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

ISO/IEC JTC 1/WG 10

Secretariat: KATS

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

WD stage

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.

Introduction

Internet of Things (IoT) has broad use in the industry and society today, and it will be further studied and developed for many years to come. Various applications and services have been adopting and adapting are IoT technology to provide innovative solutions for users, which weren't possible a few years ago. There are a number of possible applications such as 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. Thus, IoT is an enabling technology that consists of many supporting technologies, for example, different type of communication networking technology, information technology, sensing and control technologies, software technology, device/hardware technology, and so on.

In designing and developing IoT systems, three key technologies should be considered: (1) system technology; (2) communications technology; and (3) information 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 exchange data. 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 which enable to provide various applications and services. Therefore, data/information security and user privacy is the other major technology area of importance for IoT systems. Security and privacy in IoT systems are dictated by international and national legislations, and IoT systems should comply with the local security/privacy laws and regulations. Additionally, reliability, dependability, and data validation and associated requirements are the other areas that the developers of IoT Systems should consider.

ISO/IEC 30141 identifies and specifies IoT systems' Conceptual Model (CM), Reference Model (RM), and Reference Architecture (RA). The RA is described by different architectural views, namely, systems view, communications view, information view, functional view, and usage view. These views generically represent the IoT systems. These RA views provide various types of architectural elements (e.g., subsystem platforms, functional entities) as well as base building blocks to develop application-specific (or target) architectures.

In this IoT RA International Standard (IS), the reference model is given to describe 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. Thus, the IoT RA is described from the aforementioned three main technology views in this international standard (IS):

- IoT RA Systems View: Describes the IoT Systems from system perspective
- IoT RA Communications View: Describes the IoT Systems from communication technology perspective

— IoT RA Information View: Describes the IoT Systems from information technology perspective

In addition to the above three architecture views, the following two architecture views are described in this IS:

— IoT RA Functional View

— IoT RA Usage View

— The architecture entities defined in the Systems View, Communications Views, Information View, Functional View and Usage View are related across these five IoT reference architecture views. Describing the IoT RA using these five different views 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 technology views (e.g., systems, communications, and information) describing physical security, communication security, and information security while the effectiveness of security features in architecture can be evaluated by Functional and Usage Views.

The objectives of this ISO/IEC 30141 of standard are:

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

— promote open and common guiding architecture leading to seamless interoperability of IoT Systems.

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 , 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.

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

1 Scope

This International Standard specifies IoT Conceptual Model, Reference Model, and Reference Architecture from different architectural views, common entities, and high-level interfaces connecting the entities.

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*

3 Terms and definitions

Editors´ Note: ISO/IEC JTC 1/WG 10 agreed to transfer the clause 3, Terms and definitions in ISO/IEC 30141 to ISO/IEC NP 20924 in the Shanghai meeting. WG 10 instructs the Project Editors of ISO/IEC NP 20924 to review the disposition of comments on clause 3 in ISO/IEC 30141 (WG10_N0315) and forward the result to the Project Editors of ISO/IEC 30141 after separating out the definitions for ISO/IEC 30141 and ISO/IEC NP 20924 no later than 2016-02-21. The updated revised WD with clause 3 will be published to the experts for comments and contributions after 2016-02-21.
Editor's Note: Continue to call for the new comments and contributions especially for the updated contents of clause 4-8.

4 Symbols and abbreviated terms

5Vs	Volume, Velocity, Veracity, Variability, and Variety
6LoWPAN	IPv6 over Low power Wireless Personal Area Network
AL	Application Layer
ASL	Application Support Layer
CAN	Control Area Network
CM	Conceptual Model
CRA	Communication Reference Architecture
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
RM	Reference Model
SCD	Sensing & Controlling Domain
ASD	Application Service Domain
SPI	Serial Peripheral Interface
SRA	Systems Reference Architecture

TCP/IP	Transmission Control Protocol/Internet Protocol
UML	Universal Modelling Language
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 (IoT RA) represented in this International Standard provides a conceptual model, reference model and reference architecture from different architectural views, common entities, high-level interfaces connecting the entities. 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.

