributor is requested to provide the contribution on the definition for this term.

[SOURCE: Indicate the source of the contributed definition if not OED definition]

**3.7**
**conceptual model**
common structure and definitions for describing the concepts and relationships within an IoT system

[SOURCE: ISO/IEC 20006-1:2014(en), 4.8]

**Editor's Note**: Above definition from ISO/IEC 20006-1:2014(en) is for conceptual reference model, and the word "reference" has been deleted in WG10 meeting in Ottawa. At the beginning, there were two original WG10 definitions, "conceptual reference model" and "conceptual model". In Brussels Meeting, WG10 decided to merge both definitions into one definition, which is "conceptual reference model" with note: *"conceptual model" is deleted from vocabulary. "conceptual model" can still be used in the ISO/IEC 30141 with an agreement that "conceptual reference model" is inclusive of "conceptual model."* After the rename to conceptual model, this note seems obvious. Therefore, the note has been removed. The original definition of conceptual model of WG10 was "a representation of the characteristics of a *universe of discourse* by means of *entities* and *entity relationships*." With [SOURCE: Definition is from ISO/IEC 2382-17:1999(en), 17.02.02.] and Note: In ISO/IEC JTC 1 WG 10, a universe of discourse means Internet of Things (IoT).]

 

**conceptual model**
a set of diagrams and descriptions for describing the concepts, characteristics, uses, behaviour, relationships within a system

[SOURCE: modified from Smart Grid Interoperability Panel (SGIP) definition]

**Editor's Note**: Above new definition was selected and agreed by WG10 in Ottawa Meeting in N181 in compare with another new definition of conceptual model.

**3.8**
**concern**
interest in a system relevant to one or more of its stakeholders

[SOURCE: ISO/IEC 42010:2011]

Note 1 to entry: A concern pertains to any influence on a system in its environment, including developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.

**3.9**
**domain**
class of entities of similar group and common characteristic

[SOURCE: ISO 14813-5:2010(en), B.1.49]

**Editor's Note**: Above definition of domain discussed in WG 10 meeting in Belgium and agreed.

Domain is a grouping of entities.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.10**
**Digital Entity**
Digital entity is any computational or data element of an IT-based system, and it may exist as a service based in a data centre or cloud, or a network element or a gateway.

**Editor's Note**: Above definition added from SRG 5 CM contribution.

**3.11**
**Digital User**
A Digital User is an IoT-User that is a component. In other word, a Digital User is a non-human user of the IoT system and it includes automation services that act on behalf of human users.

**Editor's Note**: Above definition added from SRG 5 CM contribution.

**3.12**
**Endpoint**
An Endpoint is a component that exposes or uses network interfaces [ISO/IEC 24791-1:2010 ++].

**Editor's Note**: Above definition added from SRG 5 CM contribution.

 

**3.13**
**end-user**
a human individual who uses any computing-enabled device or appliance and who ultimately uses an IT product of service

[SOURCE: http://www.techopedia.com/definition/610/end-user]

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. This definition comes from N181.

**3.14**
**end-user asset**
property that end user owns and uses to access the information and service

[SOURCE: Contributor based on multiple sources]

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. This definition comes from N181.

**3.15**
**entity**
item inside or outside an information and communication technology system such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence

[SOURCE: ISO/IEC 24760-1:2011, 3.1.1]

**Editor's Note**: Above definition of entity discussed in WG 10 meeting in Belgium and agreed.

Entity is an item inside or outside of a system that has recognizably distinct existence.

Note 1 to entry: e.g., a person, an organization, a device, a subsystem, or a group of such items [ISO/IEC 24760-1:2011]

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.16**
**function**
**Editor's Note**: Need text of the definition

Action item – Use OED definition? – Contribution from WG 10 experts requested on the use of OED definition for this term. Provide the contribution as (1) Use of OED definition is sufficient for this IS; or (2) Use of OED definition is not sufficient for this IS. In case (2), the contributor is requested to provide the contribution on the definition for this term.

[SOURCE: Indicate the source of the contributed definition if not OED definition

**Editor's Note**: The definition of function in N181 used the definition from OED. Refer to the above action item.

 

**3.17**
**functional component**
functional building block needed to engage in an activity realized by an implementation

[SOURCE: ISO/IEC 17789:2014]

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. This definition comes from N181.

**3.18**
**gateway**
a functional unit that connects two computer networks have different network architectures.

[SOURCE: ISO/IEC 2382-18, 18.02.09]

**Editor's Note**: The above definition of gateway is from N181, and was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item.

Gateway is a forwarding component enabling various networks to be connected.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.19**
**human**
Human is a person.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.20**
**human physical entity**
A Human Physical Entity is a Human that is monitored or controlled.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.21**
**human user**
A human that is an IoT user.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.22**
**identifier**
Identifier contains detailed information that unambiguously distinguishes one entity from another one in a given identity context.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.23**
**identity**
Identity has the characteristics determining who or what a person or thing is.

 

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.24**
**identity context**
Identity context is the environment where an entity can use a set of attributes for identification and other purposes.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.25**
**interface**
shared boundary between two functional units, defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges, and other characteristics, as appropriate

[SOURCE: ISO/IEC 13066-1:2011(en), 2.15]

**3.26**
**interface device**
a hardware component or system of components that allows a human being to interact with a computer, a telephone system, or other electronic information system

[SOURCE: http://whatis.techtarget.com/definition/interface-device-IDF]

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. This definition comes from N181.

**3.27**
**Internet of Things**
an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

[SOURCE: ISO/IEC JTC 1/SWG 5&ISO/IEC 24760-1:2011, 3.1.1]

**3.28**
**IoT system**
a system that is comprised of functions that provide the system the capabilities for identification, sensing, actuation, communication, and management, and applications and services to a user

[SOURCE: Internet of Things: A Hands on Approach, Bahga & Madisetti, 2014]

**3.29**
**IoT User**
An IoT User is an entity that is interested in interacting with a physical entity. [IoT-A].

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.30**
**network**
A network connects endpoints, sources to destinations, and may itself act as a value added element in the IoT system or services.

 

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.31**
**network interface**
Named set of operations accessible on a network, that characterizes the behaviour of an endpoint.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.32**
**operator**
one who owns administration rights on the services it provides and/or on the entities it owns, is able to negotiate partnership with equivalent counterparts and define polices specifying how a service can be accessed by users

**Editor's Note**: The above definition of operator is from N181, and was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item.

**3.33**
**physical controller entity**
a physical entity that controls either mechanical or electronic actuator by a prescribed way

[SOURCE: Contributor]

**Editor's Note**: The above definition of physical controller entity is from N181, and was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item.

**3.34**
**physical entity**
a thing that is discrete, identifiable, and observable, and having material existence in real world

[Source: Contributor based on multiple sources]

**Editor's Note**: The above definition of physical entity is from N181, and was reviewed in WG10 meeting in Ottawa, and agreed.

Any physical object that is discrete, identifiable and observable and that is of interest from a user or application perspective. [IoT-A]++}.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.35**
**reference architecture**
description of common features, common vocabulary, guidelines, interrelations and interactions among the entities, and a template for an IoT architecture

[SOURCE: Modified from ISO/IEC 29182-2:2013(en), 2.2.1]

**3.36**
**Sensor**
A sensor is a component that senses or measures certain characteristics of the real world and transfers them into a digital representation. [IoT-A]

 

**Editor's Note:** The contribution of sensor in N181 was deleted from Clause 3 in the Ottawa meeting, but the above definition added from the SRG 5 CM Contribution. The original definition in N181 for sensor which was deleted in the Ottawa meeting: "device that observes and measures a physical property of a natural phenomenon or man-made process and converts that measurement into a signal."

**3.37**
**service**
A set of functions and facilities offered to a user by a provider

[SOURCE: ITU-T Y.2091 (2011)]

Service is a distinct part of the functionality that is provided by an entity through interfaces [ISO/TR 14252:1996].

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.38**
**service provider**
Abstract representation of all entities that provide a service to peer service users

[SOURCE: ISO/IEC 2382-26:1993, 26.03.10]

an organization that provides a network, storage or processing service

[SOURCE: http://www.pcmag.com/encyclopedia/term/51187/service-provider]

**Editor's Note**: Above both definitions in N181 were reviewed in WG10 meeting in Ottawa.

**3.39**
**service provider domain**
it is part of the IoT System that is associated with a given Service provider

[SOURCE: Adapted from oneM2M]

**Editor's Note**: The above definition of service provider domain is from N181, and was reviewed in WG10 meeting in Ottawa and agreed.

**3.40**
**stakeholder**
individual, team, organization, or classes thereof, having an interest in the system of interest

**Editor's Note**: The above definition of stakeholder is from N181, and was reviewed in WG10 meeting in Ottawa and agreed.

**3.41**
thing
**Editor's Note**: Need text of the definition

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. Contribution requested.

 

**3.42**
**transducer**
component that converts variations in one physical quantity, quantitatively into variations in another.

Note 1 to entry: A transducer can be either attached to or embedded inside a Physical Entity, or monitor a Physical Entity in its vicinity. [Short OED]

Note 2 to entry: Several IoT specifications have used the term Device for this concept. However, the term Device in the English dictionary has a much broader context, which is why this RA introduces Transducer as a more specific concept.

**Editor's Note**: Above definition added from the SRG 5 CM contribution.

**3.43**
**user**
any person, organization, process, device, program or system which uses services provided by others

[SOURCE: modified from ISO/IEC 29182-2]

entity using an infrastructure, system or information service, like any person, organization, process, device, program or system which uses services provided by others

[SOURCE: modified from ISO/IEC 29182-2]

**Editor's Note**: Above definition added from the N181.

**3.44**
**virtual controller entity**
a virtual entity that controls virtual actuator by a prescribed way

[SOURCE: Contributor]

**Editor's Note**: Above definition was reviewed in WG10 meeting in Ottawa, and was decided to leave this as an action item to be reviewed in the next WG10 meeting. This definition from N181.

**3.45**
**virtual entity**
a discrete software, firmware, or data, e.g., computing device/system or data storage device, that performs a task or tasks

[SOURCE: Contributor based on multiple sources]

# 4 Symbols and abbreviated terms

**Editor's Note**: The entries in this clause will be updated as this document matures.

5Vs Volume, Velocity, Veracity, Variability, and Variety

6LoWPAN IPv6 over Low power Wireless Personal Area Network

AAA Authentication, Authorisation, and Access

 

| | |
|---|---|
| AL | Application Layer |
| ASL | Application Support Layer |
| CAN | Control Area Network |
| DHCP | Dynamic Host Configuration Protocol |
| EPDL | End-Point Device Layer |
| FQDNs | Fully Qualified Domain Names |
| FTP | File Transfer Protocol |
| HAN | Home Area Network |
| HTTP | Hypertext Transfer Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IS | International Standard |
| IoT | Internet of Things |
| IRA | Information Reference Architecture |
| LAN | Local Area Network |
| LoA | Level of Assurance |
| NGO | Non-Governmental Organization |
| NL | Network Layer |
| ObD | Object Domain |
| OMD | Operation & Management Domain |
| PAN | Personal Area Network |
| QoS | Quality of Service |
| RA | Reference Architecture |
| RID | Resource Interchange Domain |
| SAD | Sensing and Actuating Domain |

 

| | |
|---|---|
| SCD | Sensing & Controlling Domain |
| SPD | Service Provider Domain |
| SPI | Serial Peripheral Interface |
| SRA | Systems Reference Architecture |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UrD | User Domain |
| URI | Uniform Resource Identifier |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |

# 5 IoT Reference architecture goals and objectives

IoT is defined as an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

The IoT Reference Architecture represented in this International Standard provides a conceptual reference model, reference architecture from different architectural views, common entities, and interfaces between IoT domains. The IoT RA not only outlines "what" the overall structured approach for the construction of IoT Systems by the architectural structure description, but also indicates "how" the architecture and its domains/entities will operate. In short, the IoT RA provides rules and guidance for developing an IoT system architecture and interfaces.

The IoT RA serves the following goals:

- to describe the characteristics and aspect of IoT systems;
- to define the IoT domains;
- to describe the reference model of IoT systems; and
- to describe interoperability of IoT entities.

Each IoT system will have specific systems requirements that should be met and can vary from one IoT system to next. The IoT RA provides the common architectural starting point with the same rules and guidance when the developers reuse the IoT RA.

The IoT RA supports the following important standardization objectives:

- to enable the production of a coherent set of international standards for IoT;

 

- to provide a technology-neutral reference point for defining standards for IoT; and
- to encourage openness and transparency in the identification of IoT benefits and risks.

The IoT RA is also intended to:

- facilitate the understanding of the operational intricacies of IoT systems;
- illustrate and provide understanding of IoT architectures from different architectural views;
- provide a technical reference to enable the international community to understand, discuss, categorize and compare IoT systems;
- facilitate the analysis of candidate use cases/applications including data/information flows; and
- facilitate the analysis of potential standards in areas including potential interface parameters, e.g., functionality, performance requirements, security/level of assurance (LoA), Quality of Services (QoS), etc.

# 6 Characteristics of IoT systems

## 6.1 Auto-configuration

### 6.1.1 Description

Auto-configuration is the automatic configuration of devices without manual intervention Auto-configuration allows an IoT system to react on conditions and add and remove of components such as devices and networks. Auto-configuration need security and handshake mechanism that allowed certified components to be configured into the system.

### 6.1.2 Relevance to IoT systems

Auto-configuration is needed for mission critical systems and benefit those users who expect robust systems. It can be set up with hardware stand by or manually introduced.

### 6.1.3 Examples

Example of auto-configuring devices and protocols: DHCP, Zero Configuration Networking (Zeroconf), etc.

## 6.2 Autonomic networking

### 6.2.1 Description

Autonomic capabilities in network control allow adaptation to different application domains, different communication environments, large numbers and different types of devices.

### 6.2.2 Relevance to IoT systems

Autonomic networking capabilities enhance the IoT systems' control functions in order to cope with the diversity of IoT system deployments with minimal dependency on humans and/or management systems.

### 6.2.3 Examples

Support of self-configuring, self-healing, self-optimizing and self-protecting techniques and/or mechanisms, for example:

- the capability of self-configuring for networking involves the abilities of autonomically configuring networking parameters based on discovered networking interfaces and predefined rules;
- the capability of self-healing for networking involves the abilities of autonomically recovering from fault status of networking based on monitoring results and predefined rules;
- the capability of self-optimizing for networking involves the abilities of autonomically optimizing networking operations based on monitoring results and predefined rules; and
- the capability of self-protecting for networking involves the abilities of autonomically protecting entities of networking from harmful operations based on predefined rules.

 

## 6.3 Autonomic service capabilities

### 6.3.1 Description

Autonomic service capabilities enable service provisioning based on pre-defined rules (e.g. configured by service provider and/or customized by IoT system's users), including autonomic capture, transfer and processing of data from things and other information (e.g. context information).

### 6.3.2 Relevance to IoT systems

Autonomic service capabilities enhance the IoT systems minimizing the dependency for service provisioning on humans and/or management systems. This is particularly beneficial for large scale and complex IoT system deployments.

### 6.3.3 Examples

Support of semantic based techniques. Support of techniques for processing of data from things (e.g. data aggregation techniques).

## 6.4 Composability

### 6.4.1 Description

The ability to compose individual components into a system to achieve a set of goals and objectives.

### 6.4.2 Relevance to IoT systems

System integration, interoperability and composability deals with how the functional building blocks are assembled to form a complete system and how the functional building blocks interface with each other via what binding mechanisms (e.g. dynamic or static, agent-based or peer-to-peer). Interoperability and composability are important topics in both the cyber and physical spaces. Composability imposes a stronger requirement than interoperability in that it requires building blocks not only compatible in their interfaces but exchangeable by other building blocks of the same kind that share the same set characteristics and properties such as in timing behaviours, performance, scalability and security. When a building block is replaced by another of the same kind that is composable, the overall system functions and characteristics are unchanged.

### 6.4.3 Examples

**Editor's Note**: Contribution requested.

## 6.5 Content-Awareness

### 6.5.1 Description

The property of being aware of the content and its associated metadata. Content-aware devices and services are able to adapt interfaces, abstract application data, improve information retrieval precision, discover services, and enable appropriate user interactions.

 

### 6.5.2 Relevance to IoT systems

Content awareness facilitates network service operations, such as path selection, routing, and service initiation, based on information such as location, quality of service requirements and activity awareness.

### 6.5.3 Examples

This capability can be essential in many applications including health services, broadcasting, surveillance systems and emergency services where some types of information or data flows have specific requirements with respect to timeliness, security, privacy etc.

## 6.6 Context-awareness

### 6.6.1 Description

The property of being aware of the context with which information is associated such as when or where an observation occurred in the physical world.

### 6.6.2 Relevance to IoT systems

Context-Awareness enables flexible, user-customized and autonomic services based on the related context of IoT components and/or users. Context information is used as the basis for taking actions in response to observations, possibly through the use of sensor information and actuators. Context in IoT means, amongst other things, an awareness of time, place, and thing (when, where, what). To fully utilize an observation and affect an action, this understanding is critical.

### 6.6.3 Examples

**Editor's Note**: Contribution requested.

## 6.7 Data 5Vs – Volume, Velocity, Veracity, Variability and Variety

### 6.7.1 Description

Data characteristics of volume, velocity, veracity, variability, and variety that require a scalable architecture for efficient storage, manipulation, and analysis.

### 6.7.2 Relevance to IoT systems

IoT Systems and devices are also expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby increasing the need to better index, store and process such data.

### 6.7.3 Examples

Logistic company is using big data is for On-Road Integrated Optimization and Navigation. The tool uses hundreds of millions of address data points, plus other data collected on the deliveries, to optimize delivery routes for efficiency.

 

## 6.8 Discoverability

### 6.8.1 Description

Discoverability allows users, services, and other devices, to find both devices on the network and the capabilities and services they offer at any particular time. Discovery services allow IoT users, services, devices and data from devices to be discovered according to different criteria, such as geographic location.

### 6.8.2 Relevance to IoT systems

Services (and information providing services) connected with the IoT system can indicate what information can be found by a Discovery/Lookup service. Discovery and lookup service of IoT systems allow the locating physical entities based on geographical parameters and the dynamic discovery of relevant virtual and physical entities and their related services based on respective specifications.

### 6.8.3 Example

Network mapping discovers the devices on the network and their connectivity. It is not to be confused with network discovery or network enumerating which discovers devices on the network and their characteristics such as operating system, open ports, listening network services, etc.

## 6.9 Heterogeneity

### 6.9.1 Description

An IoT system typically is composed of a diverse set of components/entities that interact in various manners.

### 6.9.2 Relevance to IoT systems

IoT is cross-system, cross-product, and cross-domain. Realizing the full promise of IoT will require interoperability among heterogeneous components and systems, supported by new reference architectures using shared vocabularies and definitions. This heterogeneity will create several challenges for the resulting IoT systems.

### 6.9.3 Examples

**Editor's Note**: Contribution requested.

## 6.10 Legacy support

### 6.10.1 Description

A service, protocol, device, system, component, technology, or standard that is outdated and no longer meets the requirements of the environment it is used in.

### 6.10.2 Relevance to IoT systems

Support of legacy component integration and migration can be important. When supporting legacy components it is important to ensure that the design of new components and systems do not unnecessarily limit future system evolution. To prevent prematurely stranding legacy investment, a plan for adaptation and migration of legacy systems is important. Care ought to be taken when integrating legacy components to ensure that security and other essential performance and functional

 

requirements are met. Legacy components increase risk and vulnerabilities. Since current technology will become legacy technology in the future it is important to have a process in place for managing legacy aspects of IoT. The different lifecycles of physical systems and information systems also creates additional challenges for managing legacy aspects in IoT.

### 6.10.3 Examples

**Editor's Note**: Contribution requested.

## 6.11 Location-awareness

### 6.11.1 Description

The property of being aware of the location an observation occurred in the physical world and where an action will need to occur in the physical world.

### 6.11.2 Relevance to IoT systems

IoT system components that interact with the physical world need an awareness of physical location. Both observations of a property in the physical world and actions back in the physical world need to be associated with a particular location. The accuracy requirement for location will change based upon the application. It is therefore important that components can describe not only their locations, but also the associated uncertainty of the locations. Location-awareness is related to time-awareness through velocity.

### 6.11.3 Examples

IoT system used for smart parking will operate on city-wide Wi-Fi, giving residents real-time updates on where to park and allowing them to pay with their phone. Smart bus-stops provide passengers with real-time updates via touch-screen panels, and a city-wide sensor network informs workers and residents about temperature, air quality, noise level, and pedestrian traffic.

## 6.12 Manageability

### 6.12.1 Description

Manageability addressing aspects such as device management, network management, system management, and interface maintenance and alerts is important to meet IoT system requirements. Manageability needs monitoring and reacting components to be configured into the IoT device, network and system.

### 6.12.2 Relevance to IoT systems

Most IoT devices, networks, systems are unmanned and run automatically, and they are easy to be malfunctioned, unstable, miscalibrated and destroyed during the lifetime. The efficient service could not be provided without manageability for IoT system.

### 6.12.3 Examples

The smoke sensors and fire monitoring system which are deployed in the buildings and are hard to maintain, normally are easy to malfunction. It is very dangers if the system without the manageability to find the potential problems of the system. So when we design and develop the

 

system, the manageability components are very necessary to be configured, such as the device state monitoring component, the link monitoring component, the calibration component etc.

## 6.13 Modularity

### 6.13.1 Description

The property of a component to be a distinct unit that can be combined with other components.

### 6.13.2 Relevance to IoT systems

Modularity allows components to be combined in different configurations to form systems as needed. By focusing on standardized interfaces and not specifying the internal workings of each component, implementers have flexibility in the design of components and IoT systems.

### 6.13.3 Examples

**Editor's Note**: Contribution requested.

## 6.14 Network connectivity

### 6.14.1 Description

In IoT networks, networked devices (objects/things) pass data to each other along physical links. The connections between nodes are established using either wired or wireless media. Networked IoT devices (objects/things) that originate, route and terminate the data are described as (network) nodes. Endpoint network devices (objects/things) are the Source or Destination of any kind of information. Any IoT related networking Communications protocol shall/should be layered onto (other) more specific or more general communications protocols, down to the physical layer that directly deals with the transmission media at every Node/Endpoint of a devices (objects/things).

### 6.14.2 Relevance to IoT systems

IoT systems rely on the ability to exchange information units within a structured manner based upon different but interoperable kind of Network Topologies – all within a physical, wired or wireless network – with the IoT devices (objects/things) to be called "networked" (together) when one device is able to exchange information with the other device (objects/things), whether or not they have a direct connection to each other. IoT Network structure can/should be able to be static/dynamic at any time of its existence, and (consider) structural elements like: QoS, resilience, encryption, AAA (Authentication, Authorisation, and Access).

### 6.14.3 Examples

IoT Network consists of Physical defined: 801.xx 803.xx 802.11.yy - with elements like: repeaters, hubs, bridges, switches, routers, modems, firewalls – (Classical) or newer Technologies like: ZigBee, 6WLoPAN, 802.15.4.xx. / Topologies can be: Mesh, Ring, Star, Fully connected, Line, Tree, Bus.

The Scale of an IoT Network (and their elements) can be: Nanoscale, PAN, LAN, WAN, HAN, VPN

Organisational IoT Network can be: Inter- and intra-network, Internetwork (in the meaning of networks of different kind of an architecture/structure connecting together).

 

## 6.15 Plug and play

### 6.15.1 Description

Plug and Play capability enables on-the-fly configuration and activation of interconnected components for their seamless integration and cooperation with applications, and responsiveness to application requirements. An example of its applicability concerns the automatic triggering of the device configuration procedure as soon as a device is connected to an IoT system.

### 6.15.2 Relevance to IoT systems

This capability can facilitate the deployment of IoT systems, especially in environments with lack of human technical expertise. It can also be used for purposes of security which can be critical in given environments or for given applications (e.g. protection against counterfeit devices).

### 6.15.3 Examples

Configuration and activation of devices based on semantic techniques.

## 6.16 Reliability

### 6.16.1 Description

Appropriate level of reliability in capabilities such as communication, service and data management capabilities is important to meet system requirements.

### 6.16.2 Relevance to IoT systems

Appropriate level of reliability is essential in diverse IoT system deployments and applications. It can be highly critical in some applications, e.g. for specific human body related applications.

### 6.16.3 Examples

Support of integrity checking techniques.

## 6.17 Scalability

### 6.17.1 Description

Scalability is the characteristic of a system to continue to work effectively as the size of the system or the volume of work performed by the system is increased.

### 6.17.2 Relevance to IoT systems

IoT systems involve various elements such as devices, services, applications, users, stored data, data traffic, event reports. The numbers/volumes of each of these elements can change over time and it is important that the IoT system continues to function effectively when the numbers/volumes increase.

### 6.17.3 Examples

One example of scalability is the case where the number of sensor devices attached to an IoT system is increased, for example, increasing the number of temperature sensors from those attached to a single building to those attached to all buildings in a city. The consequence of increasing the number of sensors in this way is that there are increases in the volume of sensor data flowing in the system, in the

 

volume of historical data stored in databases, in the number of devices handled by the management system, in the number of temperature readings processed by services and applications.

## 6.18 Shareability

### 6.18.1 Description

The ability to use individual components in multiple interconnected systems.

### 6.18.2 Relevance to IoT systems

Many IoT components are underutilized – a single system often uses only a fraction of a components capabilities. By providing functionality for components to be shared among multiple systems these resources can be more efficiently used.

### 6.18.3 Examples

**Editor's Note**: Contribution requested.

## 6.19 Time-awareness

### 6.19.1 Description

The property of being aware of the time an observation occurred in the physical world and when an action will need to occur in the physical world.

### 6.19.2 Relevance to IoT systems

Accurately associating a time with a measurement from the physical world is an important aspect of IoT components. It may be necessary to accurately combine or associate data from multiple sensors and data sources. Both the time value and uncertainty of the value are needed to properly assess whether a specific component can perform the requisite task. The accuracy requirement for time will change based upon the application. It is therefore important that components can describe not only their time, but also the associated uncertainty of the times. Time-awareness is related to location-awareness through velocity.

### 6.19.3 Examples

IoT systems and devices which are used for fleet management need to collect time and location related data and to act on such real-time information.

## 6.20 Timeliness

### 6.20.1 Description

The property of performing an action, function, or service within a specified period of time.

### 6.20.2 Relevance to IoT systems

Because IoT systems act on the physical world, events need to occur at certain times. To achieve this, the actions, functions, and services that lead to the action need to happen within specific time constraints. Timeliness in IoT includes not only latency related issues, but jitter, frequency/sampling rate, and phase. Timeliness (and to some extent time awareness) is also connected to location through velocity.

 

### 6.20.3 Examples

IoT system for smart meter, which needs to collect energy consumption data at specific time constrains in order to perform demand and response capabilities at grid system.

## 6.21 Unique identification

### 6.21.1 Description

**Editors' Note**: Some of the test in this section needs to be moved to the next section, "Relevance to IoT systems"→*Document editors made editorial changes in this clause* – The second paragraph has been moved to the clause "Relevance to IoT systems" below, again the second paragraph there.

Unique identification is the characteristic of a system to enable the entities to be identifiable and traceable.

### 6.21.2 Relevance to IoT systems

The entities in the IoT system such as the devices, physical and virtual objects, and end-users are essentially to be distinguished by each other which enables the interoperability and global services across the heterogeneous IoT systems. Standardised unique identification associated with each entity in IoT systems (e.g., devices and services) allows for interoperability and support services such as discovery, trace and track, and authentication across heterogeneous networks.

The unique identification is a universal construct for any entity. It is used in IoT systems that need to track or refer to entities. It is intended for use with any identification scheme.

### 6.21.3 Examples

IPv4, IPv6, URI, and Fully Qualified Domain Names (FQDNs) are used as unique identification in the Internet which may guarantee the devices can be routed and accessed, the physical and virtual objects can be managed or associated, and the end-user can be satisfied by the services from the IoT systems independently.

## 6.22 Well-defined components

### 6.22.1 Description

Components that can provide an accurate description of the component capabilities including associated uncertainties. Capability information includes not only information about the specific component functionality, but configuration, communication, security, reliability and other relevant information.

### 6.22.2 Relevance to IoT systems

Since the components that are used to assemble a IoT system will be discovered through a information system interface and no more information about the component may be available. Without understanding the capabilities of each component that will be used within a system it will be difficult to understand whether the system with meet its design goals.

### 6.22.3 Examples

**Editor's Note**: Contribution requested.

 

---

**Editors' Notes:** There are more characterisers than the listed above, such as regulation compliance, security, confidentiality and privacy, reliability, availability, interoperability, flexibility etc. New contributions from experts are requested.

**Editors' Notes:** Contributions made by Faud and Tyson were not reviewed by WG 10. WG 10 decided to remove all text except the clause headings. Faud and Tyson make their contributions toward these sub-clauses (sub-clauses 6.23 to 6.35) to be considered in the next WG 10 meeting in China.

## 6.23 Regulation Compliance

### 6.23.1 Description

### 6.23.2 Relevance to IoT systems

### 6.23.3 Examples

## 6.24 Confidentiality

### 6.24.1 Description

### 6.24.2 Relevance to IoT systems

### 6.24.3 Examples

## 6.25 Reliability

### 6.25.1 Description

### 6.25.2 Relevance to IoT systems

### 6.25.3 Examples

 

## 6.26 Identity

### 6.26.1 Description

### 6.26.2 Relevance to IoT systems

### 6.26.3 Examples

## 6.27 Accessibility

### 6.27.1 Description

### 6.27.2 Relevance to IoT systems

### 6.27.3 Examples

## 6.28 Usage, context, and environment

### 6.28.1 Description

### 6.28.2 Relevance to IoT systems

### 6.28.3 Examples

## 6.29 Interoperability

### 6.29.1 Description

### 6.29.2 Relevance to IoT systems

### 6.29.3 Examples

 

## 6.30 Flexibility

### 6.30.1 Description

### 6.30.2 Relevance to IoT systems

### 6.30.3 Examples

## 6.31 Intelligence control

### 6.31.1 Description

### 6.31.2 Relevance to IoT systems

### 6.31.3 Examples

## 6.32 Safety

### 6.32.1 Description

### 6.32.2 Relevance to IoT systems

### 6.32.3 Examples

## 6.33 Resilience

### 6.33.1 Description

### 6.33.2 Relevance to IoT systems

### 6.33.3 Examples

## 6.34 Availability

### 6.34.1 Description

### 6.34.2 Relevance to IoT systems

### 6.34.3 Examples

## 6.35 Privacy

### 6.35.1 Description

### 6.35.2 Relevance to IoT systems

### 6.35.3 Examples

# 7 Characteristics, principles, and requirement of the IoT RA

**Editors' Note**: Howard will provide new contributions for clause7 by next meeting.

**Editors' Note**: Clause IoT reference architecture framework has been moved to Annex B based on last WG10 meetings decision. It will be determined later whether to bring the content (with contributions/updates/modification) back to the main body or not. Thus, contributions and comments are requested. See Annex B.

# 8 IoT Conceptual model

**Editors' Note**: the following SRG5 contribution has been reviewed by WG10 at 3rd Meeting, content is updated according to the review result from the disposition of N190, N202 after the meeting in Ottawa.

## 8.1 Main purpose

IoT covers a wide range of applications, for example, applications in smart city, in smart energy, in smart mobility, in smart home, in smart building, in smart factory, in smart health, in smart logistic etc. Each application area has its own characteristics, which leads to different requirements on IoT system architecture. In order to develop a generic IoT reference architecture which is applicable for all application areas, it is necessary to investigate its common concepts and relationships at abstract level. Such investigation helps to establish a solid grounding for further development of the reference architecture.

The conceptual model (CM) provides common structure and definition for describing the concepts of and relationships between the entities within IoT systems. It must be generic, abstract and simple. In order to achieve this goal, it is important to clarify the fundamental of the IoT systems by asking following questions:

1. What are the key members of the family of entities in a typical IoT system?
2. What is the relationship between the entities, especially between digital entities and their physical entities?
3. Who and where are the actors?
4. How the things and services are collaborated through network?
5. What is the big picture of the overall IoT entities and their relationships?
6. What are the key concerns of security and privacy at conceptual level?

The following clauses describe the conceptual reference model focusing on above six points. The models presented here use simplified Unified Modelling Language™ (UML®, hereafter "UML"). Clause 9.2 provides a short description of the simplified UML in order to help readers to better understand CRM diagrams presented in this standard.

## 8.2 Interpreting model diagram

In this standard, UML Class diagrams have the following restrictions:

— Concepts are represented as UML Classes with no attributes.

— The documentation for each concept is the definition of the concept.

Only two kinds of associations are used:

1. Generalization (an "is-a" relationship): For example, sensor is a transducer. This generalization relationship can be expressed as shown in Figure 8-1:

 

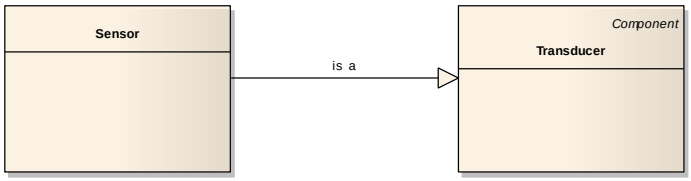


**Figure 8-1. Generalization.**

2. Directed association (expresses relationship between concepts. These association names are verbs.). Figure 8-2 expresses the association relationship that Sensor monitors Physical Entity.

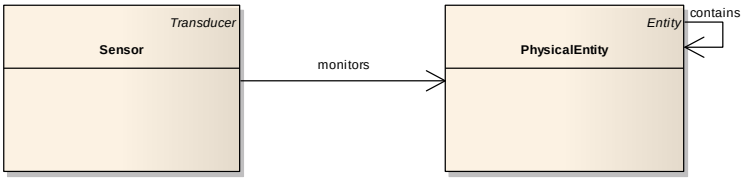


**Figure 8-2. Association.**

Cardinality constraints on association ends are not shown. At this point they all can be considered as zero or more.

**Editors' note**: We may need to add cardinality constraints later.

If a concept, which is a generalization of a concept on the diagram, is not itself shown on the diagram, the name of that generalized concept appears in italics at the top right corner of the box as shown in Figure 8-1 ("*Physical Entity*") and Figure 8-2 ("*Transducer*").

## 8.3 Concept

### 8.3.1 IoT Entities and domains

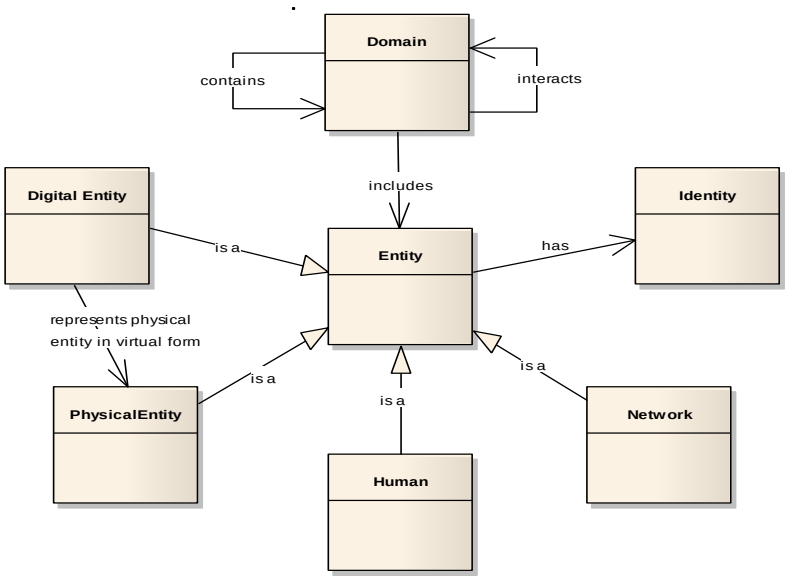


**Figure 8-3. Entity and Domain Concepts.**

Figure 8-3 shows the whole IoT family of entities. A thing with distinct and independent existence is called entity, for example, a person, an organization, a device, a subsystem, or a group of such items. We can consider that everything in IoT world is a kind of entity, and an IoT system is a collection of entities, their relationship and interactions.

Digital entity is any computational or data element of an IT-based system, which may exist as a service based in a data centre or cloud, or a network element, or a gateway, or sometimes a virtual entity which represents a physical entity etc. A person is a human entity, while physical entity is discrete, identifiable and observable, which can be monitored or controlled through human entity or digital entity. Network is another important entity in IoT world, through which the other entities can be communicated with each other. Any entity may contain an identity with which it can be identified and communicated with each other through the network.

When a system evolves and becomes more complex to manage or to develop as a whole, there is a need to decompose the system into smaller elements and group the elements with similar or common characteristic into a specific domain. Each domain has its own boundary. Showing interaction among domains instead of those among all the entities in a system can provide a simpler high level view of how the complex system works. Figure 8-4 shows that one IoT domain A interacts with another IoT domain B. Of cause, one IoT domain can also interact with multiple IoT domains.

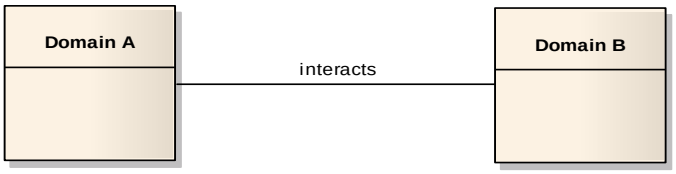


**Figure 8-4. Domain Interactions.**

Domain is composed of various types of entity. Sometimes one large domain can be segmented into more sub-domains. Figure 8-5 shows that Domain A contains two sub domains, Domain C and Domain D.

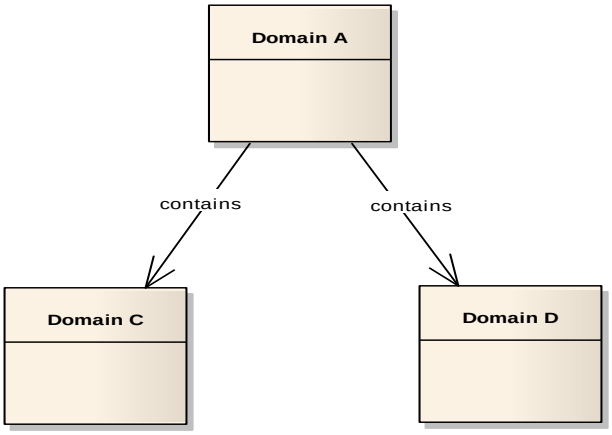


**Figure 8-5. Domain Composition.**

Following subclauses provide a short text description regarding corresponding association shown in above diagrams in table form. To avoid duplication description of relationship between two entities, only entities with outgoing relationship will be described.

 

#### 8.3.1.1 Entity

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Association | Identity | Entity has identity. |

#### 8.3.1.2 Domain

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Association | Entity | A Domain includes one or more entities. |
| **2** | Association | Domain | A Domain may contain sub Domains |
| **3** | Association | Domain | A Domain may interact with other Domains |

#### 8.3.1.3 Digital entity

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Entity | A Digital Entity is a specialization of Entity. |

#### 8.3.1.4 Physical entity

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Entity | A Physical Entity is a specialization of Entity. |
| **2** | Association | Physical Entity | A Physical Entity may contains other Physical Entities |

#### 8.3.1.5 Human

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Entity | A Human is specialization of Entity representing a person. |

 

#### 8.3.1.6 Network

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Entity | A Network is a specialization of Entity. |
| **2** | Association | Endpoints | A Network connects a group of Endpoints. |

### 8.3.2 Identity

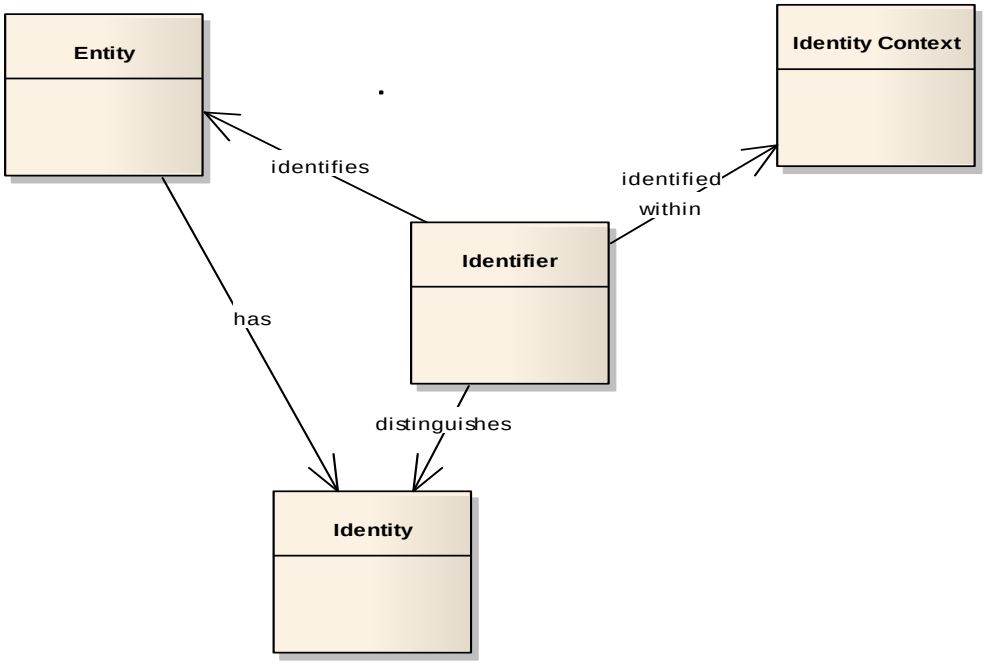


**Figure 8-6. Identity Concept**

Figure 8-6 shows the identity concept. Most entities in IoT especially physical entity ("Thing") need identity. Identifiers can be understood as a dedicated, publicly known attribute or name for an identity, a person or a device. Typically, identifiers are valid within a specific context. Thing can have more than one identifier, but it requires at least one unique identifier within any environment or context through which it can be accessed. For example, identity information from a Tag can be used as Identifier to identify the Physical Entity to which it is attached.

Following sub clauses provide a short text description regarding corresponding association shown in above diagram in table form. To avoid duplication description of relationship between two entities, only entities with outgoing relationship will be described.

#### 8.3.2.1 Identifier

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|

 

| | | | |
|---|---|---|---|
| **1** | Association | Entity | Identifier identifies Entity. |
| **2** | Association | Identity | Identifier distinguished identity. |
| **3** | Association | Identity Context | Identifier identified with a given identity context |

### 8.3.3 Services, components, and endpoints

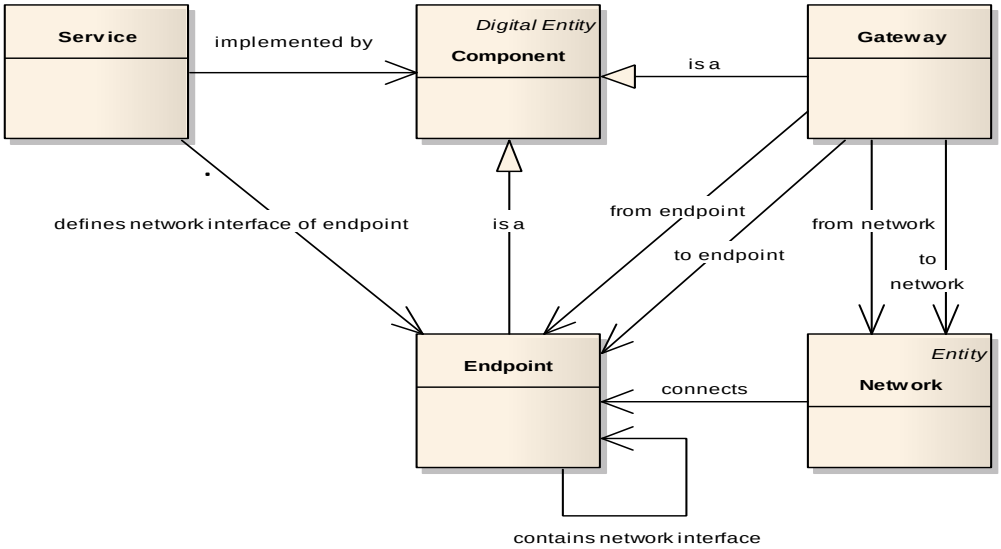


**Figure 8-7. Service, Component, and Endpoint Concepts.**

Figure 8-7 shows how services and components are collaborated through network. Service is an abstract concept. A service is realized by one or more components. There could be multiple alternative realizations of the same service. An endpoint must exist somewhere on some network. A component has one or more endpoints. A service has one or more interfaces, which is realized through component. Services, which need to be accessible remotely through network, are exposed through network interface in endpoint. Local interfaces are part of the internal implementation of a component, but are not subject to the requirements of an interface exposed on a network. Because there are different kinds of networks co-existing, which may use different network protocols for the communication, therefore, gateway is the important part of IoT communication. Gateway is a forwarding component enabling various networks to be connected.

Following subclauses provide a short text description regarding corresponding association shown in above diagram in table form. To avoid duplication description of relationship between two entities, only entities with outgoing relationship will be described.

#### 8.3.3.1 Components

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Digital Entity | A Component is a specialization of Digital Entity. |

 

#### 8.3.3.2 Endpoint

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Component | An Endpoint is a specialization of Component. |
| **2** | Association | Endpoint | An Endpoint may contain more than one network Interface. |

#### 8.3.3.3 Gateway

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Component | A Gateway is a specialization of Component. |
| **2** | Association | Network | The network from which interactions are forwarded. |
| **3** | Association | Network | The network that interactions are forwarded to |
| **4** | Association | Endpoint | An Endpoint from which interactions are forwarded |
| **5** | Association | Endpoint | An Endpoint that interactions are forwarded to |

#### 8.3.3.4 Service

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Association | Component | A Service is implemented by one or more components. |
| **2** | Association | Endpoint | A Service defines Network Interfaces of an Endpoint. |

 

### 8.3.4 IoT User

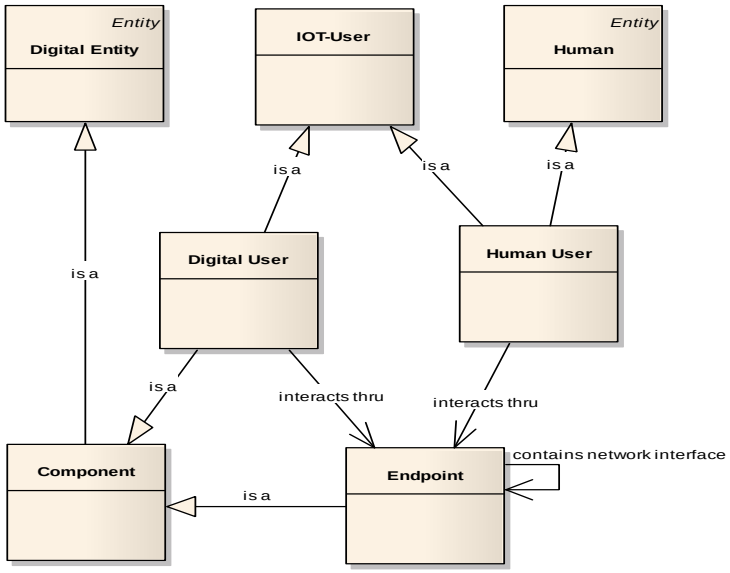


**Figure 8-8. IoT User Concepts.**

As shown in Figure 8-8, actors of IoT systems are IoT users. IoT user can be either human (Human User) or digital component (Digital User). A digital user includes automation services that act on behalf of human users, for example machine to machine. IoT user interacts with a physical entity directly or indirectly through the endpoint. IoT user also uses endpoint to communication with other IoT user or services in the network.

Following subclauses provide a short text description regarding corresponding association shown in above diagram in table form. To avoid duplication description of relationship between two entities, only entities with outgoing relationship will be described.

#### 8.3.4.1 Human user

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Human | A Human user is a specialization of a Human. |
| **2** | Generalization | IoT User | A Human User is also a specialization of an IoT user |
| **3** | Association | Endpoint | A Human User interacts across the Network thru an Endpoint, using its local user interfaces. |

#### 8.3.4.2 Digital user

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | IoT-User | A Digital User is a specialization of IoT-User |

 

| | | | |
|---|---|---|---|
| **2** | Generalization | Component | A Digital User is also a specialization of Component. |
| **3** | Association | Endpoint | Digital user interacts with an Endpoint through local (non-networked) interfaces to utilize functions offered by the IoT system across the network. A component implementation could combine the endpoint capabilities with the Digital user capabilities. |

### 8.3.5 Physical entities, digital entities, and transducers

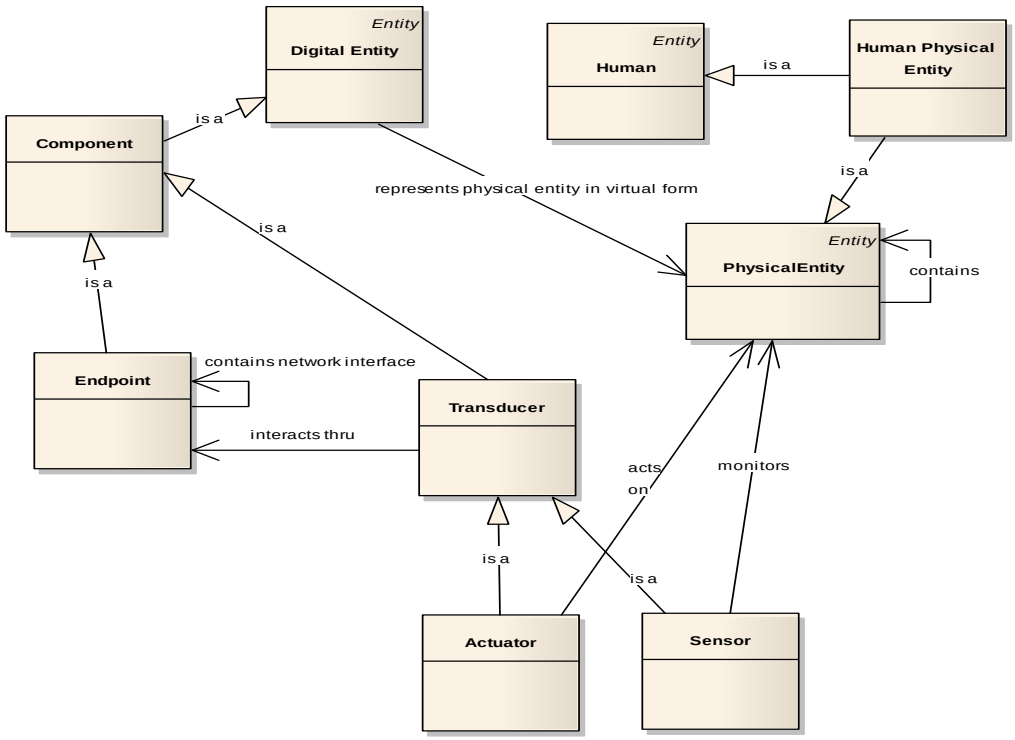


**Figure 8-9. Physical Entity, Digital Entity, and Transducer Concepts.**

Figure 8-9 shows the relationship between digital and physical entities. Digital entity can be considered as an assembly of certain components. Actuator and Sensor are the components which have direct or indirect contact with Physical Entity. Actuator executes digital information to alter some property of a physical entity. Sensor perceives certain characteristics of the real world and transfers them into a digital representation. Actuator and Sensor are kind of transducer, which converts variations in one physical quantity, quantitatively into variations in another.

Using a smartphone for example, it has a sensor to detect temperature of a physical object. A Bluetooth app on a smartphone communicates with an air conditioner to control the room temperature, where the air conditioner can be considered as an actuator. A smart phone may have locally installed database (local component) to retrieve the barcode information of the scanned object, or it may communicate with hosted catalogue system via mobile network using endpoint component at the phone (modem unit).