The IoT RA serves the following goals:

- to describe the characteristics and general requirements of IoT systems;
- to define the IoT system's domains;
- to describe the conceptual model (CM) and reference model (RM) of IoT systems; and
- to describe interoperability of IoT system's entities.

Each IoT system will have specific system requirements that should be met, and the specific system requirements can vary from one IoT system to next per user group and/or domain. The IoT RA provides the generic parts as a 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;

187 — to provide a technology-neutral reference point for defining standards for IoT;
188 and

189 — to encourage openness and transparency in thedevelopment of a target IoT
190 system architecture development and in the implementation of the IoT system.

191 The IoT RA is also intended to:

192 — facilitate the understanding of the overall intricacies of IoT systems;

193 — illustrate and provide understanding of IoT reference architectures from
194 different architectural views;

195 — provide a technical reference to enable the international community to
196 understand, discuss, categorize and compare IoT systems;

197 — facilitate the analysis of candidate use cases/applications including
198 data/information flows; and

199 — facilitate the identifying of gaps in IoT-related standards in order to initiate the
200 standardization projects.

201

6 Characteristics of IoT systems

Editor's Note: According to the shanghai meeting, the following table shows the draft structure of listed characteristics, further comments and proposals from experts are required.

Grouping	1st Level
6.1 IoT System Characteristics	6.1.1 Auto-configurations (including autonomic networking, autonomic service capabilities, plug and play)
6.2 IoT Service Characteristics	6.2.1 Content-Awareness
	6.2.2 Context-Awareness (Including: location awareness, time awareness)
	6.2.3 Timeliness
6.3 IoT Component Characteristics	6.3.1 Composability
	6.3.2 Discoverability
	6.3.3 Modularity
	6.3.4 Network connectivity
	6,3,5 Shareability
	6.3.6 Unique identification
6.4 Compatibility	6.4.1 Legacy support
6.5 Usability	6.5.1 Manageability
	6.5.2 Well-defined components
	6.5.4 Flexibility
6.6 Reliability	6.6.1 Reliability
	6.6.2 Resilience
	6.6.3 Availability
6.7 Security & Privacy	6.7.1 Confidentiality

	6.7.2 Privacy
	6.7.3 Integrity
	6.7.4 Trust/trustworthiness
6.8 Other Characteristics	6.8.1 Data 5Vs – Volume, Velocity, Veracity, Variability and Variety
	6.8.2 Heterogeneity
	6.8.3 Scalability
	6.8.4 Regulation Compliance
	6.8.5 Consumer protection

206

207 ## 6.1 IoT System Characteristics

208 ### 6.1.1 Auto-configurations

209 #### 6.1.1.1 Description

210 Auto-configuration is the automatic configuration of devices based on the interworking
211 of predefined rules (associated algorithms based on data inputs). Auto-configuration
212 includes automatic networking, automatic service capabilities and plug & play. Auto-
213 configuration allows an IoT system to react on conditions and add and remove
214 components such as devices and networks. Auto-configuration needs security and
215 handshake mechanisms to make sure that only authorised components can be auto-
216 configured into the system. Security and handshake mechanism shall be arranged
217 appropriate for each market segments..

218 #### 6.1.1.2 Relevance to IoT systems

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

221 #### 6.1.1.3 Examples

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

224 ## 6.2 IoT Service Characteristics

225 ### 6.2.1 Content-Awareness

6.2.1.1 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.

6.2.1.2 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.

6.2.1.3 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.

6.2.2 Context-Awareness (location awareness, time awareness)

6.2.2.1 Description

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

6.2.2.2 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.

6.2.2.3 Examples

Support of location-based service which provides different services according to the location on a user.