 

Following subclauses provide a short text description regarding corresponding association shown in above diagram in table form. To avoid duplication description of relationship between two entities, only entities with outgoing relationship will be described.

#### 8.3.5.1 Transducer

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Component | A transducer is a specialization of Component |
| **2** | Association | Endpoint | A Transducer interacts on the network, thru an Endpoint, which it interacts with using local (non-networked) interfaces. A component implementation could combine the endpoint capabilities with the transducer capabilities. |

#### 8.3.5.2 Sensor

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Transducer | a Sensor is a specialization of Transducer |
| **2** | Association | Physical Entity | A Sensor monitors a Physical Entity |

#### 8.3.5.3 Actuator

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Transducer | An Actuator is a specialization of Transducer |
| **2** | Association | Physical Entity | An Actuator acts on a Physical Entity. |

#### 8.3.5.4 Human physical entity

The Conceptual Model defines the following relationships from this concept.

| Nr | Relationship Type | Related Concept | Description |
|---|---|---|---|
| **1** | Generalization | Human | A Human Physical Entity is a specialization of a Human. |
| **2** | Generalization | Physical Entity | Human Physical Entity is also a Physical Entity which is monitored or controlled. |

 

### 8.3.6 Security and privacy

**Editor's Note**: Faud and Tyson will make the contribution.

## 8.4 The big picture

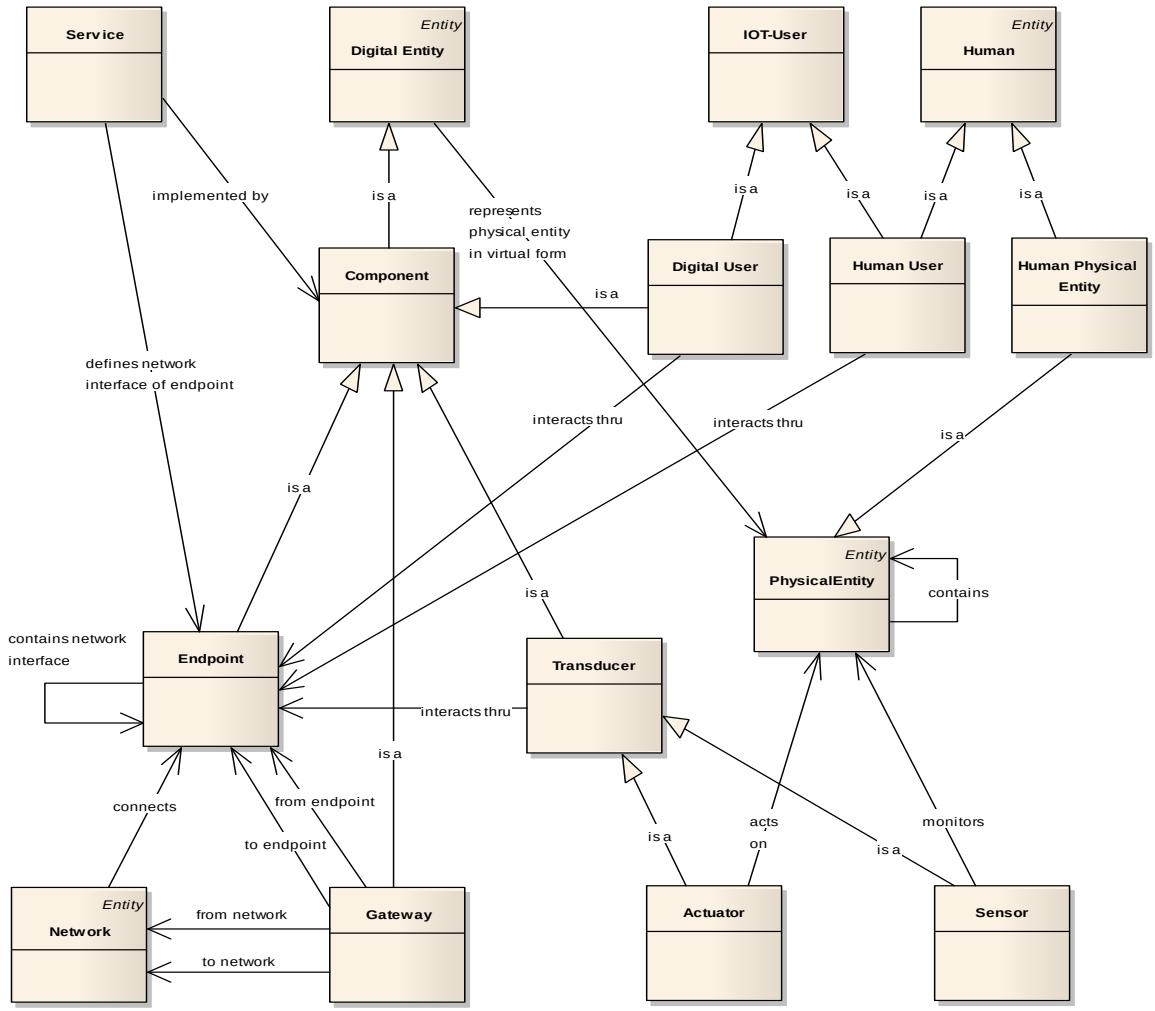


**Figure 8-10. Big Picture of IoT Concepts.**

The model diagram in Figure 8-10 provides the big picture of all key IoT entities defined in this CM, their relationships and their interactions. All entities have unique identity, so that they can be distinguished and communicated with each other in the global network. An IoT User consumes services through endpoint, which is attached to the communication network, while the gateway enables communication between different types of networks. Physical entity, which is usually represented as virtual form in digital entity, can be monitored and controlled through sensors and actuators.

# 9 Internet of Things reference architecture (IoT RA)

**Editor's Note:** Comment from WG 10 3rd Meeting in Ottawa is to move the conceptual model and reference model clauses in N184 to the reference architecture clause, and is to move the reference architecture clauses in N184 to one of the annex of this document as the implementation guidance of IoT systems.

 

**Editor's Note**: Comment from WG10 3rd Meeting in Ottawa. Claus RM describes only 6 domains approach, in RA there will be also other views or approaches. Now there are two options: option 1 rename reference model to IoT domain view or option 2 extend this to be RM for all other architecture views.

**Editor's Note**: Comment from WG10 3rd Meeting in Ottawa. Check whether 6 domains approach can be merged or harmonized with functional view from the N154 and N205.

**Editor's Note**: Comment from WG10 3rd Meeting in Ottawa. Check and update term and definitions used by 6 domains approach to be consistent with Chapter conceptual model.

**Editor's Note**: The text in Clause 9 has not reached a WG 10 consensus. WG 10 invites contributions against the text of Clause IoT RAs.

## 9.1 On Reference model (RM) and reference architecture (RA)

A reference model (RM) is an abstract framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist. A reference model is not directly tied to any standards, technologies or other concrete implementation details, but it does seek to provide a common semantics that can be used unambiguously across and between different implementations. [4]

There are a number of concepts rolled up into that of a reference model (RM). A RM is abstract, and it provides information about environments of a certain kind. A RM describes the type or kind of entities that may occur in such an environment, not the particular entities that actually do occur in a specific environment. A RM describes both types of entities (things that exist) and their relationships (how they connect, interact with one another, and exhibit joint properties). A list of entity types, by itself, doesn't provide enough information to serve as a reference model. A RM does not attempt to describe "all things." A RM is used to clarify "things within an environment" or a problem space. To be useful, a RM should include a clear description of the problem that it solves, and the concerns of the stakeholders who need to see the problem get solved. A RM is technology agnostic. A RM's usefulness is limited if it makes assumptions about the technology or platforms in place in a particular computing environment. A RM typically is intended to promote understanding a class of problems, not specific solutions for those problems. As such, it must aid the process of imagining and evaluating a variety of potential solutions in order to assist the practitioner. RM is useful to: (a) to create standards for both the objects that inhabit the model and their relationships to one another; (b) to educate; (c) to improve communication between people; (d) to create clear roles and responsibilities; and (e) to allow the comparison of different things. [5]

Reference architecture can be understood as contexts provided with common feature, vocabulary, requirements together with supporting artefacts to enable their use, where the artefacts are the description of the major foundational architecture components, that provide guidelines and constrains for instantiating solution architectures, that can be defined not only from a different emphasis or viewpoint but also at many different levels of detail and abstraction, and that consist of a list of entities and functions and some indication of their interfaces, interrelations and interactions with each other

 

and with functions located outside of predefined architecture patterns representing the entities and functions.[1]

## 9.2 IoT Reference models for IoT systems

### 9.2.1 Entity-based reference model

A composite entity-based reference model of IoT systems is shown in Figure 9-1. This figure only contains the representative, common IoT entities shown in Figure 9-2 without populating different types of Stakeholder (Figure 9-3) and the key IoT Device (Figure 9-4). Figure 9-1 provides the activity interaction arrowhead lines between the entities. Each arrowhead line is described with a concise, representative activity description to convey the activity relationships in Figure 9-1. Table 9-1 further provides additional descriptions of the activity/interaction/relationship arrowhead line between each entity pair. The first column is the number identifier of the arrowhead line, the second column list the sourcing entity, and the third column lists the sinking entity of the arrowhead line, the fourth column provides the description of the activity, interaction, and/or relationship.

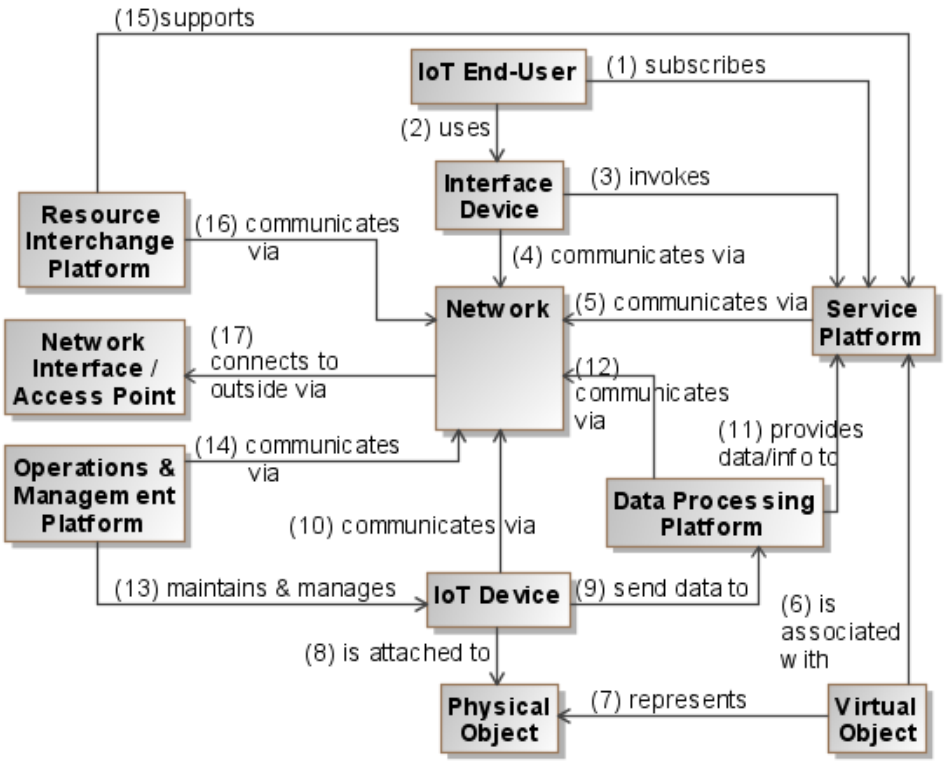


**Figure 9-1. Entity-based reference model of the IoT systems.**

**Table 9-1. Representative interaction between the representative entities shown in Figure 9-1.**

[1] Based on the descriptions from ISO/IEC JTC1/WG 10; IoT-A; http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf. Reference Architecture Description, Office of the DoD CIO, June 2010; https://en.wikipedia.org/wiki/Reference_architecture; http://www.ibm.com/developerworks/rational/library/2774.html; http://www.liteea.com/wordpress/horizongtal/what-is-reference-architecture, Rational Unified Process; and The introduction to the IBM's Master Data Management Reference Architecture.

 

| (#) | From | To | Description |
|---|---|---|---|
| **1** | IoT End-User | Service Platform | End-user subscribes for specific service(s) from the service platform which may be operated by a service provider. |
| **2** | IoT End-User | Interface Device | End-user uses a type of interface devices (e.g., keyboard, smart phone, tablet, etc.) to access various types of information or to request services.<br><br>Other types of human stakeholder in an IoT system also have their interface devices, but these are not represented in the Conceptual Model as these are the similar cases represented by the End-user example. |
| **3** | Interface Device | Service Platform | Upon the End-user's entry (e.g., request for data/information or service), the Interface Device invokes Service Platform to obtain the service. |
| **4** | Interface Device | Network | Depending on the End-User's request entry type, Interface Device communicates via Network to various other entities in an IoT system, e.g., direct access to the physical/virtual objects in the IoT system's environment, contacting the 3rd party/market organizations, etc. |
| **5** | Service Platform | Network | Service Platform communicates with other entities in an IoT system via Network, e.g., to obtain sensor data from the sensors monitoring the IoT environment. |
| **6** | Virtual Object | Service Platform | Certain virtual objects embedded in physical objects in an IoT system's environment are associated with the virtual entities in Service Platform. |
| **7** | Virtual Object | Physical Object | Virtual Object embedded in Physical Object functionally represent the Physical Object. |
| **8** | IoT Device | Physical Object | IoT Device is likely attached to Physical Object. For certain situations, IoT Device can be structurally embedded in Physical Object. For other situation, IoT Device, especially Sensor, can be located away from Physical Object monitoring the Physical Object from a distance. |
| **9** | IoT Device | Data Processing Platform | IoT Device sends its data to Data Processing Platform so that Data Processing Platform can compute, aggregate, fuse, process for information, etc., using the data. |
| **10** | IoT Device | Network | IoT Device communicates (e.g., sending data, etc.) with other entities in an IoT system via Network. |
| **11** | Data Processing Platform | Service Platform | Data Processing Platform provides the processed data and/or extracted information to Service Platform so that Service Platform can further refined the data/information received in order to fulfil End-Users' service request. |
| **12** | Data Processing | Network | Data Processing Unit communicates with other entities in an IoT system via Network. |

 

| (#) | From | To | Description |
|---|---|---|---|
| | Platform | | |
| **13** | Operations & Management Platform | IoT Device | Operations & Management Platform monitors, operates, maintains, and manage various assets in an IoT system including, but not limited to, Network, IoT Devices, physical/virtual objects in the IoT system's environment, etc. |
| **14** | Operations & Management Platform | Network | Operations & Management Platform communicates with other entities in an IoT system via Network. |
| **15** | Resource Interchange Platform | Service Platform | Resource Interchange Platform supports End-User to gain access to the resources outside of an IoT system providing End-User flexibilities getting the 3rd party/market services. |
| **16** | Resource Interchange Platform | Network | Resource Interchange Platform communicates with other entities in an IoT system via Network. |
| **17** | Network | Network Interface / Access Point | Network is connected to Network Interface / Access Point not only to reach other domains within an IoT system but also to provide the IoT system's entities to gain access to outside of the IoT system. |

#### 9.2.1.1 Domain/entity relationships, and common and representative IoT Entities

From the study and system decomposition of many different, implemented IoT systems, Figure 9-2 provides the identified, representative, and common IoT entities found in most of the IoT systems. Additionally, this figure provides a very high level relationship between Domain and Entity. The concept of Domain is further discussed in the next clause.

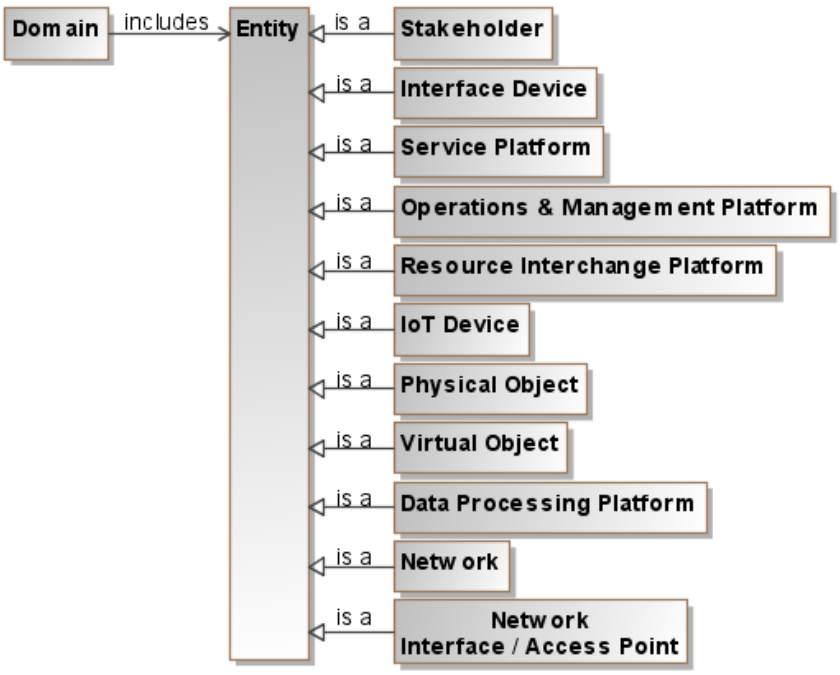


 

**Figure 9-2. Domain and entity relationship, and representative conceptual entities in the IoT systems.**

Table 9-2 below provide the high level descriptions of the entities found in Figure 9-2.

**Table 9-2. Descriptions of the entities in Figure 9-2.**

| Name | Description |
|---|---|
| Domain | Class of entities of similar group and common characteristics |
| Entity | Item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence |
| Stakeholder | Individual, team, organization, or classes thereof, having an interest in the system of interest, and in this conceptual model, the stakeholder are humans or organization operated by humans. |
| Interface Device | a hardware component or system of components that allows a human being to interact with a computer, a telephone system, or other electronic information system |
| Service Platform | Integrated physical/virtual entity system having various applications in order to provide IoT services to End-User. |
| Operations & Management Platform | Integrated physical/virtual entity system which observes, operates, maintains, and manages all IoT systems asset including, but not limited to, networks, IoT environments, IoT Devices, etc. |
| Resource Interchange Platform | Integrated physical/virtual entity system supporting an IoT system's external connectivity with 3rd party suppliers, markets, and temporary stakeholders of the IoT system. |
| IoT Devices | The key IoT devices are sensor, controller, actuator, tag & tag reader, and IoT gateway, and these devices are grouped as the IoT Devices.. |
| Physical Object | a physical entity that is within the purview of an IoT system, that forms an environment for which the IoT system is responsible and whose characteristics, function, status, or behavior is sensed, monitored or controlled by the IoT system |
| Virtual Object | a virtual entity that is within the purview of an IoT system, that forms an environment for which the IoT system is responsible and whose characteristics, function, status, or behavior is sensed, monitored or controlled by the IoT system |
| Data Processing Platform | Integrated physical/virtual entity system that performs various types and levels of data and information processing from the sensor data received from the IoT systems sensors that observe and monitor the IoT system's environment. This system can also produce signals for controllers to manipulate the environment using the actuators in the environment. |
| Network | Various types of networks are used in the IoT systems. All types of networks are represented by this Network entity type. |
| Network Interface / Access Point | This entity type represents various types of devices that allow the connectivity from one network to another network, one domain to another domain, and so on. The devices in this entity type are routers, gateways, etc. |

 

#### 9.2.1.2 Stakeholder in IoT systems

Stakeholder in IoT systems range from individual using an IoT system to those who (or a company) operate the IoT system to the owner of assets involved in the IoT system. Figure 9-3 shows the common and representative IoT systems' stakeholders. Stakeholder takes vital role in the IoT systems from the perspective of system usage, device, network, operation, services, business and related assets such as physical objects.

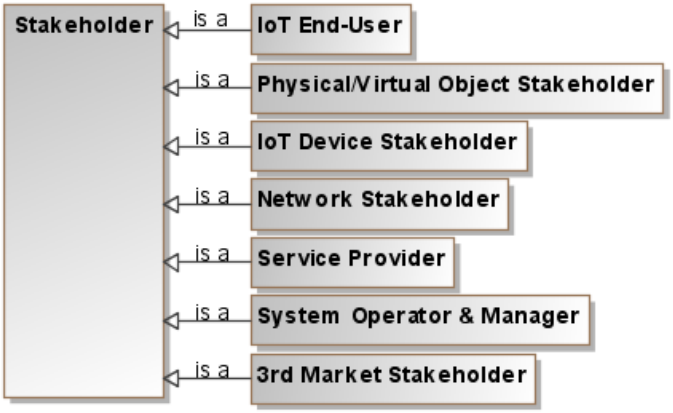


**Figure 9-3. Types of representative IoT Stakeholders identified.**

Table 9-3 provides the description of each stakeholder type which appeared in Figure 9-3.

**Table 9-3. Description of Stakeholder shown in Figure 9-3.**

| Stakeholder | Description |
|---|---|
| IoT End-User | An individual human user or various size of organizations made of from humans, who requests IoT services and who is provided the requested service fulfilled by a service provider in an IoT system. |
| Physical/Virtual Object Stakeholder | A human or a group of human (e.g., organization) having the ownership of the physical and virtual objects in an environment that an IoT system is responsible for. |
| IoT Device Stakeholder | A human or a group of human (e.g., organization) having the ownership of the IoT Devices (e.g., sensors, controllers, actuators, gateways, etc.) that reside in an IoT system. |
| Network Stakeholder | A human or a group of human (e.g., organization) having the ownership of the network(s) within an IoT system. |
| Service Provider | An organization of human who are responsible for providing services, usually by subscription from the IoT End-Users, to the End-Users. |
| System Operator & Manager | An organization of human who are responsible for monitoring, operating, maintaining, and managing various types of assets (e.g., networks, IoT devices, physical/virtual objects in the environment, etc.) of an IoT system. |
| 3rd Market Stakeholder | A human or an organization of human who may join an IoT system temporarily by the request of the permanent stakeholders (e.g., system operators & manager, service provider, or end-user) of the IoT systems to fulfil a specific |

 

| Stakeholder | Description |
|---|---|
| | need or service that may not be available from own IoT system. |

#### 9.2.1.3 Key IoT devices

An IoT-Device is the technical artefacts for bridging the real world of physical objects with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, computation, storage, communicating and processing capabilities [3].

In the IoT systems, there are some basic types of IoT-Devices, and they are identified in Figure 9-4. These devices take vital role in the IoT systems for providing the technological interface for interacting with or gaining information about the physical object, and enhancing the physical object and allowing the latter to be part of the digital world [3]. The IoT-Device can be aggregation of several devices of different types.

Figure 9-4 show the key IoT devices in an IoT system. Table 9-4 provides the description of each IoT Device types.

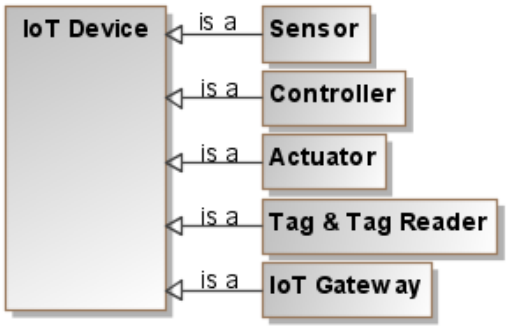


**Figure 9-4. The key IoT devices.**

**Table 9-4. Description of the IoT devices shown in Figure 9-4.**

| IoT Device Name | Description |
|---|---|
| Sensor | Sensor provides the data and/or information about the physical object being monitored. Information in this context ranges from the identity of the physical object to measures of the physical state of the physical object. Sensors can be attached or embedded in the physical structure of the physical object. Or, sensors can be placed in the environment away from the physical object performing non-contact or remote sensing. |
| Controller | Controllers generates control signals for actuators. There are two types of controllers: (1) controllers for physical actuation; and (2) controllers for virtual actuation. |
| Actuator | Actuators manipulate or alter physical objects' state in an IoT system's environment. For example, they can manipulate own sensor or other sensors in its network (e.g., pan, tilt, zoom, etc.) or alter a sensor platform passage (e.g., to |

 

| IoT Device Name | Description |
|---|---|
| | engage thrusters in a satellite) or alter its environment by certain types of actuators. Some actuators can activate or deactivate functionalities of a physical object or a group of physical objects. There are three types of actuators: (1) mechanical actuator; (2) electronic actuator; (3) virtual actuator. |
| Tag & Tag Reader | Tags are used to identify physical objects to which they are attached. The identification process is called 'reading,' and it is carried out by specific Tag Readers. The sole purpose of tag is to facilitate and increase the accuracy of the identification process. |
| IoT Gateway | IoT Gateway is a forwarding device enabling the connections between the sensing or actuating subsystem in the real environment to the other subsystems in the IoT system. |

### 9.2.2 Domain-based reference model of IoT systems

#### 9.2.2.1 Common domains of IoT systems for developing the RM

In this standard, after examining various kinds of deployed IoT systems and developing IoT Conceptual Model (CM) through IoT system decomposition, common and representative domains of IoT systems are identified by focusing on the IoT systems' stakeholders and hardware/software. Using these common and representative domain provides an effective and representative Reference Model (RM) of the IoT systems for the various purposes and uses of the RM.

Based on the common entities listed in Figure 9-2 and the CM of IoT system in Figure 9-1, the IoT Reference Model's domains are derived as shown in Table 9-5.

**Table 9-5. Derivation of IoT Reference Model domains.**

| Category | Entity or Entity Type | IoT Reference Model Domains |
|---|---|---|
| Stakeholder | IoT End-User | End-User Domain (EUD) |
| Stakeholder | Service Platform | Service Providers Domain (SPD) |
| Stakeholder | Operations & Management Platform | Operations & Management Domain (OMD) |
| Stakeholder | Resource Interchange Platform | Resource Interchange Domain (RID) |
| Hardware/Software | IoT Devices | Sensing & Actuating Domain (SAD) |
| Hardware/Software | Physical Object and Virtual Object | Object Domain (OBD) |

Each identified domain is mutually exclusive from the other domains, Hardware (i.e. physical entities) and software (i.e. virtual entities) appear in the domains other than the OBD and the SAD. These hardware and software in the domains other than the OBD and the SAD support functions and capability of the domain to which they belong, and they do not interact (e.g., sense and actuate) with an environment for which an IoT system is responsible and monitoring.

 

The IoT system's environment is mainly formed by the OBD, but certain situations, part of the SAD entities can be allotted as a part of the environment.

Table 9-6 provides the description of the IoT RM domains.

**Table 9-6. Description of the Reference Model domains of IoT systems.**

| RM Domain Name | Stakeholder/actor & Description |
|---|---|
| End-User domain (EUD) | End-users are the stakeholder/actor of the EUD. Various types of end-users exist in IoT, e.g., an individual person, family (e.g., home), building, industrial or governmental organizations, etc. |
| Service providers domain (SPD) | Service providers are the stakeholder/actor of the SPD. Organizations providing services to the end-users through IoT system(s). |
| Operations & management domain (OMD) | System operators and managers are the stakeholders/actors of the OMD. The operators and managers maintaining overall health of IoT system(s). |
| Resource interchange domain (RID) | Non-permanent/temporary organizations that participate in an IoT system voluntarily or involuntarily are the stakeholders of the RID. These organizations range from a coffee shop to utility companies to governmental organizations. |
| Sensing & actuating domain (SAD) | The stakeholder is an owner or owners of the SAD, yet, this stakeholder may not show up as an entity in the SAD. No human type actor is expected in the SAD. The SAD consists of sensors (including sensor networks), controllers, actuators, and tag readers. It could have data/processing platform. It also has various kinds of virtual objects supporting the entities in the SAD. Thus, actors in the SAD can be physical entities (e.g., sensors, controllers, actuators, computers, etc.) and virtual entities (e.g., software). |
| Object domain (OBD) | The stakeholder is an owner or owners of the OBD, yet, this stakeholder may not show up as an entity in the OBD. A person or persons can be one of the objects in the OBD. The OBD forms the environment for which an IoT system is responsible; thus, the OBD can have all types of physical and virtual entities. Actors in the OBD can be physical entities and virtual entities in the IoT system's environment. |

The Reference Model (RM) of the IoT systems supports planning and organization of the diverse, expanding collection of interconnected networks. Interconnected networks provide communication connectivity (including data link which can be a point-to-point link) in IoT systems (e.g., inter- and intra-domain), between IoT systems, and with other systems and organizations. The connected networks should maintain an interoperability from one network to another.

The network mainly provide pathways for communication and data/information exchange. Thus, the key role of the networks is to support and provide an IoT system's required networks for communication and data/information exchange activities and interactions. Types of the activities and interactions between two entities, between two domains, or between two IoT systems determine their relationships between the entities, the domains, and the IoT systems, respectively.

 

#### 9.2.2.2 Reference models of the common domains

##### 9.2.2.2.1 Reference model of End-User Domain and its interaction with other domains

The EUD interacts with other domains in the IoT systems as shown in Figure 9-5. The interacting domains are SPD, OBD, SAD, OMD, and RID. Table 9-7 provides the representative interactions of the EUD with other interacting domains.

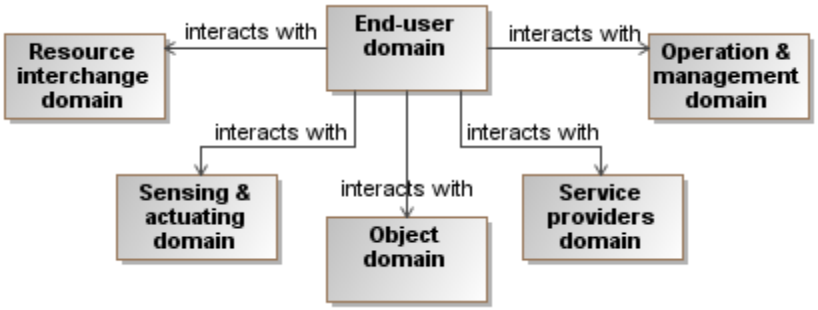


**Figure 9-5. End-user domain interacts with other IoT domains.**

**Table 9-7. Representative EUD interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| End-user Domain (EUD) | requests services from | Service providers domain |
| | can request or access data/information from | Sensing & actuating domain |
| | can request or access data/information from | Object domain |
| | reports issues to | Operations & management domain |
| | can request service from other IoT systems through | Resource interchange domain |

##### 9.2.2.2.2 Reference model of Object Domain and its interaction with other domains

The OBD interacts with other domains in the IoT systems as shown in Figure 9-6. The interacting domains are EUD and SAD. Table 9-8 provides the representative interactions of the OBD with other interacting domains.

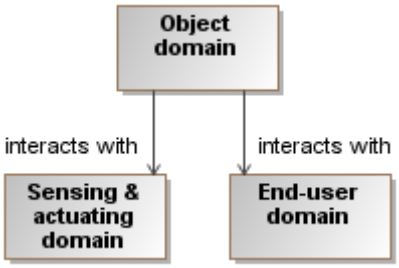


**Figure 9-6. Object domain interacts with other IoT domains.**

**Table 9-8. Representative OBD interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| Object Domain (OBD) | when allowed, provides data/information to | End-user domain |
| | provides data/information to, feedbacks upon; and command/control signals to | Sensing & actuating domain |

#### 9.2.2.2.3 Reference model of Sensing & Actuating Domain and its interaction with other domains

The SAD interacts with other domains in the IoT systems as shown in Figure 9-7. The interacting domains are EUD, OBD, SAD, OMD, and RID. Table 9-9 provides the representative interactions of the SAD with other interacting domains.

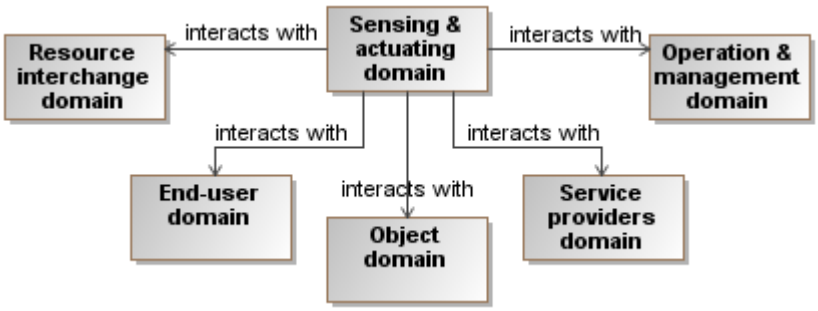


**Figure 9-7. Sensing & actuating domain interacts with other IoT domains.**

**Table 9-9. Representative SAD interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| Sensing & Actuating Domain (SAD) | sends data & information requested to | Service providers domain |
| | when allowed, provides data/information to | End-user domain |
| | monitors, collects data/information from; and send command/control signals to | Object domain |
| | provides entity status to | Operations & management domain |
| | when allowed, provides data/information to | Resource interchange domain |

#### 9.2.2.2.4 Reference model of Service Provider Domain and its interaction with other domains

The SPD interacts with other domains in the IoT systems as shown in Figure 9-8. The interacting domains are EUD, SAD, OMD, and RID. Table 9-10 provides the representative interactions of the SPD with other interacting domains.

 

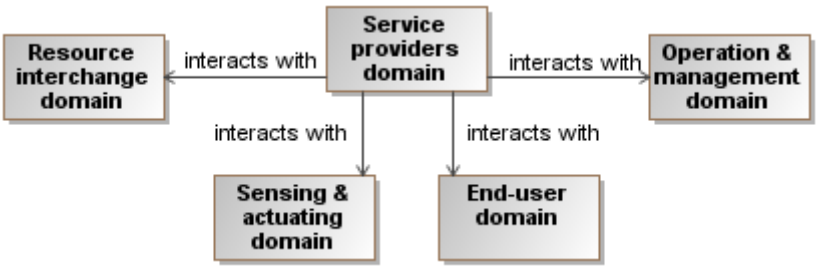


**Figure 9-8. Service providers domain interacts with other IoT domains.**

**Table 9-10. Representative SPD interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| Service Providers Domain (SPD) | provides services to | End-user domain |
| | inquires data & information per service request from | Sensing & actuating domain |
| | reports issues to | Operations & management domain |
| | can request data/info through | Resource interchange domain |

#### 9.2.2.2.5 Reference model of Operations and Management Domain and its interaction with other domains

The OMD interacts with other domains in the IoT systems as shown in Figure 9-9. The interacting domains are EUD, SAD, SPD and RID. Table 9-11 provides the representative interactions of the OMD with other interacting domains.

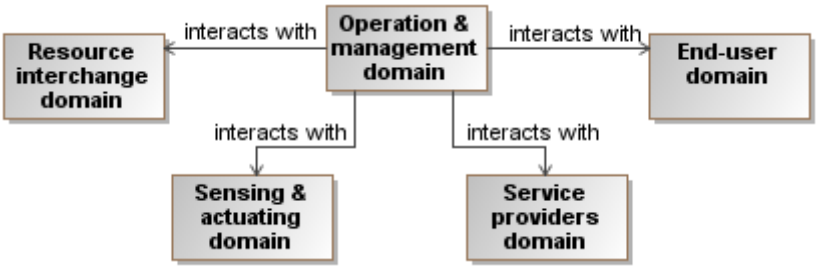


**Figure 9-9. Operations & management domain interacts with other IoT domains.**

**Table 9-11. Representative SPD interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| Operations & management domain | resolves issues for | Service providers domain |
| | operates and manages | Sensing & actuating domain |
| | resolves issues for | End-user |
| | interacts with outside systems and reports status, when allowed, through | Resource interchange domain |

 

#### 9.2.2.2.6 Reference model of Resource Interchange Domain and its interaction with other domains

The RID interacts with other domains in the IoT systems as shown in Figure 9-10. The interacting domains are EUD, SAD, SPD and OMD. Table 9-12 provides the representative interactions of the RID with other interacting domains.

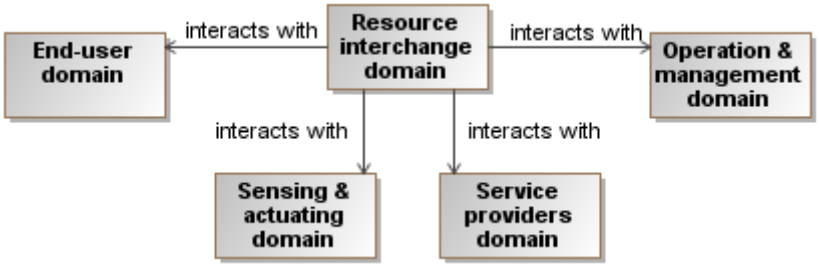


**Figure 9-10. Resource interchange domain interacts with other IoT domains.**

**Table 9-12. Representative RID interaction descriptions.**

| Domain A | Interaction descriptions | Domain B |
|---|---|---|
| Resource Interchange Domain (RID) | fulfils the requests from | Service providers domain |
| | requests data/info from | Sensing & actuating domain |
| | fulfils the requests from | End-user domain |
| | relays incoming requests from outside systems to | Operations & management domain |

### 9.2.3 Composite reference model of IoT systems

Combining the individual domain Reference Model in Clause 9.2.2, a composite IoT RM is produced in Figure 9-11, showing the six high-level IoT Domains. Figure 9-11 also shows the representative interactions between the domains, communications and data/information flows by arrows, and interfaces between domains by connecting points of an arrow between the domains.

 

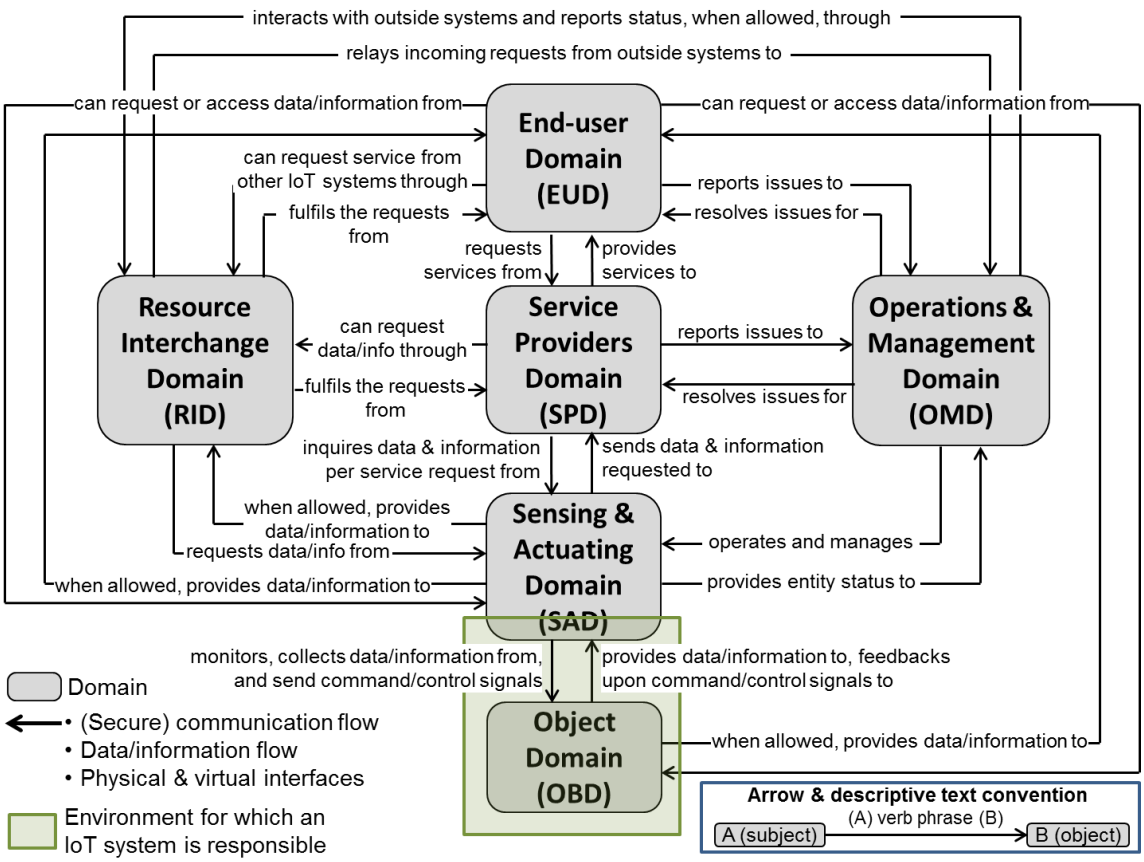


**Figure 9-11. Reference Model (RM) of IoT systems by high-level domains.**

The Reference Model shown in Figure 9-11 can be used to describe use cases. A use case is a story, told in structured and detailed steps, about how actors work together to reach a goal. A use case would be represented in the Reference Model by a path connecting several stakeholders/actors across multiple domains. Using the IoT RM in Figure 9-11, an example use case for a high-rise building with 200 apartment units is presented in Annex A of this standard to illustrate relationships, activities, behaviours, and interfaces between the domains.

The networks and communication connectivity is accomplished by wire-line and wireless connections. There are various types of networks (e.g., local area network, cellular network, sensor network, control network, home area network, etc.) and communication connectivity (e.g., a point-to-point communication link, etc.). Thus, various network/communication components and protocols make up an IoT system's network/communication infrastructure.

## 9.3 High-level, overall IoT infrastructure reference model

In Figure 9-12, the IoT reference model (RM) from the network view is presented. In this figure, four levels of IoT network infrastructure are identified: (a) Level 1 – networks supporting entities in a domain, e.g., intra-domain; (b) Level 2 – networks supporting entities between two or more domains, e.g., inter-domain; (c) Level 3 – networks supporting between two IoT systems and/or supporting an IoT system and organizations outside of the IoT system, and (d) Level 4 – networks supporting an IoT system to connect to an IoT platform (e.g., nation-wide, province-wide, city-wide, or corporation-wide). Figure 9-12 also provides a conceptual big picture of a high-level, overall IoT infrastructure.

 

For the connectivity to the Level 3 and Level 4 network infrastructure, the resource interchange domain (RID) provides the network connectivity for communication and data/information exchange with an IoT system. Because Level 3 and Level 4 network infrastructures are not in the scope of this standard document, the focus is given to Level 1 and Level 2 network infrastructures which are intra- and inter-domain network connectivity, respectively, in an IoT system.

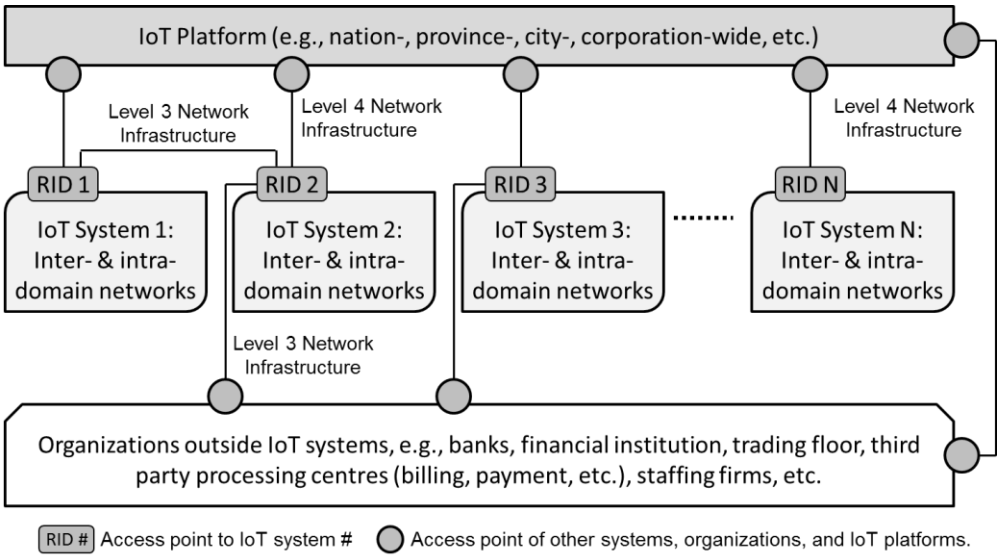


**Figure 9-12. Reference model (RM), a big picture of a high-level, overall IoT Infrastructure.**

## 9.4 IoT Reference architecture (IoT RM) views

The IoT RA is described in the following five reference architecture views:

a) System Reference Architecture (SRA) view;

b) Communications Reference Architecture (CRA) view;

c) Information Reference Architecture (IRA) view;

d) Usage view, and

e) Functional view

The IoT RAs becomes an application- or service-specific system architecture or a target system architecture (e.g., agricultural system, environmental system, smart grid system, smart home/building, smart city, etc.) when the RA is tailored to a specific set of requirements.

Furthering the IoT Conceptual Reference Diagram shown in Figure 9-11 into the IoT RAs, the additional entities in each domain are introduced and described. Interfaces connecting the entities between domains, e.g., inter-domain interfaces, and the entities within a domain, e.g., intra-domain interfaces, are also described.

Figure 9-13 below illustrates a method or convention to describe the IoT RA in this international standard. The entities shown in the system level can be considered as domain-level entities connected by interfaces designated by E1 to E4. The entities shown in the subsystem level are considered the

 

entities within a domain connected by the inter-domain interfaces B1 to B6. All entities and interfaces, both in system level and in subsystem level, will be fully described for the IoT RA.

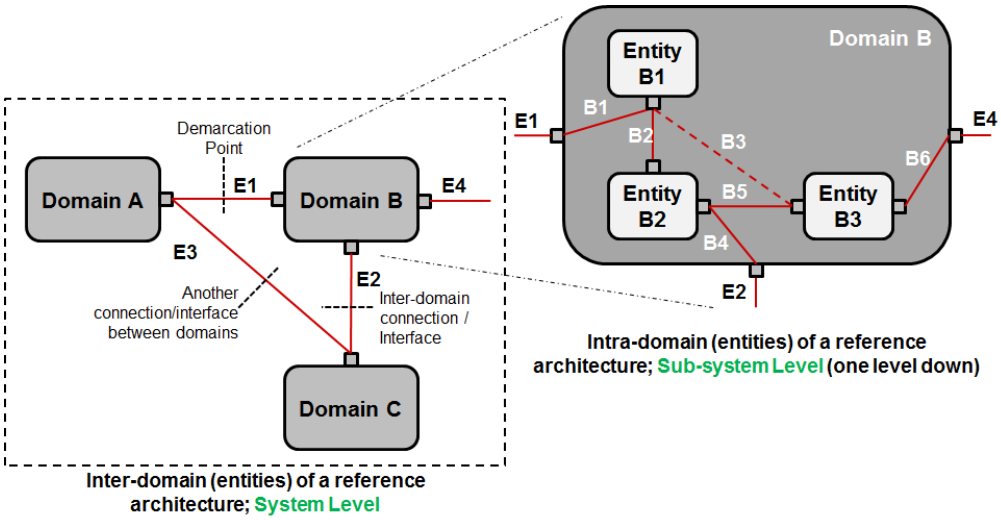


**Figure 9-13. Reference architecture description convention and methodology.**

### 9.4.1 IoT RA Systems view

In Figure 9-14, IoT RA Systems view is shown along with all the entities involved in each function domain and the interfaces among them from the viewpoint of system function. It is based on IoT conceptual model.

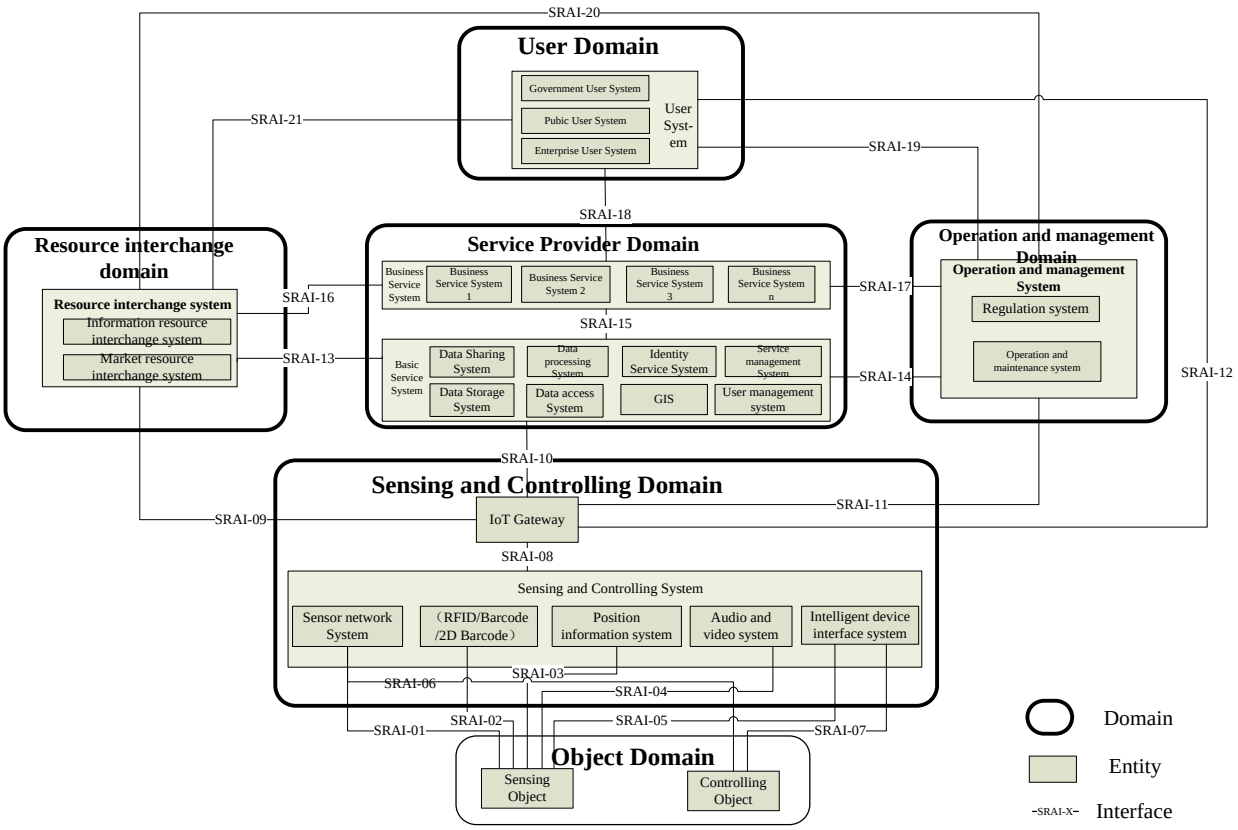


 

**Figure 9-14. IoT RA Systems view.**

The entity descriptions are presented in Table 9-13.

**Table 9-13. IoT RA Systems entity descriptions.**

| IoT Domains | Domain Entities | Entity descriptions |
|---|---|---|
| User Domain | User system | User system is the interface system to support user access to the Internet of things, and to use of service of the Internet of things. Form the general viewpoint it can be classified as government user system, enterprise user system, the public user system, etc. |
| Object Domain | Sensing Objects | Sensing objects are physical entities those related to IoT application, interested by users, and can be acquired information by sensing equipment. |
| | Controlling Objects | Controlling objects are physical entities those related to IoT application, interested by users, and can be controlled by controlling equipment. |
| Sensing and controlling Domain | IoT Gateway | IoT gateway is entity to support controlling system connect with other systems, and to manage sensing and controlling Domain. IoT gateway can provide the function of protocol conversion, address mapping, data processing, information fusion, certification, equipment management, etc. IoT gateway can be independent equipment; also can be integrated with other with sensing and controlling devices. |
| | Sensing and Controlling System | Sensing and Controlling system can acquire information and perform operations on related object through different sensing and controlling function unit. It can achieve a certain local information processing and fusion. Sensing and controlling system can include sensor network system, label automatic identification system, position information system, audio and video system and intelligent device interface system. The systems can sense and control objects independently or collaboratively. |
| Service Provider | Business service system | Business service system provides IoT business service according to the requirement of particular |

 

| IoT Domains | Domain Entities | Entity descriptions |
|---|---|---|
| Domain | | user. Business service may include information query, analysis and comparison, alarm warning, operation control, joint coordination, etc. |
| | Basic service system | Basic service system provides foundational support to business service system. Foundation service may include data access, data processing, data fusion, data storage, identity resolution, geographic information service and user management, inventory management, etc. |
| Operation and Management Domain | Operation and Management system | Operation and Management system is to guarantee equipment and systems operate safely and reliably. It may include system access management, system security management, system operation and system maintenance, etc. |
| | Regulation system | Regulation system is to guarantee IoT application system in line with the relevant laws and regulations. It provides inquiry, supervision and execution of the relevant laws and regulations. |
| Resource interchange Domain | Information Resource interchange system | Information Resource interchange system is to provide or obtain information Resource to meet the service requirements of particular user. It mainly achieves exchange and sharing of resource information between different systems. |
| | Market Resource interchange system | Market Resource interchange system is to provide effective support to IoT application system. It may achieve the exchange of information flow, service flow, and capital flow. |

The IoT SRA interface descriptions/definitions are listed in Table 9-14 below according to the interface numbers found in Figure 9-14 above.