In cases of emergency like fire at the arrival of the fire brigade the doors shall be unlocked. The security policy that governs the door's access can be enhanced with context. The context here is that an emergency situation is currently happening and first responders are in the vicinity. Based on these two contextual inputs the policy could unlock the door and provide access without the need to be properly authorized.

The ability to blend GPS information (date, time, altitude, and location) with sensor data (e.g. environmental monitoring, surveillance, etc.) will enable self-describing context to sensor output.

6.2.3 Timeliness

6.2.3.1 Description

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

6.2.3.2 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.

6.2.3.3 Examples

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

In an industrial manufacturing process, multiple production elements such as inputs, personnel, machines and support services are engaged and timely response among them is critical for order execution and dispatch, resource scheduling, production performance analysis, safety management and so on.

6.3 IoT Component Characteristics

6.3.1 Composability

6.3.1.1 Description

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

6.3.1.2 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.

6.3.1.3 Examples

Editor's Note: Contribution requested.

6.3.2 Discoverability

6.3.2.1 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, security, safety and privacy.

6.3.2.2 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 in accordance with predefined different security classification / authentication for each market segments. 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.

6.3.2.3 Example

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

6.3.3 Modularity

6.3.3.1 Description

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

6.3.3.2 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.

6.3.3.3 Examples

Editor's Note: Contribution requested.

6.3.4 Network connectivity

6.3.4.1 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).

6.3.4.2 Relevance to IoT systems

IoT systems rely on the ability to exchange information units in 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, authentication and authorisation.

6.3.4.3 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, 6LoWPAN, 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).

6.3.5 Shareability

6.3.5.1 Description

The ability to use individual components in multiple interconnected systems.

6.3.5.2 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.

6.3.5.3 Examples

Motion detection capabilities of a lighting control system would be leveraged by the security system to increase the security systems capability.

6.3.6 Unique identification

6.3.6.1 Description

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

6.3.6.2 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.

6.3.6.3 Examples

IPv4, IPv6, URI, and Fully Qualified Domain Names (FQDNs) are used as unique, unambiguous identification in the Internet applications. These identifications may guarantee and allow routing to and accessing devices of interest. Additionally, the identifications can provide effective managing of physical and virtual objects. All these allowed by identification is to satisfy end-users by IoT system's services provided.

6.4 Compatibility

6.4.1 Legacy support

6.4.1.1 Description

A service, protocol, device, system, component, technology, or standard that is outdated but which is current use and thus needs to be incorporated into an IoT system..

6.4.1.2 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.

6.4.1.3 Examples

Editor's Note: Contribution requested.

6.5 Usability

6.5.1 Manageability

6.5.1.1 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.

6.5.1.2 Relevance to IoT systems

Many IoT devices, networks, and systems are unmanned and run automatically. Special care must be taken to ensure that the systems remain manageable even when the system malfunctions on certain areas of operation or is unstable or miscalibrated in certain areas of operation.

6.5.1.3 Examples

Devices including smoke sensors are deployed in various locations of buildings. These devices are hard to maintain because of their locations. Any type of malfunction could cause undesirable events and consequences. Thus, the manageability should be configured from the system design and throughout development of the system. The configured manageability component may include device state monitoring component, the link monitoring component, the calibration component, etc.

6.5.2 Well-defined components

6.5.2.1 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.

6.5.2.2 Relevance to IoT systems

The components are used to assemble an IoT system. They will be discovered through an information system interface and information about the component may not 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 will meet its design goals.

6.5.2.3 Examples

Editor's Note: Contribution requested.

6.5.3 Flexibility

6.5.3.1 Description

Editor's Note: Contribution requested.

6.5.3.2 Relevance to IoT systems

Editor's Note: Contribution requested.

6.5.3.3 Examples

Editor's Note: Contribution requested.

6.6 Reliability

6.6.1 Reliability

6.6.1.1 Description

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

6.6.1.2 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 and industrial manufacturing operations.

6.6.1.3 Examples

Support of integrity checking techniques. Data reliability is of utmost importance for the decision making processes of IoT systems. Communication reliability is important for ensuring the availability of data/devices.