**Table 9-14. IoT RA Systems interface descriptions/definitions.**

| SRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| SRAI-01 | Sensing Object | Sensor Network System | The interface specified relationship between sensing object and sensor networks. Sensor node acquired physical, chemical, biological properties of sensing object through this interface. This interface is not data interface but physical, chemical, biological |

 

| SRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| | | | relationship. |
| SRAI-02 | Sensing Object | label automatic identificatio n system | The interface specified relationship between sensing object and label automatic identification system. The tag reader can automatically read and write the content related to particular objects through the label attached on the target object. This interface is not data interface but the binding relationship between label and object. Existing label system generally includes RFID, bar code and QR Code, etc. |
| SRAI-03 | Sensing Object | Position information system | The interface specified relationship between sensing object and position information system. Spatial position information of object can be obtained through the binding between position information terminal and the object. The interface is non-data interface, but to achieve the binding relationship between position information terminal and the object. |
| SRAI-04 | Sensing Object | audio and video system | The interface specified relationship between sensing object and audio and video system. Audio and video system acquires audio, image, video and other non-structured data of sensing object through this interface. The interface is non-data interface, but to realize development relationship between sensing object and audio and video terminal. |
| SRAI-05 | Sensing Object | intelligent device interface system | The interface specified relationship between sensing object and intelligent equipment interface system. The intelligent equipment interface system acquires parameter, state and basic attribute information of object through this interface. This interface is data interface, including serial bus, parallel bus and USB, etc. |
| SRAI-06 | Controlling Object | Sensor Network System | The interface specified relationship between controlling object and sensor network system. The execution unit of sensor network can obtain the running state of the controlled object through this interface, and can realize the operation to controlled object. The interface is data interface, including serial bus, parallel bus and USB, etc. |

 

| SRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| SRAI-07 | Controlling Object | intelligent device interface system | The interface specified relationship between controlling object and intelligent device interface system. Intelligent device interface system can the running state of the controlled object through this interface, and can realize the operation to controlled object. The interface is data interface, including serial bus, parallel bus and USB, etc. |
| SRAI-08 | Sensing and Controlling System | IoT Gateway | The interface specified relationship between sensing and controlling system and IoT gateway. IoT gateway can adapt, connect to the different sensing and controlling system through this interface, and can realize information interaction and system management, etc. The interface is data interface, including short distance wireless communication network, Ethernet, WLAN, mobile communication network, etc. |
| SRAI-09 | IoT Gateway | Resource interchange system | The interface specified relationship between IoT gateway and resource interexchange system. Resource interexchange system can connect IoT gateway through this interface, and can realize information sharing and interacting under the permissions. The interface is data interface, including internet, Ethernet, WLAN, etc. |
| SRAI-10 | IoT Gateway | Basic service system | The interface specified relationship between IoT gateway and Basic service system. Basic service system can connect IoT gateway through this interface, and can realize information sharing and interacting under the permissions. The information mainly includes sensing object information and control command, etc. The interface is data interface, including internet, Ethernet, WLAN, etc. |
| SRAI-11 | IoT Gateway | Operation and Managemen t system | The interface specified relationship between IoT gateway and operation and management system. Operation and Management system can connect IoT gateway through this interface, and can realize information sharing and interacting under the permissions. The information mainly includes operation and management state information, and system and equipment control command, etc. The interface is data interface, including internet, Ethernet, WLAN, etc. |

 

| SRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| SRAI-12 | IoT Gateway | User system | The interface specified relationship between IoT gateway and user system. User system can interchange information with IoT gateway through this interface, and can obtain local service of Sensing and Controlling Domain. The interface is data interface, including Bluetooth, WLAN and serial port, etc. |
| SRAI-13 | Basic service system | Resource interchange system | The interface specified relationship between Basic service system and resource interchange system. Basic service system can interchange information with other system through this interface. The information mainly includes necessary resources to provide integrated IoT services.<br><br>The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-14 | Basic service system | Operation and Managemen t system | The interface specified relationship between Basic service system and Operation and Management system. Operation and Management system can monitor and control the running state of the basic service system through this interface, and can ensure the operation of basic service system compliance with relevant laws and regulations. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-15 | Basic service system | Business service system | The interface specified relationship between basic service system and business service system. Business service system can obtain the foundation services provided by the basic service system, mainly including data storage, data processing, identification analytical service, geographic information services. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-16 | Business service system | Resource interchange system | The interface specified relationship between business service system and resource interchange system. Business service system can achieve resources interexchange with other related system through this interface, such as market resources, payment information etc. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |

 

| SRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| SRAI-17 | Operation and Manageme nt system | Business service system | The interface specified relationship between Operation and Management system and business service system. Operation and Management system can monitor and control the running state of the service system through this interface, and ensure the operation of Business service system compliance with relevant laws and regulations. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-18 | Business service system | User system | The interface specified relationship between business service system and user system. User system can obtain the relevant IoT service through this interface. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-19 | User system | Operation and Managemen t system | The interface specified relationship between user system and Operation and Management system. Operation and Management system can monitor and control the running state of the user system through this interface, and ensure the operation of user system compliance with relevant laws and regulations. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-20 | Resource interchang e system | Operation and Managemen t system | The interface specified relationship between resource interchange system and Operation and Management system. Operation and Management system can monitor and control the running state of the resource interchange system through this interface, and ensure the operation of resource interchange system compliance with relevant laws and regulations. The interface is data interface, including internet, VPN, Ethernet and WLAN, etc. |
| SRAI-21 | Resource interchang e system | User system | The interface specified relationship between resource interchange system and user system. User system can interchange resources with other systems through this interface. The interface is data interface, including internet, mobile communication network, etc. |

 

### 9.4.2 IoT RA Communications technology view

Communications Technology view, utilized by the IoT system linking the various domains for data/information transmission and reception.

From the interconnection of each entity of IoT system view, the IoT communications reference architecture prescribe the communication relation of each entity of IoT system, to provide the communication support and guarantee for the realization of the IoT information collection, information aggregation, information processing, information resource sharing, information service and system operation and control.

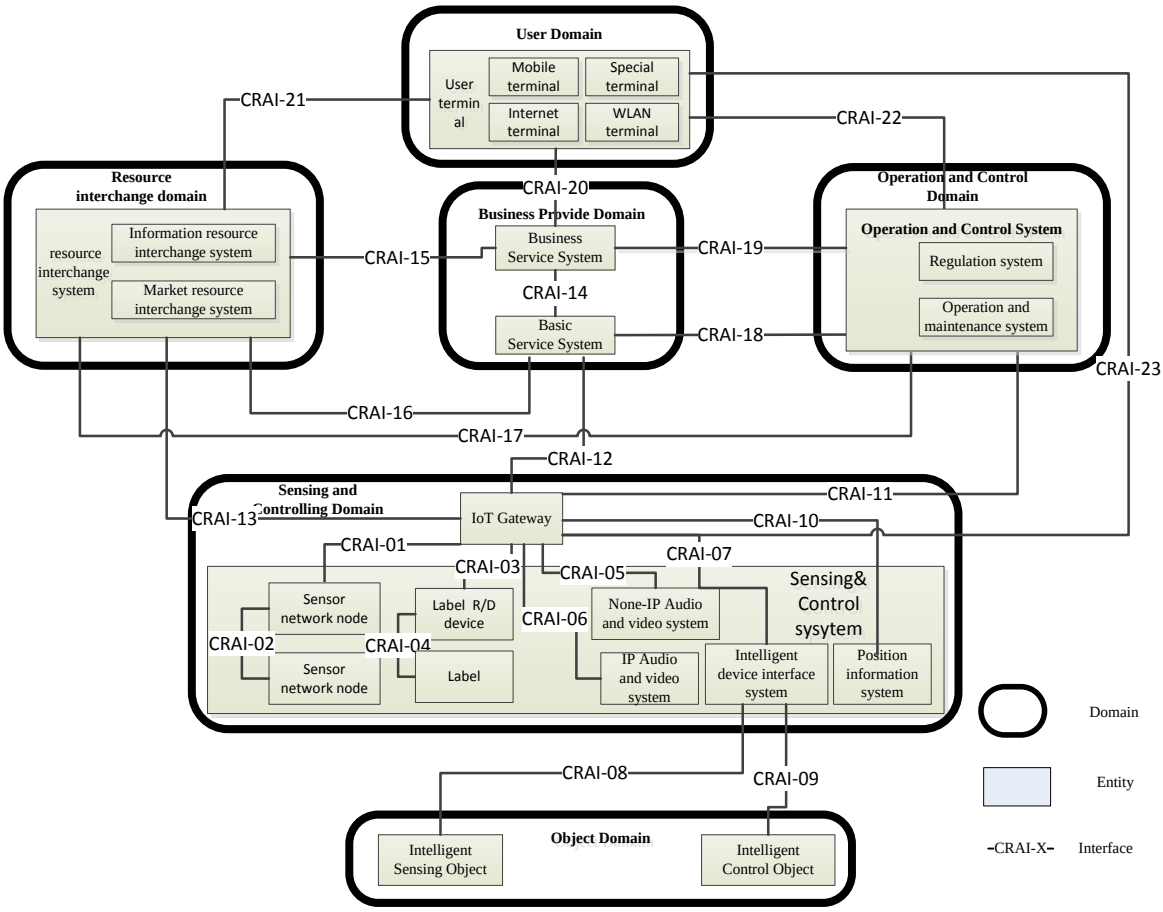


**Figure 9-15. IoT RA Communications technology view.**

The entities related to the internet of things communications reference architecture as shown in Table 9-15.

**Table 9-15. IoT RA Communication technology entity descriptions.**

| IoT Domains | Domain Entities | Entity descriptions |
|---|---|---|
| User domain | User terminal | The user terminal is the interactive device to support the user access and use IoT services. From communication access method view, the user terminal includes mobile terminal, internet terminal, iWLAN terminal and special |

 

| IoT Domains | Domain Entities | | Entity descriptions |
|---|---|---|---|
| | | | terminal. Different Users system includes different user terminal. |
| Object domain | Intelligent sensing object | | Intelligent sensing object is a physical entity relating to the IoT application, users interesting, and which can obtain relevant information through digital or analogue interface. The sensing objects have direct communication connection with intelligent interface, and have none-data communication interface relation with other sensing control system. |
| | Intelligent control object | | Intelligent control object is a physical entity relating to the IoT application, users interesting, and which can obtain relevant information through digital interface. The control objects have direct communication connection with intelligent interface, and have none-data communication interface relation with other sensing control system. |
| Sensing and controlling domain | IoT gateway | | From the perspective of network communication, IoT gateway mainly realizes the connection between sensing control system and other IoT service system, including the protocol transition, address mapping, security authentication, network management and other functions. At the same time, as the interaction centre of service related sensing and control system, the IoT gateway can coordinate and manage different sensing control system. When the sensing control system uses the IP address, IoT gateway can be designed as an application gateway logic device. |
| | Sensing and controlling system | Sensor network node | Sensor network nodes are generic terms of various function units in sensor network, including sensor node, sensor network gateway etc., it mainly complete the information collection and controlling, information processing, network communication and network management functions. |
| | | Label R/D device | Label R/D device is electronic equipment to access data and (or) write data to label. |
| | | Label | The label has information storage and read/write functions, used to identify and describe the characteristics of an object, mainly include RFID, bar code, two-dimensional code label. |
| | | IP audio and video system | Based on IP network device to get audio and video information of object. |
| | | None-IP audio and video system | Based on none-IP network device to get audio and video information of object. |

 

| IoT Domains | Domain Entities | | Entity descriptions |
|---|---|---|---|
| | | Intelligent device interface system | Intelligent device interface system is used to connect intelligent sensing object and control object, and implement data interaction. It provides network communication, data processing and protocol transition function. |
| | | Position informatio n system | Position information system can obtain sensing object position information based on the locating technology of Beidou system, GPS system or mobile communication network, and can realize the information interaction |
| Service provider domain | Basic service system | | Basic service system is a communication network to support interconnection and interworking between the entities in the basic service system and interaction with other outside entities. Generally it adopts local area network construction and implement interconnection and interworking with outside network according to some level of security. |
| | Business service system | | Business service system network is a communication network to support interconnection and interworking between the entities in the business service system and interaction with other outside entities. It should support multi-communization access method for different terminals. |
| Operation and control domain | Operation and maintenance system | | Operation and maintenance system is a communication network to support interconnection and interworking between the entities in the operation and maintenance system and interaction with other outside entities. Generally it adopts local area network construction and implement interconnection and interworking with outside network according to some level of security. |
| | Regulation system | | Regulation system is a communication network to support interconnection and interworking between the entities in the regulation system and interaction with other outside entities. Generally it adopts local area network construction and implement interconnection and interworking with outside network according to some level of security. |
| Resource interchange domain | Resource interchange system | | Resource interchange system is a communication network to support interconnection and interworking between the entities in the resource interchange system and interaction with other outside entities. Resource interchange system also provide the interconnection and interworking between the IoT application system with other IoT application systems or information resource network. |

Table 9-16 provides the interface descriptions for IoT RA Communication technology view.

**Table 9-16. IoT RA Communication technology view interface descriptions/definitions.**

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| CRAI-01 | Sensor network node | IoT gateway | This interface regulates communication relation between sensor network node and the IoT gateway. It can adopt the wireless or wired communication interface according to different IoT service requirement. The physical layer of wireless communication interface mode may adopt IEEE 802.15.4-2006, GB/T 15629.15-2010 protocol; media access control layer may adopt IEEE802.15.4-2006, GB/T 15629.15-2010 protocol; network transmission layer may adopt Zigbee Specification 2005, IETF 6LoWPAN protocol. This interface can generally support the data transmission rate from a few bytes to several megabytes. |
| CRAI-02 | Sensor network node | Sensor network node | This interface regulates communication relation between sensor network nodes. According to the requirements of the interaction between different nodes, the physical layer and media access control layer may adopt IEEE 802.15.4-2006, GB/T 15629.15-2010 protocol; network transmission protocol may be used Zigbee Specification 2005, Bluetooth, IWA-PA and ISA100.11a protocols. This interface can generally support the data transmission rate from a few bytes to several megabytes. |
| CRAI-03 | Label R/D device | IoT gateway | This interface regulates communication relation between label R/D device and IoT gateway. Through this interface, the label R/D device transmit the data to IoT gateway, data transmission mode may support synchronous mode, asynchronous mode and batch mode. Communication method of this interface is divided into the cable connection and wireless connection. The cable connection may use serial communication (such as RS232, RS485 or USB) or Ethernet communication; wireless connection may use IEEE802.11 protocol, mobile communication networks or Bluetooth technology and multi-kinds of short distance wireless communication technology. |
| CRAI-04 | Label R/D device | Label | This interface regulates communication relation between label R/D device and label. Labels can be divided into RFID and bar code labels. Bar code labels reading and writing interface obtain the label information by scan mode; RFID connect with label R/D device through the air interface. Label R/D device sends commands to the label, and receive the respond from label. RFID label read-write interface protocol may adopt ISO14443, ISO15693, ISO18000 series standards. |
| CRAI-05 | IoT gateway | IP audio and video device | This interface regulates communication relation between IoT gateway and IP audio and video device. IoT gateway acquires IP audio and video device monitoring information and manage IP audio and video device via IP network. This interface can be wired interface or wireless interface. Wired communication mode may be based on xDSL, LAN access, PON access and so on; the wireless communication mode may be based on WLAN |

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| | | | technique, mobile communication network or special wireless transceiver device. |
| CRAI-06 | IoT gateway | None-IP audio and video device | This interface regulates communication relation between IoT gateway and none-IP audio and video device. IoT gateway acquires none-IP audio and video device monitoring information and manage IP audio and video device via none-IP network. This interface may be cable interface or wireless interface. The cable connection can use coaxial cable connecting wire, wireless connection may use microwave wireless connection technology. |
| CRAI-07 | IoT gateway | Intelligent device interface system | This interface regulates communication relation between IoT gateway and intelligent device interface system.<br>IoT gateway exchanges the information with intelligent device interface system through the wired or wireless communication mode. The wireless communication mode may adopt mobile communication network and short distance wireless communication technique; the wired communication mode may use Ethernet, serial communication and bus communication. Wireless transmission may use IEEE802.11 protocol, ZigBee protocol or Bluetooth protocol; wire transmission can adopt IEEE802.3 protocol and serial communication protocol (such as RS232, RS485, USB, IEEE1394) or the CAN bus communication protocol. |
| CRAI-08 | Intelligent device interface system | Intelligent sensing object | This interface regulates communication relation between Intelligent sensing object and intelligent device interface system. The intelligent device interface system get the sensing object information through this interface. This interface can be divided into analogue signal interface and digital signal interface, and analogue signal interface represent the current sensing information through the continuous change of the voltage or electricity, and digital interface represents the current sensing information through the 0/1 digital value. |
| CRAI-09 | Intelligent device interface system | Intelligent control object | This interface regulates communication relation between Intelligent control object and intelligent device interface system. The intelligent device interface system transmits control information through this interface. The communication mode of the interface may be bus communication or serial communication, and CAN bus communication may adopt CAN, SPI, I2C, USB protocol; serial communication may adopt RS-232 or RS-485 etc. |
| CRAI-10 | IoT gateway | Position informati on system | This interface regulates communication relation between position information system and IoT gateway. According to user requirements for obtaining position information in real time or periodically, the communication mode of the interface may be mobile communication networks, Internet, LAN or special |

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| | | | communication network, the communication network should guarantee privacy requirement of position information. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol. |
| CRAI-11 | Operation and maintenance system | IoT gateway | This interface regulates communication relation between operation and maintenance system and IoT gateway. This interface is used to transfer state information and control information related to operation and maintenance system. It may adopt mobile communication network, Internet, LAN or special communication network. The underlying link protocol of network communication may be using IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may adopt HTTP, HTTPS protocol. |
| CRAI-12 | Basic service system | IoT gateway | This interface regulates communication relation between basic service system and IoT gateway. According to the real-time and accuracy requirement of IoT service, this interface may adopt mobile communication network, Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may use TCP/IP protocol, the upper application protocol may adopt HTTP, FTP, and streaming media transmission protocol. |
| CRAI-13 | Resource interchange system | IoT gateway | This interface regulates communication relation between resource interchange system and IoT gateway. According to the real-time and accuracy requirement of IoT service, this interface may adopt mobile communication network, Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may use TCP/IP protocol, the upper application protocol may adopt HTTP, FTP, and streaming media transmission protocol. |
| CRAI-14 | Business service system | Basic service system | This interface regulates communication relation between business service system and basic service system. This interface can be internal interface of IoT system, or be open API provided by basic service system for personalized business development for the different industries and applications. The communication connection of this interface may be Internet or LAN. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol and the upper application protocol may use HTTP, FTP or Telnet protocol according to the application and function requirement. |
| CRAI-15 | Resource | Business | This interface regulates communication relation between |

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| | interchange system | service system | resource interchange system and business service system. According to the real-time and reliability requirement for resource request and exchanging function of the information resource and the market information from business service system, this interface may adopt Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may adopt HTTP, FTP, streaming media protocol, mail protocol or e-bank protocol. |
| CRAI-16 | Resource interchange system | Basic service system | This interface regulates communication relation between resource interchange system and basic service system. According to the real-time and reliability requirement for resource request and exchanging function of the information resource and the market information from basic service system, this interface may adopt Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may adopt HTTP, FTP, streaming media protocol, mail protocol or e-bank protocol. |
| CRAI-17 | Resource interchange system | Operation and maintenance system | This interface regulates communication relation between resource interchange system and operation and maintenance system. According to the operation and maintenance, system management, and regulatory control function requirement of operation and maintenance system, this interface may adopt Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt HTTP, FTP, Telnet or mail protocol. |
| CRAI-18 | Basic service system | Operation and maintenance system | This interface regulates communication relation between basic service system and operation and maintenance system. According to the operation and maintenance, system management, and regulatory control function requirement of basic service system, this interface may adopt mobile communication network, Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt HTTP, FTP, Telnet or mail protocol. |
| CRAI-19 | Business service system | Operation and maintenance | This interface regulates communication relation between business service system and operation and maintenance system. According to the operation and maintenance, system management, and regulatory control function requirement of |

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| | | system | business service system, this interface may adopt mobile communication network, Internet, LAN or special communication network. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt HTTP, FTP, Telnet or mail protocol. |
| CRAI-20 | User terminal | Business service system | This interface regulates communication relation between business service system and user terminal. This interface may adopt mobile communication network, Internet, LAN or special communication network to support different user terminal types, and the user terminal can access to IoT gateway by B/S or C/S method. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may use HTTP, FTP, Telnet, mail protocol, stream media protocol and e-bank protocol. |
| CRAI-21 | User terminal | Resource interchange system | This interface regulates communication relation between user terminal and resource interchange system. This interface may adopt mobile communication network, Internet, LAN or special communication network to support different user terminal types, and the user terminal can access to IoT gateway by B/S or C/S method. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may use HTTP, FTP, Telnet, mail protocol, stream media protocol and e-bank protocol. |
| CRAI-22 | User terminal | Operation and maintenance system | This interface regulates communication relation between User terminal and operation and maintenance system. This interface may adopt mobile communication network, Internet, LAN or special communication network to support different user terminal types, and the user terminal can access to IoT gateway by B/S or C/S method. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may use HTTP, FTP, Telnet and stream media protocol. |
| CRAI-23 | User terminal | IoT gateway | This interface regulates communication relation between user terminal and IoT gateway. This interface may adopt mobile communication network, Internet, LAN or special communication network to support different user terminal types, and the user terminal can access to IoT gateway by B/S or C/S method. The underlying link protocol of network communication may adopt IEEE802.3 or IEEE802.11 protocol, |

 

| Interface | Entity 1 | Entity 2 | Interface Description |
|---|---|---|---|
| | | | the network transport layer protocol may adopt TCP/IP protocol, and the upper application protocol may use HTTP, FTP, Telnet and stream media protocol. |

### 9.4.3 IoT RA Information technology view

Information technology view, implemented for the IoT system and providing necessary data/information to various data/information consumers, which utilizes the communication/data links described by the communication technology.

In Figure 9-16, IoT RA information technology view is shown along with all the entities involved and the interfaces among them.

**Figure 9-16. IoT Information Reference Architecture (IoT IRA) Diagram.**

The entities found in IoT RA information technology view are shown in Table 9-17 below.

**Table 9-17. IoT IRA Entity Descriptions.**

| IoT Domains | Domain Entities | Entity descriptions |
|---|---|---|
| | | |
| | | |

The IoT RA information technology view's interface descriptions/definitions are listed in Table 9-18.

**Table 9-18. IoT IRA Interface Descriptions/Definitions.**

| IRA IF# | Entity 1 | Entity 2 | Descriptions/Comments |
|---|---|---|---|
| | | | |
| | | | |

### 9.4.4 IoT RA Usage view

**Editor's Note**: Call for contribution.

The user view addresses the following concepts:

— activities;

 

— roles and sub-roles;

— parties;

— services; and

— cross-cutting aspects.

### 9.4.5 IoT RA Functional view

**Editor's Note**: Updated with new text contribution from Anish and Tom, WG10 N205.

**Editor's Note**: The functional view has been summarized reviewed in Ottawa meeting and agreed to keep it in the main body. The additional information still continue calling for the contribution.

The functional view is a technology-neutral view of the functions necessary to form a system. The functional view describes the distribution of, and dependencies between, functions necessary for the support of activities described in the user view, and addresses the following concepts:

— functional components;

— functional layers; and

— multi-layer functions.

Each functional component is realized by one or more implementations of actual system components, which may be deployed to form a working system.

#### 9.4.5.1 IoT Functional domains and cross-domain functions

Figure 9-17 is an overview of the IoT Functional View, showing functional domains and a high level view of cross domain functions. Green arrows represent data/information flows, grey/white arrows represent decision flows, and red arrows represent command/request flows.

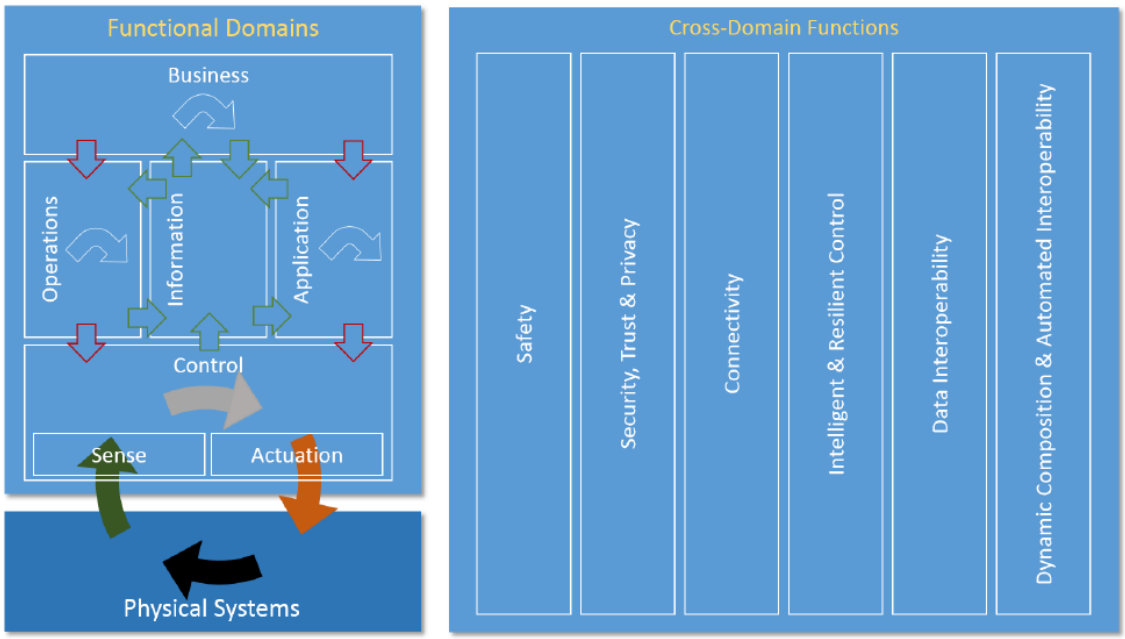


 

**Figure 9-17. IoT Functional View - Functional Domains and Crosscutting Functions.**

IoT systems can be decomposed into five functional domains:

- Control domain
- Operations domain
- Information domain
- Application domain
- Business domain

### 9.4.5.2 IoT Reference architecture functional view

Figure 9-18 shows a decomposition of the IoT Functional Domains into Functional Components.

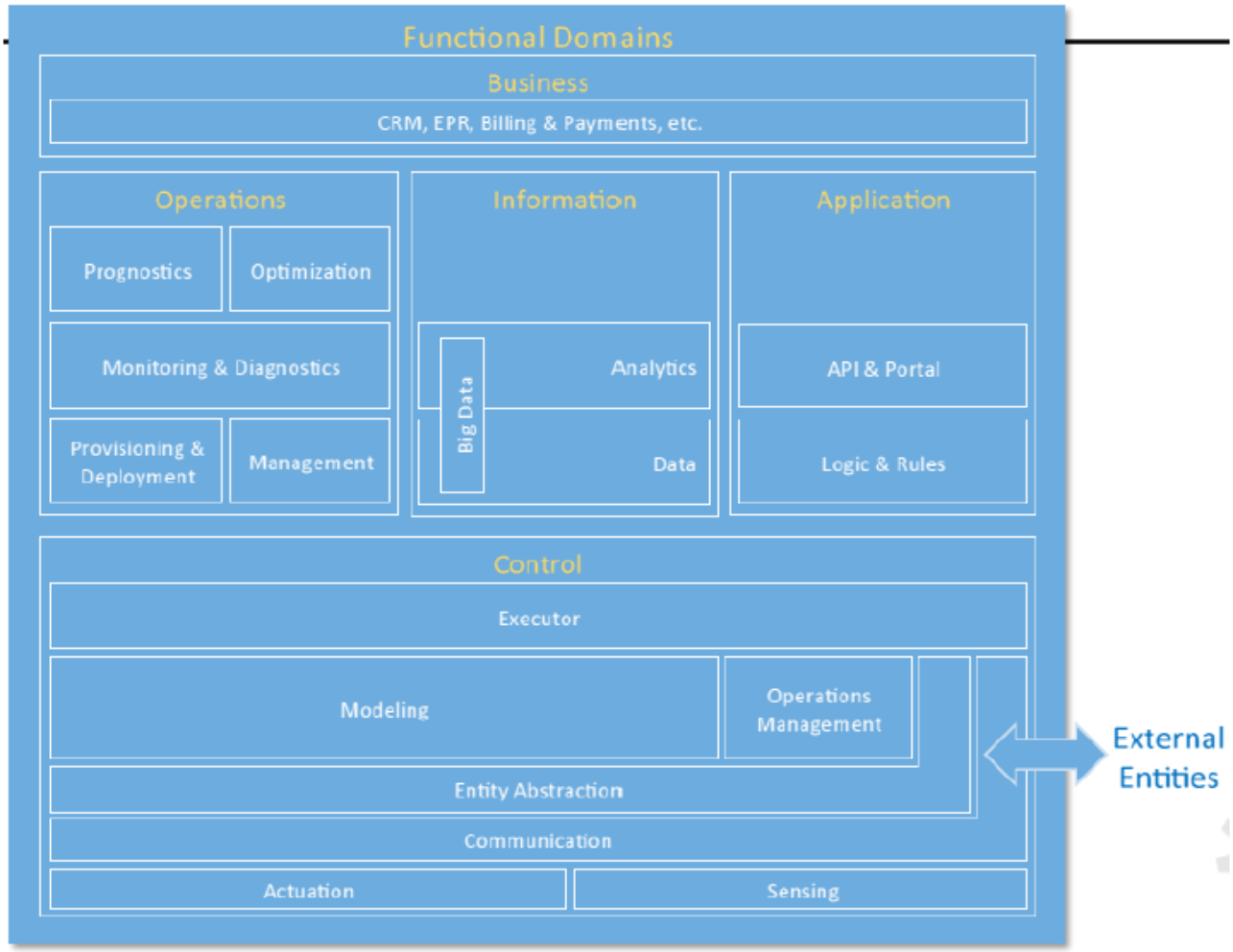


**Figure 9-18. IoT Functional View - Functional Domain Decomposition.**

#### 9.4.5.3 The control domain

The Control Domain represents the collection of functions that are performed by control systems. The core of these functions comprises fine-grained closed-loops, reading data from sensors ("sense" in Figure 9-17), applying rules and logic, and exercising control over the physical system through actuators ("actuation"). Both accuracy and resolution in timing is usually critical. Components or systems implementing these functions (functional components) are usually deployed in proximity to the physical systems they control, and are therefore geographically distributed. They may not be easily accessible physically by maintenance personnel, and physical security of these systems may require special consideration.

The Control Domain comprises a set of common functional components, as depicted in Figure 9-18. Their implementation may be at various levels of complexity and sophistication depending on the systems, and, in a given system, some components may not exist at all. We describe each in turn.

Sensing is the functional component that reads sensor data from sensors. Its implementation spans hardware, firmware, device drivers and software elements. Note that active sensing recursively, requires control and actuation, and may therefore have a more complex linkage to the rest of the control system, for example, an attention element to tell the sensor what is needed.

Actuation is the functional component that writes data and control signals to an actuator to enact the actuation. Its implementation spans hardware, firmware, device drivers and software elements.

Communication functional component connects sensors, actuators, controllers, gateways and other edge systems. The communication mechanisms take different forms, such as a bus (local to an underlying system platform or remote), or networked architecture (hierarchical, hubs and spokes, meshed, point-to-point), some statically configured and others dynamically. Quality of Service (QoS) characteristics such as latency, bandwidth, jitter, reliability and resilience must be taken into account.

Entity abstraction is a functional component which, through a virtual entity representation, provides an abstraction of scores of sensors and actuators, peer controllers and systems in the next higher tiers, and expresses relationships between them. This serves as the context in which sensor data can be understood, actuation is enacted and the interaction with other entities is carried out. Generally, this includes the semantics of the terms used within the representations or messages passed between system elements.

Modelling is the functional component dealing with understanding the states, conditions and behaviours of the systems under control and those of peer systems by interpreting and correlating data gathered from sensors and peer systems.

A data abstraction functional component may be needed for cleansing, filtering, de-duplicating, transforming, normalizing, ignoring, augmenting, mapping and possibly persisting data before the data are ready for analysis by the models or destroyed.

Operations Management is the functional component that enables operations management of the control systems including system on-boarding, configuration, policy, system, software/firmware updates and other lifecycle management operations.

Note: the IIC RA V1.1 (N113) has replaced this functional component with the Asset Management functional component, to avoid confusion with the Management component of Operations Domain.

 

Executor is the functional component that executes control logic to the understanding of the states, conditions and behaviour of the system under control and its environment in accordance with control objectives.

#### 9.4.5.4 The operations domain

The Operations Domain represents the collection of functions responsible for the provisioning, management, monitoring and optimization of the systems in the control domain.

Functional components in the Operations Domain are shown in Figure 9-18.

Provisioning and Deployment functional component consists of a set of functions required to configure, on-board, register, and track assets, and to deploy and retire assets from operations. These functions must be able to provision and bring assets online remotely, securely and at scale.

Management functional component consists of a set of functions that enable management centres to issue a suite of management commands to the control systems, and from the control systems to the assets in which the control systems are installed, and the control systems and the assets to respond to these commands.

Monitoring and Diagnostics functional component consists of functions that enable detection and identification of problems before they occur.

Prognostics functional component consists of the set of functions that serves as a predictive analytics engine of the IoT system. The main goal is to identify potential issues before they occur and provide recommendations on their mitigation.

Optimization functional component consists of a set of functions that improves asset reliability and performance, reduces energy consumption, and increase availability and output in correspondence to how the assets are used.

#### 9.4.5.5 The information domain

The Information Domain represents the collection of functions for gathering data from various domains, most significantly from the control domain, and transforming, persisting, and modelling or analysing those data to acquire high-level intelligence about the overall system. The data collection and analysis functions in this domain are complementary to those implemented in the control domain. There, these functional participate directly in the immediate control of the physical systems, while in the information domain, they are for aiding decision-making, optimization of system-wide operations and to improve the system models over the long term.

Components implementing these functions may or may not be co-located with their counterparts in the control domain.

The decomposition of the Information domain is illustrated in Figure 9-18.

Data functional component consists of functions for:

- Ingesting sensor and operation state data from all domains
- Quality-of-data processing (data cleansing, filtering, de-duplication, etc.)

 

- Syntactical transformation (semantic assignment, context injection and other data augmentation processing based on metadata and other collaborating data set)
- Data persistence and storage (e.g. for batch analysis),
- Data distribution (e.g. for streaming analytic processing).

*Analytics* functional component has a set of functions for data modelling, analytics and other advanced data processing, such as rule engines.

*Big Data* functional component provides functions for storage and retrieval of large volumes of IoT data.

#### 9.4.5.6 The application domain

The Application Domain represents the collection of functions implementing application logic that realizes specific business functionalities. Functions in this domain apply application logic, rules and models at a coarse-grained, high level to optimize with a global scope. They do not maintain low-level continuing operations, as those are delegated to those in the control domain, which must maintain local rules and models in the event of losing connectivity.

The decomposition of the application domain is illustrated in Figure 9-18.

*Logics and Rules* functional component comprises core logics, e.g., rules, models, engines, activity flows, etc., implementing specific functionality that is required for the use case under consideration.

*APIs and Portal* functional component comprises a set of functions that an application exposes its functionalities as APIs for other applications to consume, or human user portal enabling human interactions with the application.

#### 9.4.5.7 The business domain

The business domain functions enable end-to-end operations of the IoT Systems by integrating them with traditional or new types of IoT specific business functions including those supporting business processes and procedural activities. Examples of these business functions include enterprise resource management (ERP), customer relationship management (CRM), billing and payment, human resource, work planning and scheduling systems.

### 9.4.6 IoT Business model

**Editors' Note**: Should this business model become a business view in IoT RAs? Contributions/comments are requested from the WG 10 experts.

The following business model reflects the emerging division of service providers and stakeholders found in the business ecosystem of the IoT.

 

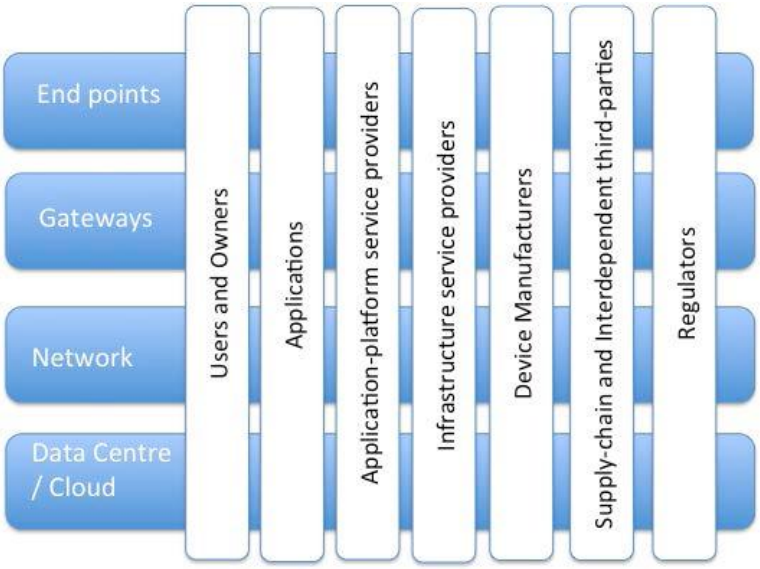


**Figure 9-19. IoT Business Model.**

**Table 9-19. Horizontal layers in the IoT business model in Figure 9-19.**

| Horizontal element | Definition |
|---|---|
| Endpoint | The elements which collect/sense/receive data from users or the physical world. |
| Gateways | Devices which facilitate the transmission of the data from endpoints to backhaul networks connected endpoint to centralized services. |
| Networks | Standards-based, backhaul networks designed to very wide ranges of service levels, and transmit data over medium to great distances. |
| Data Centre / Cloud | The aggregation points for data from the endpoints, and location of either centralized applications processing or application management and monitoring. Big data repositories. |

**Table 9-20. Vertical IoT stakeholders in the business model in Figure 9-19.**

| Vertical element | Definition |
|---|---|
| Users and owners | The beneficial operator of the device in the IoT. |
| Applications | The system and processes specifically configured for the beneficial users and operators/owners. |
| Application Platform Service provider | A flexible, configurable, multi-tenanted platforms upon which distinct applications can be configured, installed or developed. Many IoT systems will be built from component elements, not a single, monolithic design. Requirements established for the system should be viable in the context of the different vendors' platforms solutions that must be integrated. |
| Infrastructure Service-providers and Operators | Who is managing the basic physical and logical elements at the endpoint, in the network and DC or Cloud? Telecommunications carriers will frequently be part of this mix, but so too may entirely private or dedicated networks. The interface points between each of the asset horizontals" may have their |

 

| | |
|---|---|
| | own independent brokers and aggregators, in addition to the providers themselves. |
| Device Manufacturers | The producers of the physical and logical elements of end-point, network and data centre/cloud devices. Who is building the physical devices that compose the solution at the endpoint, gateway, inside the network and within the DC or Cloud? They will be building the same equipment to support many different clients and applications. They are seeking to maximize utility of features and functions and (probably) minimize costs. |
| Supply chain and Interdependent third parties | Who is providing critical (minute to minute) inputs on a direct basis like energy, physical security, water, physical space, manpower?<br><br>Who is providing critical inputs to the critical inputs?<br><br>(Secondary dependencies / cascade dependencies?) For instance: public security and emergency services, utilities, shipping and logistics, out-of-band communications and networking?<br><br>Who is depending on the Users, and their ability within the IoT and the given IoT system under assessment?<br><br>Who are the Users depending on to provide necessary goods or services (information) required for the operation of the IoT system under consideration? |
| Regulators | From locale to locale regulation may differ. In some locale the particular application or system within the IoT may be regulated, and in others laissez-faire. What level of government has oversight? What sanctions can they exercise for regulatory breech? What are the conditions of licensure? |

 

# Annex A (informative) Use case for illustrating the IoT systems' domains using a sample example

## A.1 Use case: A high rise building with 200 apartment units

A high-rise building houses 200 individual apartment units. An IoT system for the building is also installed when the building became operational supported by a building area network (BAN). Each apartment is equipped with a smart digital thermostat and a heating/cooling unit. The thermostat is powered by a battery, and the battery energy level is monitored by a dc-current sensor. The thermostat also has a controller with a simple switching circuitry with an embedded software that controls the heating/cooling unit to maintain the apartment ambient temperature within ±0.5°C of a set temperature by the apartment owner. Each apartment has a high speed Internet connection but the Internet service is provided by a third party network provider. An apartment owner can hire a home monitoring service provider for the apartment monitoring and security. The home monitoring service installs a home area network (HAN) to monitor and control various household equipment and to provide home security.

Services provided by the service provider includes apartment temperature monitoring and control, lighting conditions, curtain settings, intruder detection and reporting, fire and smoke detection and reporting, and various other reporting options to the building operators and managers, utility companies, law enforcement offices, etc. One example of optional reporting is to send the apartment's 24-hour temperature profiles with a 15 min-resolution once a day to the power utility company for potential discount in monthly utility bills.

In this example, a scenario of the activities of the IoT system is described when the apartment owner reset the apartment's digital thermostat prior to returning to the apartment. The owner also signed up for the power utility bill discount option through the service provider.

The apartment owner accesses his home monitoring service provider's website by using his smart phone connected to a Wi-Fi hotspot and requests the current temperature setting and the current temperature of the apartment. The service provider's application replied through its webpage 23°C and 23.4°C, respectively. The owner than submits a request to have the service provider reset the room temperature to 18°C so that the apartment temperature can be lowered to 18°C from 23.4°C before returning to the apartment. The service provider's application also informed that it would estimate 30 minutes to fulfil the request. And the service provider application sends an e-mail message when the request is fulfilled.

This example is pictorially represented in Figure A.1 using the IoT RM diagram in Figure 9-11. The activities associated with the active network or communication links are also described in Figure A.1.

 

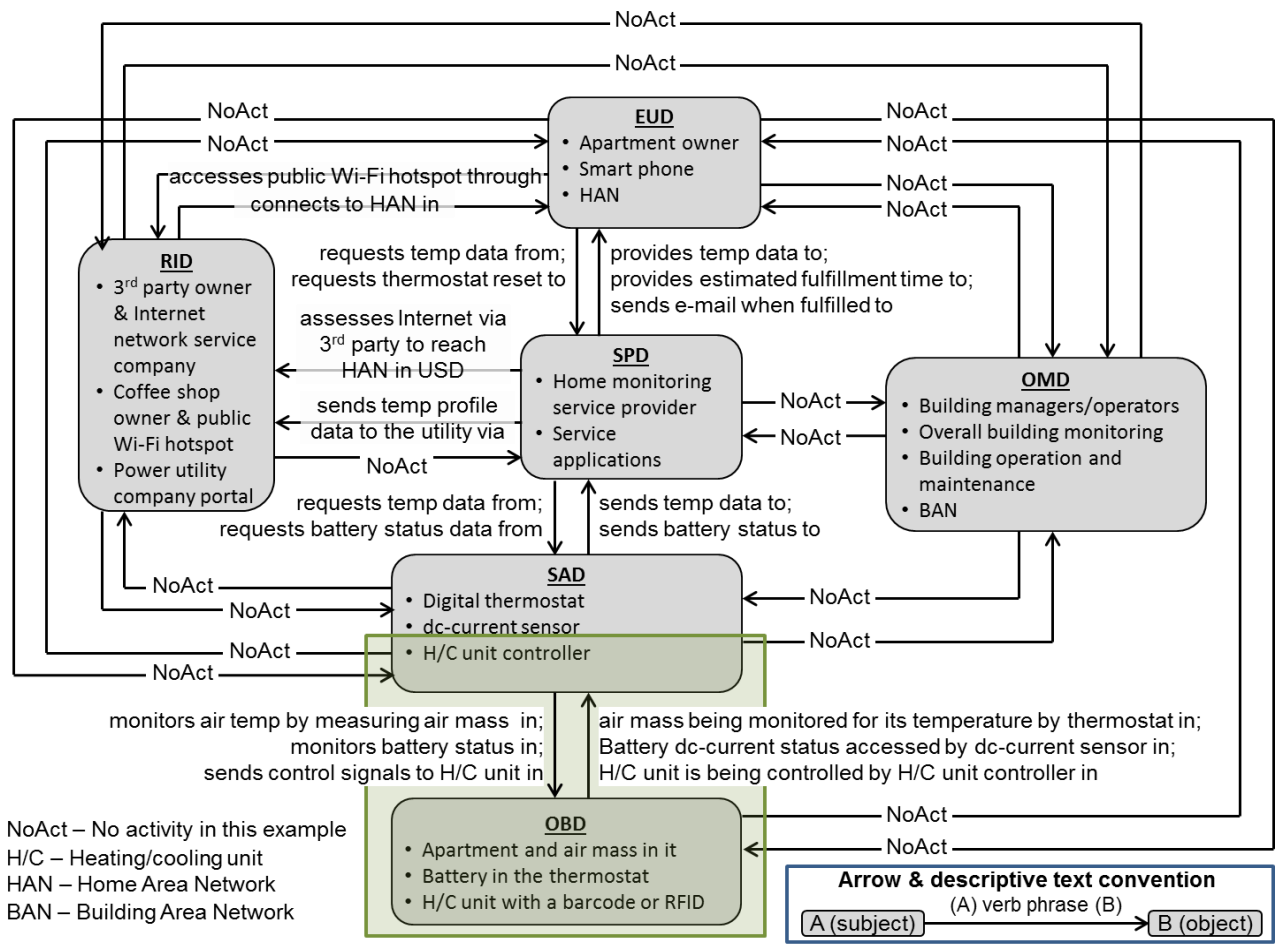


**Figure A.1 — Example represented by using the IoT RM diagram.**

In this example the domains of the IoT systems can be described as:

End-User domain (EUD) has the apartment owner as the end user and a stakeholder, the owner's smart phone as the user interface device, and the home area network (HAN) installed by the service provider. The generic entities in OBD in this example are then:

— End User;

— End-User's interface device (Note: User Interface can have both physical and virtual entities); and

— Network.

Object domain (OBD), in this example, has the air mass in the apartment which is being monitored for its temperature, the battery in the digital thermostat that is being monitored by the dc-current sensor, and the heating/cooling unit. The heating/cooling unit has a barcode or a RFID for its serial and model number and other tracking information. Thus, OBD had physical objects (c.f. physical entities) that compose the environment for which the IoT system is responsible. The generic entities in OBD derived from this example are then:

— Physical objects being monitored, measured, sensed, manipulated via actuation, and/or controlled;

 

— Virtual objects tightly coupled with physical objects; and

— The tag, e.g., barcode and RFID attached to physical objects.

Sensing & actuating domain (SAD), in this example, has a digital thermostat for the apartment's air mass temperature monitoring, a dc-current sensor to monitor the health of the digital thermostat's battery, and the heating/cooling unit controller to control the heating/cooling unit by generating control signals for electronic switches. Then the generic entities in SAD from this example are:

— Various types of sensors to monitor, measure, and/or report;

— Various types of controller to generate control signals for actuators;

— Various types of actuators to manipulate the physical objects;

— Various types of virtual entities in sensors, controllers, and actuators that provides various functions; and

— In case of tags (barcode and RFID), tag reader.

Service providers domain (SPD), in this example, has the home monitoring service provider as a stakeholder and various types of services provided such as home environment monitoring (e.g., temperature, air quality, humidity, etc.) and control, lighting condition and control, intruder detection and reporting, fire and smoke detection, and warning and reporting messages, etc. to the home owner or the building operators/managers, utility companies, law enforcement and fire department, etc. SPD can host multiple service providers.

— Service provider as a stakeholder;

— Service provider's interface devices;

— Various types of service applications and functions that support end-user which are mostly virtual entities which runs within physical entities, such as servers or local computing platforms; and

— Network that touches various other networks to fulfil the end-user requests.

Operations & management domain (OMD) has the building managers and operators as stakeholder. OMD provides overall building monitoring via the building area network (BAN) allowing building operations and maintenance. The generic entities in OMD are then:

— OMD stakeholder;

— OMD stakeholder's interface device/system;

— Applications and functions associated with building monitoring, operation, and maintenance; and

— Network

 

Resource interchange domain (RID) in this example has the 3rd party Internet service provider as one of the stakeholders, Internet access service applications and functions, the coffee shop owner as the other stakeholder, and the public Wi-Fi service function, and the utility company operators as another stakeholder and the interface portal. The generic entities in RID derived from this example are:

- Various types of stakeholders who provide services to an IoT system when such services are not available within an IoT system;
- RID stakeholders' interface device/system; and
- Various types of service applications and functions provided by the stakeholders (Note: the various types of service applications and functions have sub-entities).

It should be noted that:

- The generic entities identified for each domain of an IoT system using this example are not all inclusive, but typical ones have been identified;
- An entity can be physical entity or virtual entity, or has both;
- An entity can have one or more sub-entities;
- A physical entity can have one or more physical sub-entities or one or more virtual sub-entities, or both; and
- A virtual entity can only have one or more virtual sub-entities.

In developing a IoT Reference Model (IoT RM), a top level entities are needed, and the sub-entities are involved in the various views of IoT Reference Architecture (IoT RM).

 

# Annex B (informative) IoT Reference architecture framework

The architecture framework shown in Figure B.1 can be considered as an overarching IoT RA Framework. The purposes of this IoT RA Framework are:

a) to illustrate the IoT RA in a familiar representation to other related reference architecture, e.g., communications reference architecture, sensor network reference architecture, etc., for an easier understanding to the users of this international standard;

b) to be prelude to the IoT Systems Reference Architecture (IoT SRA), the IoT Communications RA (IoT CRA), and the IoT Information Reference Architecture (IoT IRA) as these RAs are presented and described in a difference way compared to the layered structured RAs;

c) to show the main components of the IoT in a layered structure which combines physical, virtual, functional, logical parts all together, which are associated to the parts in IoT SRA, IoT CRA, and IoT IRA;

d) to identify needed standardisation areas (see the bolded characters in Figure B.1) in IoT Systems by showing either the standard gap areas or lack of standards and requirements, and this is one of the responsibilities of the IoT RA framework or any useful reference architecture; and

e) to associate any relative or related standards to each entity in the IoT RA Framework, which lead to an IoT Technical Reference Architecture, showing the available standards to the user of this IoT RA International Standard.

The arrows in the framework shown in Figure B.1 represent various types of top-level interactions between the blocks in the diagram. The interactions can be: (1) standard updates per evolving IoT system technology and component development; (2) function modifications per application and service updates; and/or (3) interfaces which are described in the three IoT RAs.