6.6.2 Resilience

6.6.2.1 Description

Resilience is the ability of the system to recover from faults and failures.

6.6.2.2 Relevance to IoT systems

Communication, device or software failures are relative commonplace in IoT systems and can escalate quickly causing the global failure of the system. Thus, IoT systems have to incorporate self-monitoring and self-healing techniques to improve the system resilience.

6.6.2.3 Examples

The IoT system has to be resilient to gateway failures to ensure the data availability.

6.6.3 Availability

6.6.3.1 Description

Availability is the ability of the system to function as required during a period of time.

6.6.3.2 Relevance to IoT systems

In IoT systems, availability can be seen in terms of devices, data and services. Availability of devices is related with their network lifetime and the reliable connectivity of the devices. Availability of the data is related with the ability of the system to get the requested data from a system component. Availability of services is related with the ability of the system to provide the requested service to users with a pre-defined QoS. [RERUM D2.2]

6.6.3.3 Examples

In some critical applications, i.e. health monitoring or intrusion detection, devices and data have to be always available so that alarms can be sent to the system immediately when raised.

6.7 Security & Privacy

6.7.1 Confidentiality

6.7.1.1 Description

The property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. (Excerpt from ISO27000)

6.7.1.2 Relevance to IoT systems

In an IoT system the confidentiality protection is responsible to prohibit other network participants to read data or control messages when they are not the intended recipients. Apart from it being a pre-requisite for a secure operation especially when the data to be transmitted contains secret tokens, e.g. for access control, confidentiality is required to enable privacy: Confidentiality of PII must be confidentiality protected before sent over the potentially insecure channels (many IoT communication are done wireless or over the Internet) to reach only the intended (and consented) recipient.

6.7.1.3 Examples

The neighbour or a burglar is not able to read the actual value of the room temperature sensors to infer if somebody is home. All the attacker sees is random looking data that might still be identifiable as originating from a temperature sensor (protection from this would require anonymous communication).

6.7.2 Privacy

6.7.2.1 Description

Privacy protection, a.k.a, as ‘privacy’ and ‘data protection’ is a legal/regulatory requirement whenever an IoT system involves ‘personal information’ anywhere in its operation.

Privacy is the ability of an individual human to be left alone, out of public view, and in control of information about oneself. The concept of privacy overlaps, but does not coincide, with the concept of data protection. With respect to data protection it ensures that PII is not gathered or processed or disclosed to unauthorized entities. In this

context, entities include both individuals and processes. If PII is disclosed it must be based on prior informed consent given by the PII principal.

6.7.2.2 Relevance to IoT systems

Many IoT systems do not collect or interchange recorded information, i.e., data on or about an identifiable individual, i.e., personal information. However, any `IoT system which does collect, receive and/or interchange personal information needs to ensure that in such IoT systems (and their interactions) with other IoT systems (or IT systems in general) are in full compliance with privacy protection requirements of applicable jurisdictional domains. Privacy protection is a right of an individual and an obligation on an organization (or public admonition) where the latter collects, receives, interchanges, etc. personal information. From n international common requirements perspective that are eleven (11) common privacy protection principles.1. In addition to the key principle of "Informed Consent", privacy protection requirements also require that timeliness, accuracy, relevance and integrity of personal information be maintained throughout its life cycle.

What constitute each individual's privacy might be different among individuals. It might be different due to legal, social or cultural norms. However when end-users give away data about themselves and it is used for a different purpose than for which they understood it being used at the time of release, than this is a breach of privacy.

Being able to fully respect the privacy is thus essential for the societal and legal acceptation of IoT systems by the public.

6.7.2.3 Examples

A key target market for the application and use of things in IoT are those where an individual is the end-point linked to a "thing" in an IoT context. Here the use of a smartphone (and associated apps) used by an individual represent a key example. This is in addition, to existing use of computers, tablets. And other smart devices by individuals. One notes that there is a continuing dynamic between ensuring privacy protection on the one hand, and on the other that of organization (public and private sector) wanting access and use of personal information for business, national security, law enforcement, etc. purposes. Addressing issues of this nature is outside of the scope of this standard. However the IoT-RA sis designed to be able supports there real world requirements.