Another use of the IoT Reference Architecture Framework is Technical Reference Architecture where each module in Figure B.1 can be mapped and shows the standard(s) associated with that particular module.

 

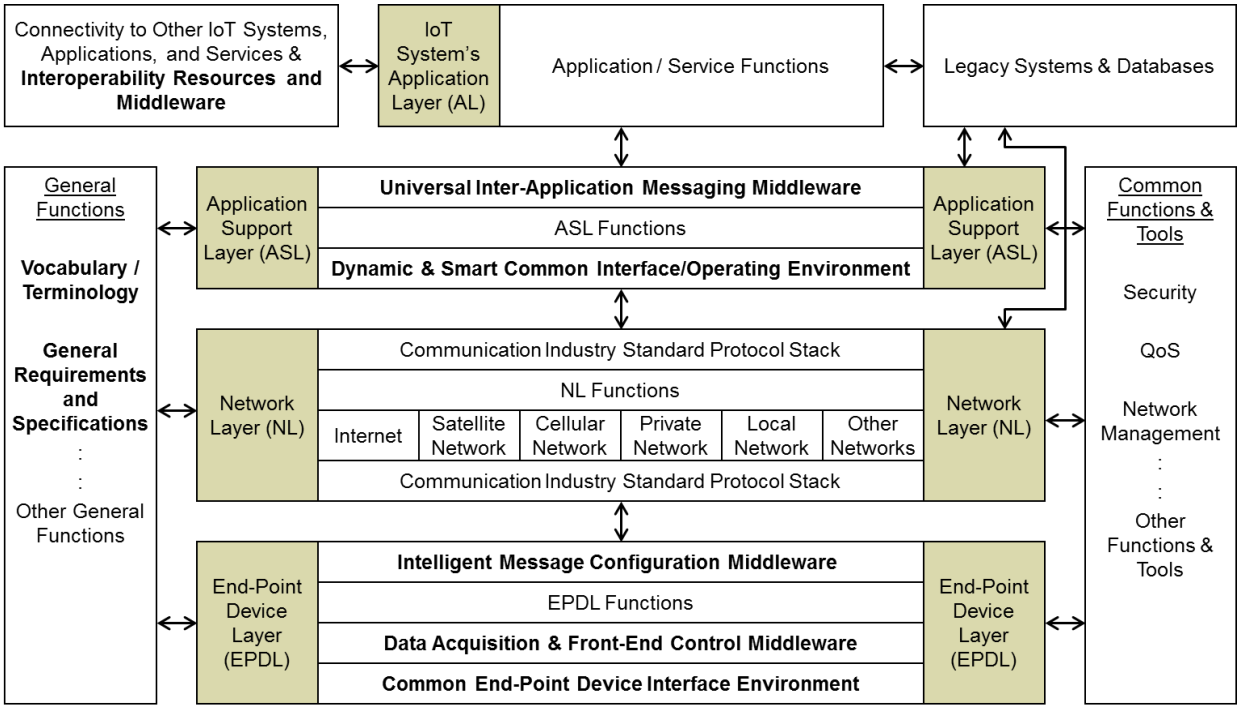


**Figure B.1 — IoT Reference architecture framework.**

 

# Annex C (informative) IoT System Implementation Guidance

## C.1 Reference architecture of End-User Domain (EUD)

End-User Domain (EUD) is the domain that houses the following EUD's common and representative entity types:

a) Different end-user entity type [Entity type name: User]

End-user can be an individual person, a group of persons (e.g., a household), industry (e.g., a company, a corporation, or an enterprise); or local/state/provincial/federal governments' organizations (e.g., transportation department, agricultural department, water department, etc.).

b) End-user assets that are owned by an end-user and/or within the user premise included in the EUD [Entity type name: User Asset)

1) Various types of end-users' interface devices that the end-users use to access an IoT system or a conventional system to access specific application(s), service(s), data, and/or information at any given time [Entity type name: User Interface Device].

The end-user interface devices include, but are not limited to, wearable/mobile electronics (e.g., smart phone), mobile computing systems (e.g., laptop, tablet), stationary/fixed computing systems (e.g., personal computer, specialty computer) [Entity type name: User Other Asset].

2) Various types of end-users' assets other than the end-users' interface devices

Other than the end-users' interface devices include, but are not limited to, non-electronic entities (e.g., desk, chair, books), electronic entities (e.g., TV, refrigerator, digital thermostat, printer, monitor/display, camera). The non-electronic entities may be attached with a barcode or a RFID.

Note: In a case or scenario when an end-user's .asset(s) become the subject of an IoT system, the asset(s) are the objects associated with the IoT system; therefore, the asset(s) belong to the object domain (OBD) instead of the EUD is such case or scenario.

Note 1: An individual end-user asset is a physical entity in the EUD.

Note 2: Some users' assets consist of both a physical entity and one or more virtual entities.

Note 3: A certain end-user asset may provide end-user specific application(s) or service(s).

Note 4: Network-related end-user assets are categorized under the network entity.

c) Wired and/or wireless network(s) that interconnect the end-user's assets in the EUD

The EUD's networks can be, but are not limited to, local area network (LAN), home area network (HAN), building area network (BAN), industrial networks (e.g., fieldbus), corporate/enterprise network (e.g., Intranet, private wide area network), etc., depending on end-user type.

Note: One-directional or bidirectional point-to-point data link is included in a network.

d) Bidirectional interfaces or access point (AP) entity types includes devices like routers, gateways, etc. There are three interface/AP entity types.

 

1) Other domains within an IoT system

The EUD interacts with the entities in object domain (OBD), sensing & actuating domain (SAD), service providers domain (SPD), operations & management domain (OMD), and resource interchange domain (RID). Therefore, the EUD provides bidirectional inter-domain interfaces and/or access point(s).

2) Other IoT systems

The end-users in the EUD in one IoT system can access other IoT system(s) at any given time directly through interfaces and/or portals in the RID or through the IoT Platform via the RID, as shown in Figure C.1.

3) 3rd party services

The system operators and managers can access 3rd party services available to them through its own IoT system(s) or any other IoT systems that they have access to. These 3rd party services are provided by third party service providers who are shown in Figure C.1 at the bottom of the diagram, "Organizations outside of IoT systems."

— Figure C.1 is the EUD reference model (RM) which shows the decomposition of the EUD into its common and representative entity types along with the representative interactions between the entity types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

 

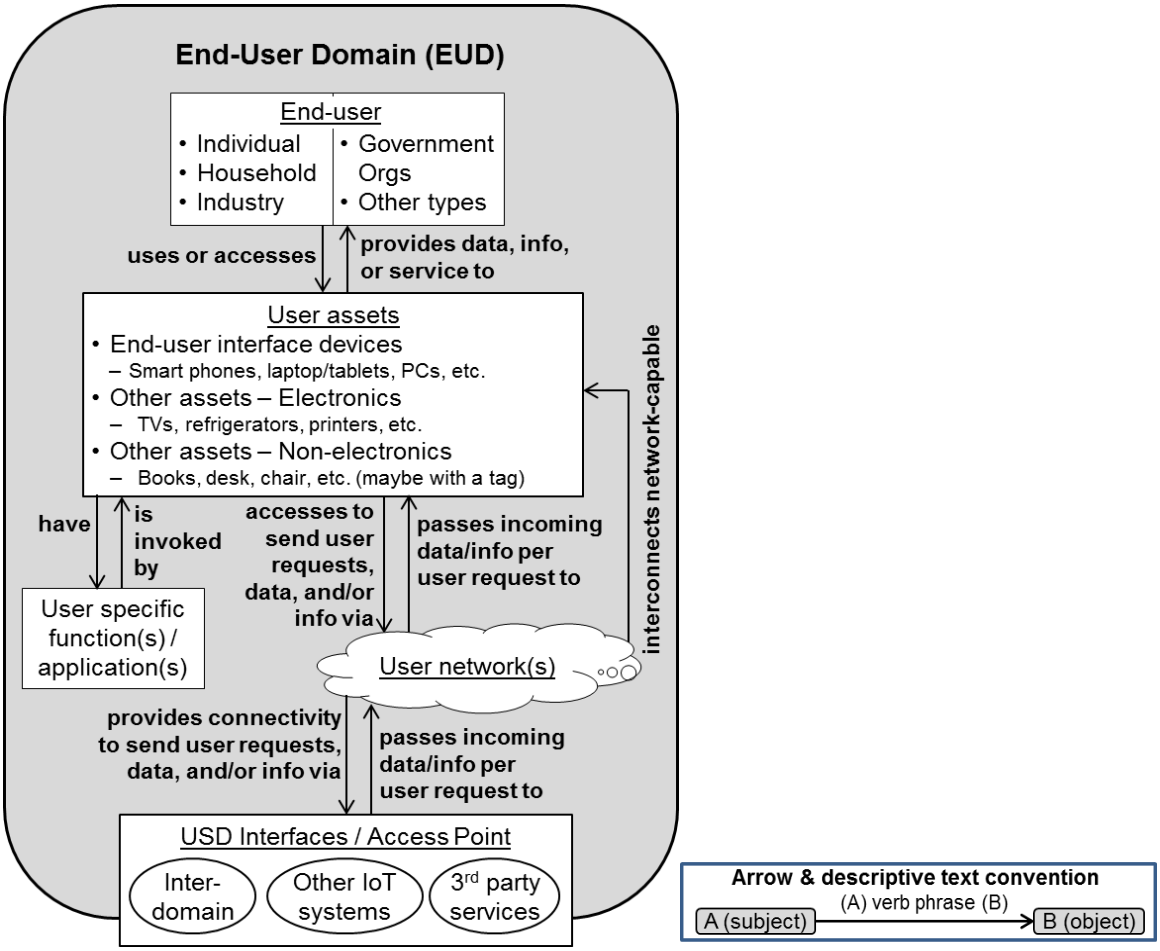


**Figure C.1 — End-User Domain (EUD) reference architecture.**

## C.2 Reference architecture of Object Domain (OBD)

Object domain (OBD) is populated with objects that are "the things within the purview of an IoT system." Therefore, the OBD is the primary environment that an IoT system is responsible for its given tasks or functions such as monitoring, sensing, controlling, manipulating, etc. Therefore, the objects in the OBD can be a myriad of things of many different physical and virtual kinds. Although it may be next to impossible to list all potential objects that can reside in the OBD, the objects in the OBD can be mainly in nine entity types:

a) Physical objects being under the purview of an IoT system

Physical objects in the OBD can be further classified as being tangible and intangible.

1) A tangible physical object (TPO) is a physical object that has a form, shape, and boundary (e.g., surface) that defines the object visually and felt by touch.

Examples of the tangible physical objects are wearable/portable electronics (e.g., smartphone, smart watch, etc.), human/person, animal, transportation systems (e.g., automobile, airplane, underwater vehicle, space vehicle, etc.), household appliances (e.g., television, refrigerator, radio, etc.), buildings, medical equipment (e.g., imaging systems such as MRI, CT, etc.) and medicine (e.g., prescription drugs, vaccine vial, etc.), agricultural products (e.g., rice, apple,

 

grape, etc.), livestock (e.g., cow, pig, chicken, etc.), liquids (e.g., water, oil, liquid nitrogen, liquid chemical solution, paint, etc.), and so on. In certain situations, TPO can include sensors, controllers, and actuators (see Clause 9.3.3 Sensing & Actuating Domain).

— A tangible physical object may not have any virtual object embedded in it.

Examples of the tangible physical objects that do not have any virtual object embedded in them are traditional furniture (e.g., chair, sofa, bed, etc.), dining utensils (e.g., knife, fork, etc.), certain mechanical devices (e.g., lawn mower, air blower, etc.), certain electronic devices (e.g., shaver, can opener, etc.), stationery (e.g., paper, envelope, pen, pencil, etc.), food, cosmetics, and so on.

— A tangible physical object may have one or more virtual objects embedded in it.

Examples of the tangible physical objects that have one or more virtual objects embedded in them are smartphones, computers (including fixed, mobile, portable computers), and modern/advanced household appliances, just to name a few.

2) An intangible physical object (IPO) is a physical object that does not have a form, shape, or boundary that defines itself which may not be visible or not be felt by touch.

Examples of the intangible physical objects are gaseous media (e.g., air, carbon monoxide, other toxic and non-toxic gases, smoke, etc.), vacuum, heat or coldness (can be felt but not be touched), and so on.

b) Virtual object(s) tightly coupled with a tangible physical object

Virtual object(s), which are embedded software/firmware as introduced in Item (a.1) above, resides in the OBD with the tangible physical object. The virtual object(s) in the tangible physical object not only may define the tangible physical object's characteristics but also provide the tangible physical object's function or functions.

c) Tags, either barcode or RFID, adhere to tangible physical objects

A tag, such as barcode or RFID, that is firmly adhere to a tangible physical object resides in the OBD.

d) Various types of sensors that measure, threshold, process, and/or report

Sensors in the OBD are the sensors "in-environment" which is formed by the OBD that an IoT system is responsible for. These sensors are either physically attached to the physical objects or surrounded by a physical object (e.g., air). Thus, these sensors are difficult to be separated from the OBD and placed in the SAD. The sensor entity type can be further categorized by five levels of smartness.

Note: See Clause C.3 (a) for details of the sensor entity type.

e) Various types of controllers to generate control signals for actuators

Controllers in the OBD are the controllers "in-environment" which is formed by the OBD that an IoT system is responsible for. These controllers are typically in "in-environment" sensors or "in-environment" actuators. Thus, these controllers are difficult to be separated from the OBD and

 

placed in the SAD. The controller entity type can be categorized into physical and virtual controller entity types.

Note: See Clause C.3 for details of the controller entity type.

f) Various types of actuators to manipulate the physical objects

Actuators in the OBD are "in-environment" actuators. These actuators are typically physically attached to physical objects in the environment that is formed by the OBD. Thus, these actuators are difficult to be separated from the OBD and placed in the SAD. The actuator entity type can be further categorized by electronic, mechanical, and virtual actuator entity types.

Note: See Clause C.3 for details of the actuator entity type.

g) Tag reader for tags (barcodes, RFID, and other types of tags)

Tag readers in the OBD are "in-environment" tag readers. These tag readers are in the environment that is formed by the OBD.

h) Wired and/or wireless network(s) that interconnect objects in the OBD

Networks in the OBD should be defined by an IoT system type. For example, if an IoT system is for home monitoring for security, it can be a home area network (HAN); if for industry, it would be an industrial control network such as fieldbus; if for corporate enterprise IoT system, it can be Internet, Intranet, or private wide area network, and so on. The network types in the OBD are based on what assets, systems, and/or environment for which an IoT system is responsible.

Note: One-directional or bidirectional point-to-point data link is included in a network.

i) Bidirectional interfaces or access point (AP) to other domains within an IoT system

The OBD interacts with the entities in the End-User Domain (EUD) and the sensing & actuating domain (SAD). Therefore, the OBD provides bidirectional inter-domain interfaces and/or access point(s) from and to the EUD and the SAD. The interfaces/AP devices include routers, gateways, etc.

The first three categories of the objects in the OBD introduced, Items (a), (b), and (c), are a much generalized way of classifying the objects under the purview of an IoT system (e.g., the environment of an IoT system's responsibility). Depending on types of IoT systems, the objects in the OBD can be further defined and categorized specific to an IoT system of interest.

The objects in the OBD are assets, and the assets have owners. An owner or owners of the assets in the OBD are responsible for maintaining the assets and for assets' proper status, e.g., physical conditions, functionalities, operational status, etc. The owners are likely one of the stakeholders, for example, individual person, investors, industry organizations, and government.

Figure C.2 is the OBD reference model (RM) which shows the decomposition of the OBD into its common and representative entity types along with the representative interactions between the entity types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

 

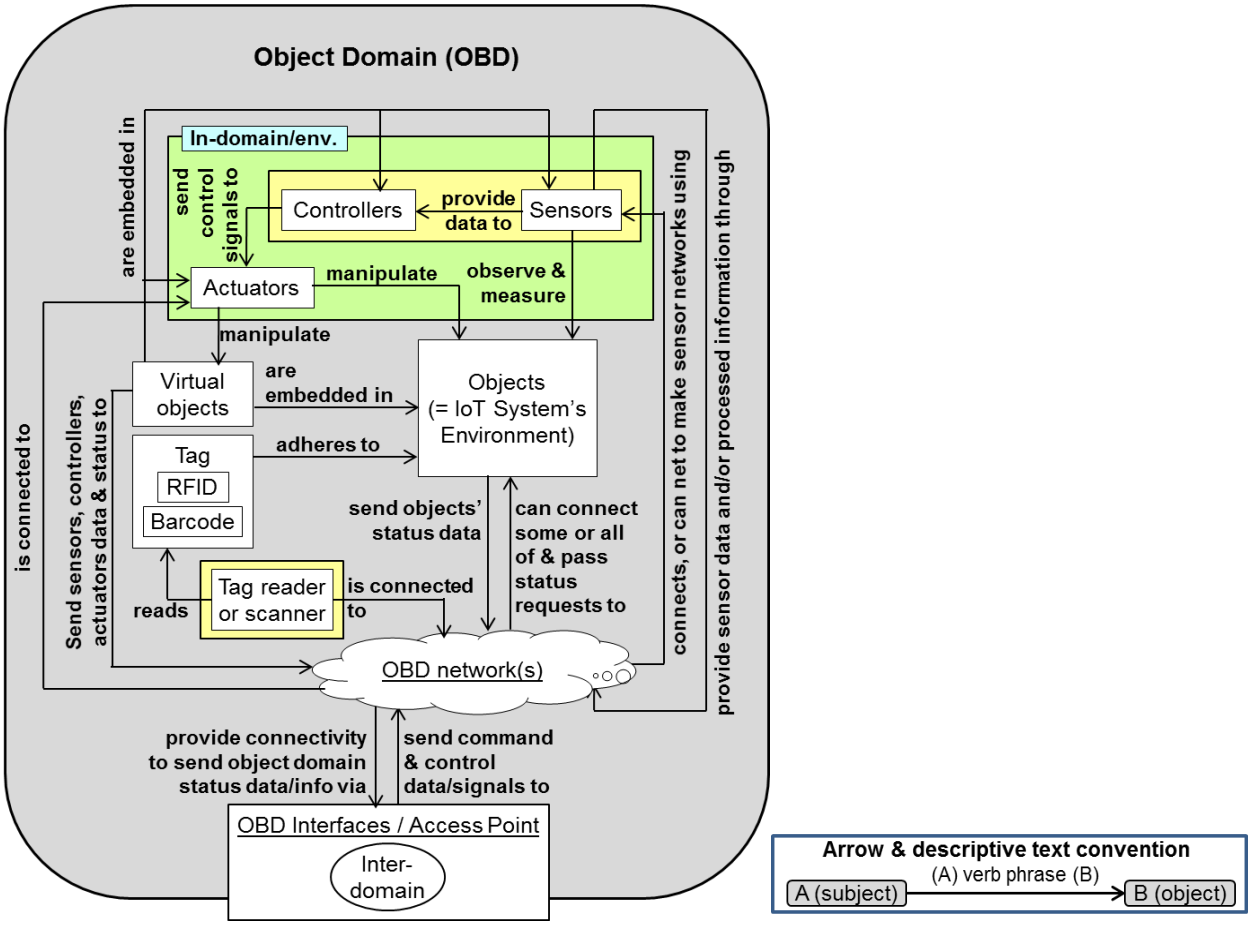


**Figure C.2 — Object Domain reference architecture.**

## C.3 Reference architecture of Sensing & Actuating Domain (SAD)

Sensing and actuating domain (SAD) is the most essential domain of an IoT system because the SAD provides critical data and information about an environment (i.e. object domain, OBD) to all other domains of an IoT system.

As shown in Figure C.3, the entities in the SAD may play a part in forming an environment of an IoT system with the entities in the OBD. This is because sensors and actuators architecturally reside in the SAD, yet they may be attached to the physical entities (both tangible and intangible) in the OBD, which means that they are physically in the OBD, which is already described in Clause C.2.

Unlike the sensor, controller, and actuator entities in the OBD which are "in-environment" entities, the sensor, controller, and actuator entities in the SAD are "out-of-environment" or "remote" entities, meaning that they do not belong in the OBD. The sensors in SAD are for remote sensing (e.g., sensors on satellites observing the earth's weather conditions, radars for air traffic control, etc.). The controllers and actuators in the SAD are also "out-of-environment" or "remote." The controllers may generate control signals for the actuators in own sensor or other sensors in its network (e.g., pan, tilt, zoom, etc.) or alter a sensor platform course (e.g., to engage thrusters in a satellite). The controller may also generate control signals for the "in-environment" actuators in the OBD. The actuators in the SAD execute the control and command signals from the controllers in the SAD.

The entities in the SAD can be classified into seven types. They are:

 

a) Various types of sensors that measure, threshold, process, and/or report

Sensors can be categorized by many different ways as shown below:

1) By complexity

— Simple sensors, e.g., thermocouples; and

— Complex sensors, e.g., high resolution infrared imaging sensors.

2) By environment, e.g., operational space

— Ground;

— Gas, e.g., air or other gaseous chambers;

— Liquid, e.g., underwater or chemical solution; and

— Space.

3) By wavelength or frequency or radiation type

— Infrasound

— Acoustic (audible)

— Ultrasound

— Radio waves

— Microwaves

— Infrared

— Visible light

— Ultraviolet

— X-ray

— Magnetic

4) By output dimensionality

— One dimensional (e.g., x)

— Two dimensional (e.g., x and y, or x plus time)

 

— Three dimensional (e.g., x, y, and z, or x and y plus time)

— Four dimensional (e.g., x, y, z, and time)

5) By operation

— Passive

— Active

6) By capability or smartness

— Measuring (or sensing) only;

— Measuring and converting to standard measurement units;

— Measuring, converting, and simple pre-set thresholding;

— Measuring and processing; and

— Measuring, processing, and reporting.

In this standard, sensors are categorized by their capability or smartness. Thus, the sensor entities are designated by:

1) Sensor smartness level 0 (SSL0): Measuring (or sensing) only

Sensor entity type SSL0 is for a primitive or basic sensor that only measures a phenomenology for which it is designed. SSL0 does not perform any processing of measured data; therefore, this type of sensor does not have virtual entity or entities, e.g., embedded algorithm or software. Typical SSL0 type sensors are operated by means of mechanical (e.g., thermocouples), chemical (e.g., reaction), light (e.g., photons), etc., which output its measurement in electrical current (mA) or voltage (V) levels. Typically, the output current or voltage is in a form of analogue signals. The sensor entity type SSL0 does not have any virtual entity.

2) Sensor smartness level 1 (SSL1): Measuring and converting to standard measurement units

Sensor entity type SSL1 is a sensor with the capability of SSL0 plus a simple conversion capability from the analogue signals in either electrical current or voltage to standard measurement units, e.g., Celsius, Fahrenheit, pound-force per square inch (psi), pascals (Pa), torr, grey/colour scales, etc. In the process of unit conversion within this type of sensors, a digitization may also be performed, outputting a digitized measurement data stream. Thus, the sensor entity type SSL1 may have a virtual entity that has an analogue-to-digital conversion function.

3) Sensor smartness level 2 (SSL2): Measuring, converting to standard measurement units, and simple pre-set thresholding

 

Sensor entity type SSL2 has the capability of SSL0 and SSL1 plus a type of a simple thresholding based on a pre-set threshold. The thresholding can be performed on either analogue or digital signals. The SSL2 type sensor may provide an indicator, e.g., a bit either 0 or 1, indicating when the threshold condition is met. Thus, the sensor entity type SSL2 has virtual entity to perform comparing measured signals to a pre-set threshold and to declare when the thresholding condition is met. It may also have a virtual entity to perform analogue-to-digital conversion.

4) Sensor smartness level 3 (SSL3): Measuring and processing with an option of storing.

Sensor entity type SSL3 has the capabilities of SSL0, SSL1, and SSL2 plus processing to convert measured data into various levels of (actionable) information. The processing functions are performed by various types of virtual entities (e.g., embedded software, dedicated algorithms) on a microprocessor or microcontroller residing in the SSL3 sensor type. Functions provided by virtual entities range from simple to complex, e.g., simple or adaptive thresholding, detection, recognition, identification, tracking, trending, data/information fusion, diagnostic & prognostic, estimation, prediction, and so on. The SSL3 type sensor can have a local storage capability to store either measured data or processed data.

5) Sensor smartness level 4 (SSL4): Measuring, processing, storing, and reporting

Sensor entity type SSL4 has the capability of SSL0, SSL1, SSL2, and SSL3 plus capabilities in generating an automated reports summarizing events, environment changes (e.g., OBD entity changes), etc., over a specified time duration.

b) Various types of controllers to generate control signals for actuators

There are two major controller entity types:

1) A controller that generates a controlling signal or signals for physical actuation to a tangible physical object or objects in the OBD.

This type of controller entity is denoted as Cont-P. Cont-P uses a simple logic or a virtual entity to generate the controlling signal or signals.

2) A controller that generates or designates code, routine(s), firmware, embedded software or application software for replacement or update to those existing one(s) in a virtual object or objects in the OBD.

This type of controller entity is denoted as Cont-V. Cont-V uses all virtual entities to achieve the generation or designation.

c) Various types of actuators to manipulate the physical objects

The actuator or actuation mechanism entity can be largely categorized into three different types:

1) Electronic actuator/actuation, entity designated as Act-E

Upon receiving a control signal generated by a controller (Cont-P), an electronic actuator (Act-E) either connected or adhere to a tangible physical object in the OBD provide an electronic actuation, e.g., electronic switch or digital switch.

2) Mechanical actuator/actuation, entity designated as Act-M

 

Upon receiving a control signal generated by a controller (Cont-P), an mechanical actuator (Act-M) either connected or adhere to a tangible physical object in the OBD deliver a physical actuation, e.g., opening and closing of a garage door, elevator operation (moving up or down, stop at a floor, open/close door).

3) Virtual actuation, entity designated as Act-V

A virtual object (Act-V), associated with a virtual object or objects in the OBD, which receives code, routine, firmware, embedded software, or application software from the virtual controller (Cont-V) in the SAD performs virtual operations to replace or update the existing code, routine, firmware, embedded software, or application software in a designated virtual object or objects with the received one.

d) Various types of virtual entities in sensors, controllers, and actuators that provides various types of sensing, controlling and actuating functions

The various virtual entities in the SAD have been introduced while describing the SAD entity types, e.g., SSL1 to SSL4 sensor entities, Cont-P, Cont-V, Act-E, Act-M, and Act-V.

e) Tag reader or scanner for barcode and RFID

The entities in SAD include a barcode reader entity and an RFID reader entity for barcodes and RFIDs that are adhere to tangible physical objects in the OBD.

f) Wired and/or wireless network(s) that interconnect objects in the SAD

Networks in the SAD can be many different types, e.g., wired vs. wireless, Internet, intranet, local area network, wide area network, and so on. These networks can make up sensor networks, control networks, and so on; and also depending on the environment of an IoT system, the networks could be a home area network (HAN), an industrial control network, private corporate wide area network, and so on. Thus, the network types in the SAD are tightly associated with the networks in the OBD because the networks in SAD should interface and interact with the networks in the OBD and/or because SAD needs to leverage the networks available in the OBD.

In case of sensor networks, the sensor network can provide network level smartness, such as collaborative information processing (i.e. multi-sensor data fusion), data/information aggregation, etc.

Note: One-directional or bidirectional point-to-point data link is included in a network.

g) Bidirectional interfaces or access point (AP) to other domains within an IoT system

The SAD interacts with the entities in the object domain (OBD) the service providers domain (SPD), the operations & management domain (OMD), the end-user domain (EUD), and the resource interchange domain (RID). Therefore, the SAD provides bidirectional inter-domain interfaces and/or access point(s) from and to the OBD, the SPD, the OMD, the EUD, and the RID. The interface/AP entity types are typically routers and gateways.

Figure C.3 is the OBD reference model (RM) which shows the decomposition of the OBD into its common and representative entity types along with the representative interactions between the entity

 

types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

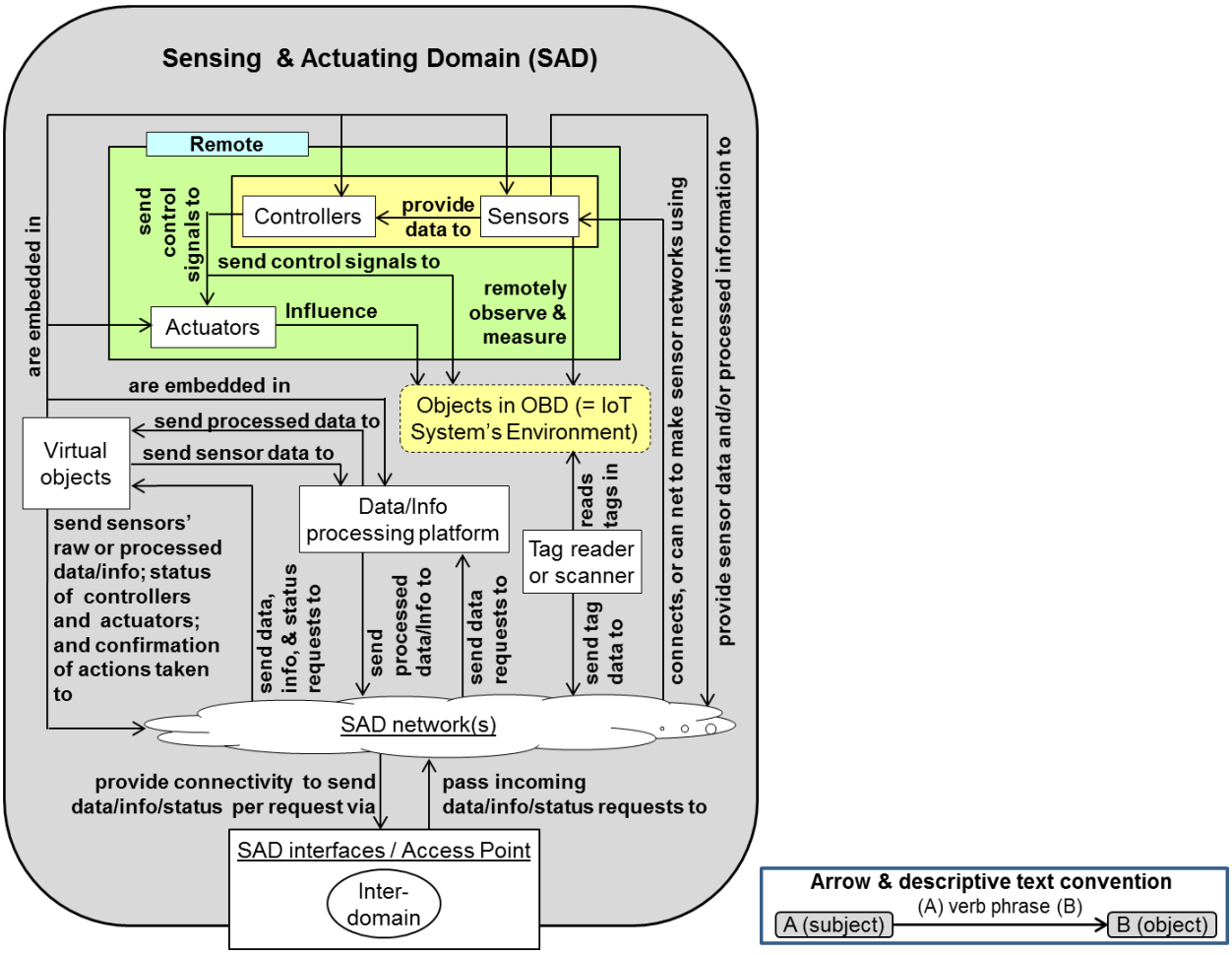


**Figure C.3 — Sensing & Actuating Domain reference architecture, the dotted box "Object in OBD" does not belong in SAD but shown in this model for completing the interaction.**

## C.4 Reference architecture of Service Provider Domain (SPD)

Service providers domain (SPD) is mainly for all types of service providers involved in an IoT system. Thus, the service providers interact not only with the users (i.e. end-users) in the EUD providing services to fulfil the users' requests, but also with the sensors/actuators/readers in the SAD to gain data/information from objects (i.e. environment that an IoT system is responsible for) in the OBD. Additionally, the SPD interacts with the OMD if an OMD stakeholder become a client of a service provider in the SPD directly or indirectly (e.g., through an end-user's request). The SPD are likely interact with the organizations (e.g., other IoT systems, IoT platform, law enforcement, utility, financial institutions, government, etc.) of its own IoT system via the resource interchange domain (RID).

The main entity types in service providers domain (SPD) are identified and listed below:

a) Service provider(s) that is one of the stakeholders in IoT systems

Within an IoT system, one or more service provides can exist and be involved. Many different types of service providers, e.g., smart home application and service providers, home monitoring and

security service providers, data storage and computing service providers, elder care service providers, smart traffic service providers, and so on.

b) Service provider's interface devices

Service providers use a type or types of interface devices to perform their services using applications in the service providers' physical entities, e.g., servers, computing platforms, etc. The interface devices can physically attached to service providers' physical entities, or they can be remotely located with wireless, Internet, or other types of communication networks.

c) SPD's virtual entities, e.g., entities that provide applications and functions that support service providers' mission and goals.

The service providers' applications, which are considered as virtual entities, runs in the SPD's physical entities, such as servers or local computing platforms. Depending on an IoT system, the virtual entities that meet the IoT system's requirements will be implemented by the service providers and exist in the IoT system.

d) Service providers' network(s) that link with various other networks

Service providers have their networks to serve their internal communications with their systems (e.g., interface devices, servers, application platforms, etc.) as well as to operate their services to the customers. The service providers' networks can be wired and/or wireless.

Note: One-directional or bidirectional point-to-point data link is included in a network.

e) Bidirectional interfaces or access point (AP) entity types include routers and gateways. There are three types of interfaces/APs:

1) Other domains within an IoT system

The SPD interacts with the entities in end-user domain (EUD), sensing & actuating domain (SAD), operations & management domain (OMD), and resource interchange domain (RID). Therefore, the SPD provides bidirectional inter-domain interfaces and/or access point(s) to the EUD, the SAD, the OMD, and the RID.

2) Other IoT systems

The service providers in the SPD in one IoT system can access other IoT system(s) at any given time directly through interfaces and/or portals in the RID or through the IoT Platform via the RID, as shown in Figure 9-12.

3rd party services: The system operators and managers can access 3rd party services available to them through its own IoT system(s) or any other IoT systems that they have access to. These 3rd party services are provided by third party service providers who are shown in Figure 9-12 at the bottom of the diagram, "Organizations outside of IoT systems."

Figure C.4 is the SPD reference model (RM) which shows the decomposition of the SPD into its common and representative entity types along with the representative interactions between the entity types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

 

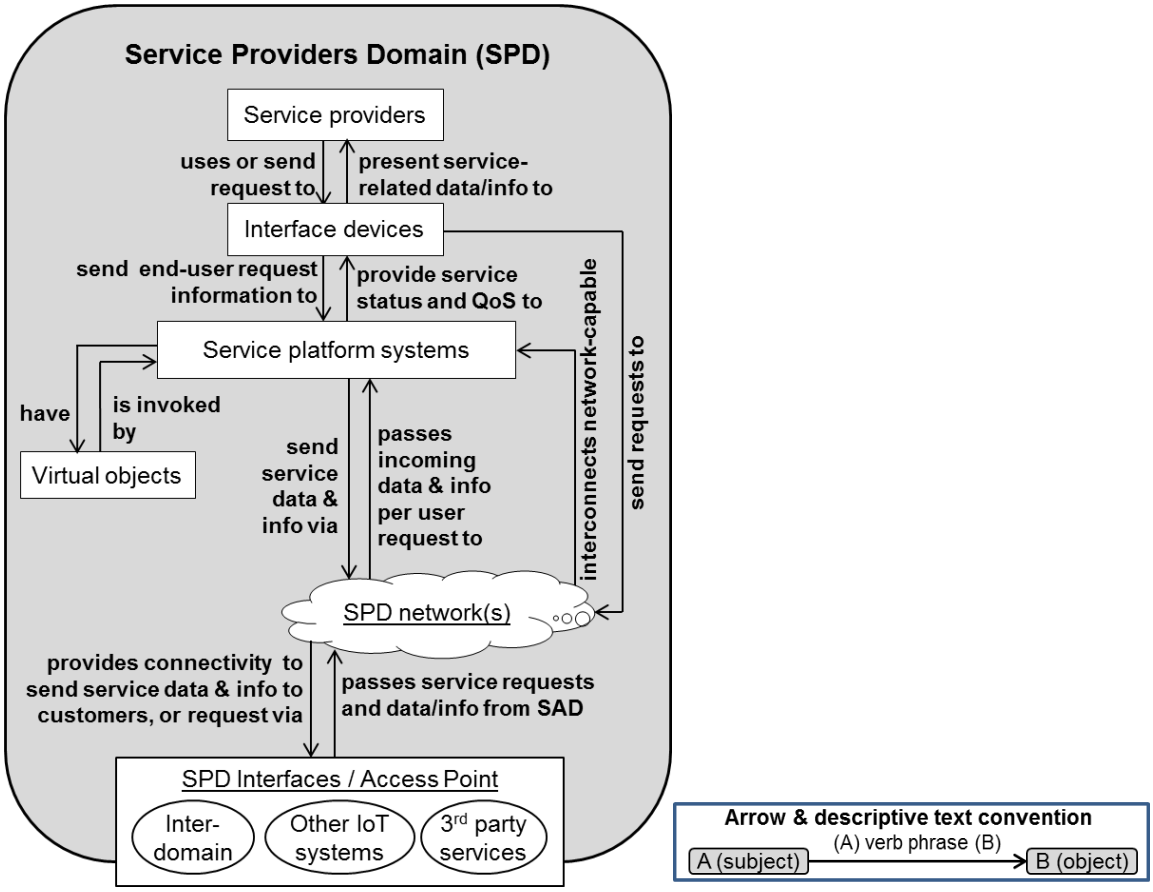


**Figure C.4 — Service Providers Domain reference architecture.**

## C.5 Reference architecture of Operations & Management Domain (OMD)

Operations & management domain (OMD) has entities that are responsible for the operation of an IoT system. The main responsibilities of the OMD are mainly in the entities in the SAD and the entities in the OBD. The OMD is also responsible not only for monitoring the activities are legitimate and following the rules and regulations but also especially for ensuring the network security in order to protect the IoT systems from harmful intrusions or hacking. The OMD involvement in the SPD is minimal because the service providers in the SPD are likely independent organizations maintaining their systems (e.g., all the entities in the SPD) by themselves. Additionally and importantly, the OMD is responsible for the inter-domain networks (i.e. Level 2 Network Infrastructure, refer to Figure 9-12) for communications and data exchanges between the domains in an IoT system.

The representative entity types in the OMD are listed and described below:

a) Operators and system managers, the OMD stakeholder as one of the stakeholders in an IoT system

   There is at least one system operator and manager in the OMD per an IoT system. Depending on the size of the IoT system (e.g., a small system that deals with a locality, a large system of systems that has distributed systems globally), more than one system operator and managers may be required.

b) Interface devices for the system operators and managers

 

System operators and managers use various types of interface devices to perform their operations and management accessing operations/management functions enabled by applications in the operators/managers' physical entities, e.g., servers, computing platforms, etc. The interface devices can physically attached to the physical entities, or they can be remotely located with wireless, Internet, or other types of communication networks.

c) Applications and functions that supports IoT system operations and management

The functions and services provided by various system operations/management applications are the virtual entities in the system operators/managers' physical entities.

d) System operator/manager's network(s) that link with various other networks

System operators/managers have their networks to serve their internal communications with their systems (e.g., interface devices, servers, application platforms, etc.) as well as to operate their operations and management functions for an IoT system's assets and inter-domain communication/data networks. The system operator/manager's networks can be wired and/or wireless.

Note: One-directional or bidirectional point-to-point data link is included in a network.

e) Bidirectional interfaces or access point (AP) entity types include routers and gateways. There are three types of interfaces/APs:

1) Other domains within an IoT system

The OMD interacts with the entities in end-user domain (EUD), sensing & actuating domain (SAD), service providers domain (SPD), and resource interchange domain (RID). Therefore, the OMD provides bidirectional inter-domain interfaces and/or access point(s) to the EUD, the SAD, the SPD, and the RID.

2) Other IoT systems

The system operators and managers in the OMD in one IoT system can access other IoT system(s) at any given time directly through interfaces and/or portals in the RID or through the IoT Platform via the RID, as shown in Figure 9-12.

3) 3rd party services

The system operators and managers can access 3rd party services available to them through its own IoT system(s) or any other IoT systems that they have access to. These 3rd party services are provided by third party service providers who are shown in Figure 9-12 at the bottom of the diagram, "Organizations outside of IoT systems."

Figure C.5 is the OMD reference model (RM) which shows the decomposition of the OMD into its common and representative entity types along with the representative interactions between the entity types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

 

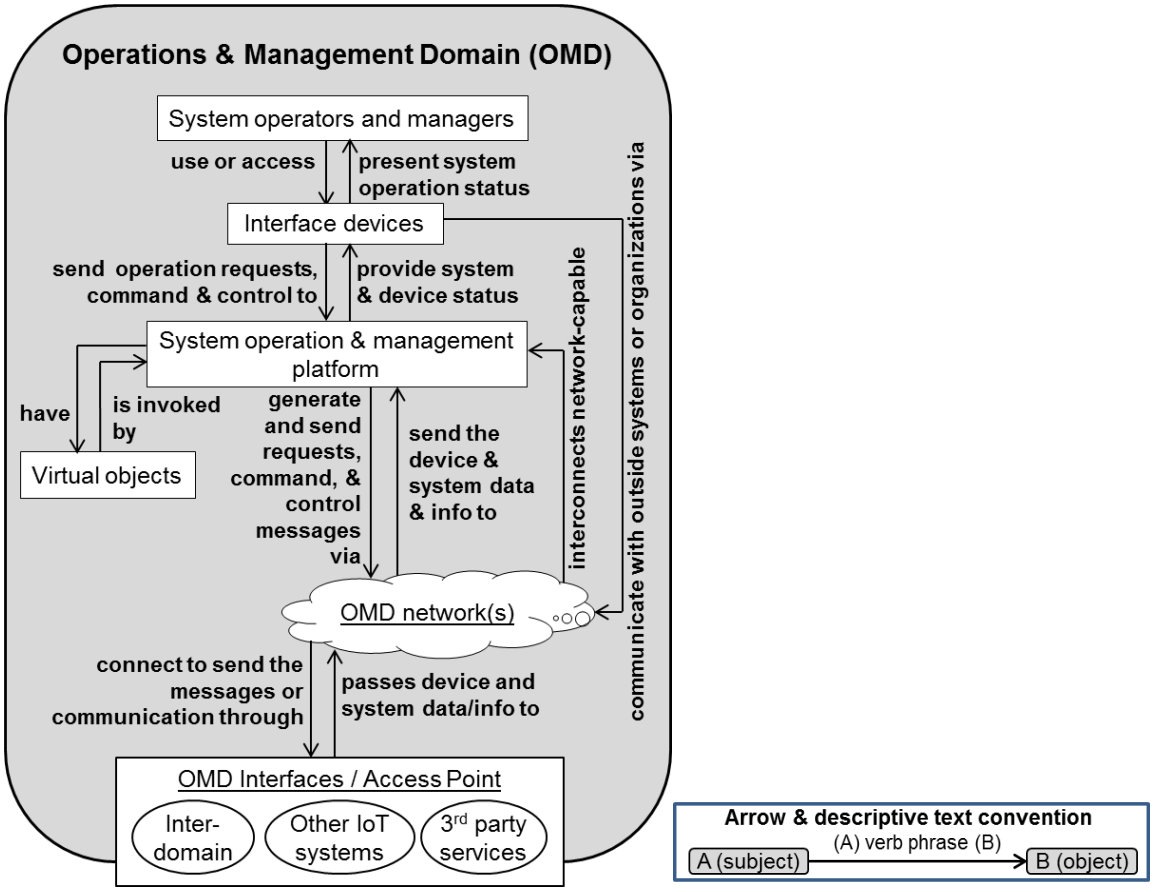


**Figure C.5 — Operations & Management Domain reference architecture.**

## C.6 Reference architecture of Resource Interchange Domain (RID)

Resource interchange domain (RID) provides three main connectivity types to the outside world of an IoT system by accessing Level 3 and Level 4 Network Infrastructures. The first main connectivity type is from one IoT system to other IoT systems using Level 3 Network Infrastructure; the second main connectivity type is from an IoT system to various types of 3rd party service providers (e.g., banks, financial institutions, billing or filing processing centres, etc.) again using Level 3 Network Infrastructure; and the third main connectivity type is from an IoT system to an IoT platform or platforms (e.g., nation-, province/state-, city-, corporation-wide, etc.) using Level 4 Network Infrastructure.

The RID can also have various kinds of stakeholders who may benefit from an IoT system, especially those stakeholders that do not belong to the IoT system permanently. The non-permanent or temporary stakeholders in the RID are more obvious for mobile end-users. For example, the mobile end-users that belong to the EUD of an IoT system may access the IoT system's service from any coffee shop with a Wi-Fi hot spot. When a mobile end-user goes to a coffee shop with a free Wi-Fi hot spot and connects to an IoT system, the coffee shop owner becomes a non-permanent stakeholder in the RID as this stakeholder is benefited by offering the free Wi-Fi hotspot. Another example is that an end-user signs up a certain service outside of an IoT system using the service provider in the SPD, the outside or a 3rd party service is accessed by a network interface or a portal in the RID. Then the 3rd party owner becomes a temporary stakeholder in the RID.

 

The entity types in the RID are:

a) Various types of non-permanent/temporary stakeholders

   There are many different and various types of non-permanent/temporary stakeholders who can be accessed by an IoT system.

b) RID stakeholders' interface device, systems, and networks

   The stakeholders in the RID can have their interface devices, systems (e.g., computers, Wi-Fi devices, etc.), and networks (e.g., Wi-Fi hotspot, local area networks, etc.)

c) Various types of service applications and functions provided by the non-permanent/temporary stakeholders (Note: the various types of service applications and functions have sub-entities)

   These service applications and functions are the virtual entities in the RID.

d) Bidirectional interfaces or access point (AP) entity types include routers and gateways. There are three types of interfaces/APs:

   1) Other domains within an IoT system

      The RID interacts with the entities in end-user domain (EUD), sensing & actuating domain (SAD), service providers domain (SPD), and operating & management domain (OMD). Therefore, the RID provides bidirectional inter-domain interfaces and/or access point(s) to the EUD, the SAD, the SPD, and the OMD.

   2) Other IoT systems and the 3rd party service providers

      The RID provides an IoT system with the connectivity to Level 3 Network Infrastructure, as shown in Figure 9-12.

   3) IoT platforms

      The RID provides an IoT system with the connectivity to Level 4 Network Infrastructure as shown in Figure 9-12.

Figure C.6 is the RID reference model (RM) which shows the decomposition of the RID into its common and representative entity types along with the representative interactions between the entity types, communications and data/information flows by arrows, and interfaces between entity types by connecting points of an arrow between them.

 

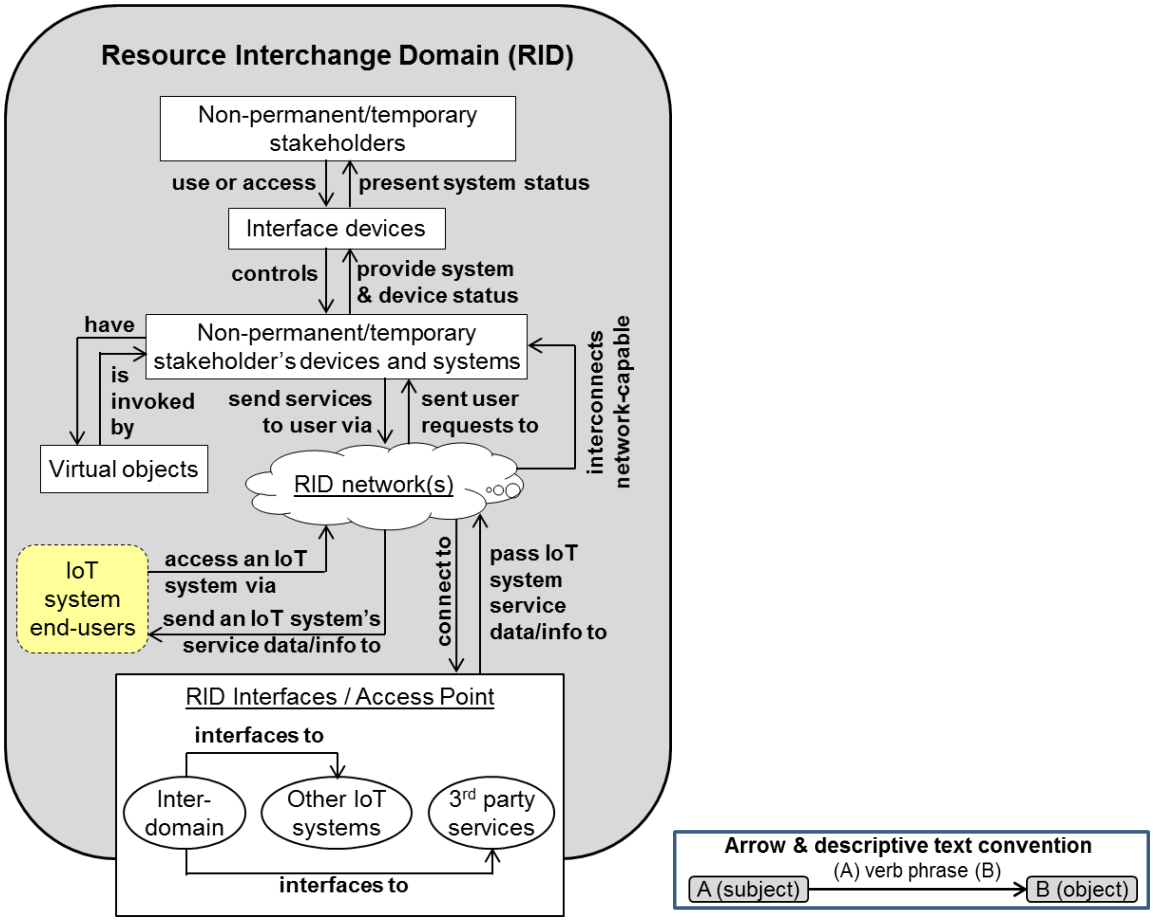


**Figure C.6 — Resource Interchange Domain reference architecture, the dotted box "IoT system end-users" does not belong in RID but shown in this model for completing the interaction.**

## C.7 Inter-domain communication/data networks

Although the inter-domain communication/data networks are not specifically designated as one of the six domains, these networks take a critical role in an IoT system. Depending on the IoT systems, the inter-domain communication/data networks can be Internet, Intranet, enterprise backbone network, wide area network, and so on. Business-to-business (B2B) networks are also considered as inter-domain communication/data network.

 

# Bibliography

[1] ISO/IEC 29182-2 Information technology – Sensor Network: Sensor Network Reference Architecture (SNRA) – Part 2: Vocabulary/Terminology

[2] http://www.sgip.org/Introduction-to-The-Smart-Grid-Conceptual-Model.

[3] IoT-A's public deliverable documents on IoT Reference Architecture Model.

[4] OASIS SOA Reference Model, OASIS SOA Technical Committee.

[5] https://en.wikipedia.org/wiki/Reference_model

[6] Howard Choe, "Generalized IoT systems' models and the role of sensor networks in IoT," Workshop on Sensor Networks and Internet of Things (IoT), in conjunction with the meeting of ISO/IEC JTC 1 WG 7 (8-10 September 2015), Singapore, 7 September 2015

 