The end-user wants to share his monthly energy consumption data with his energy provider for billing purposes, he also needs to share – in a more timely manner e.g. every hour – the current load to allow the grid provider to maintain the grid's health. This data could be emitted by separate services and would come with different access control policies due to different consents given by the PII principal.

Different example, the end-user wants to participate in participatory sensing of traffic jams, obviously he does not want the IoT to detect his whereabouts in any detail unnecessary for the application to work.

6.7.3 Integrity

6.7.3.1 Description

Data integrity is the property that data has not been altered or destroyed in an unauthorized manner [ISO_27040:2015--3.9]

6.7.3.2 Relevance to IoT systems

Data integrity is highly related to IoT to ensure that the data that are used for decision making processes of the system have not been altered by unauthorized or malicious users/devices. The protection of the integrity of the data is a key requirement to ensure the security of the IoT system.

6.7.3.3 Examples

In IoT deployments that comprise of multi hop wireless sensor networks there is a threat that intermediate nodes may alter the data and this can have impact on the decisions of the system. For example, an intermediate node may increase the value of the temperature of a room which will make the air-conditioning system to work in a higher mode.

6.7.4 Trust/trustworthiness

6.7.4.1 Description

Trustworthiness is degree to which a user or other stakeholder has confidence that a product or system will behave as intended [ISO25010:2011, 4.1.3.2].

6.7.4.2 Relevance to IoT systems

Editor's Note: Contribution and comments requested.

device, data and service trustworthiness is of utmost importance for IoT systems to ensure that only trusted devices will participate in the decision making process of the system, resulting in the provision of trustworthy applications.

6.7.4.3 Examples

Editor's Note: Contribution requested.

If there is an IoT application that gives the average measurement of a room considering the mean value reported by 5 sensors, if 2 sensors report false values (either they are misbehaving/faulty or malicious) the resulting mean measurement will be false. By having mechanisms that evaluate the trustworthiness of the data/devices the false measurements will not be taken into account.

6.8 Other Characteristics

6.8.1 Data 5Vs – Volume, Velocity, Veracity, Variability and Variety

6.8.1.1 Description

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

6.8.1.2 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.

6.8.1.3 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.

6.8.2 Heterogeneity

6.8.2.1 Description

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

6.8.2.2 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.

6.8.2.3 Examples

Smart container using RFID tags and sensors needs interaction of RFID systems and sensor network systems.

6.8.3 Scalability

6.8.3.1 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.

6.8.3.2 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.

6.8.3.3 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.

6.8.4 Regulation Compliance

6.8.4.1 Description

Editor's Note: Contribution requested.

6.8.4.2 Relevance to IoT systems

Editor's Note: Contribution requested.

6.8.4.3 Examples

Editor's Note: Contribution requested.

6.8.5 Consumer protection

6.8.5.1 Description

"Consumer protection" pertains to the need to support applicable legal/regulatory requirements whenever an IoT system (or interconnected IT systems) involves a consumer anywhere in its operation.

NOTE 1: In many jurisdictional domains, consumer protection requirements apply only to individuals. In some jurisdictional domains "consumer protection "also applies to organizations, i.e., legal or artificial Persons.

NOTE 2: In those jurisdictional domains which define consumer protection focussed on individuals that is an overlap, i.e. complimentary between consumer protection and privacy protection requirements with respect to "personal information"

6.8.5.2 Relevance to IoT systems

A major development and one of the driving forces in the expansion of IoT is that of manufacturers of physical products imbedding "things" with Internet WiFi capability to connect via an IoT system in the products which they sell.

A such these embedded devices in products collect, receive, and/or transmit data with respect to the device bought by a consumer and as such shall comply with applicable consumer protection requirements. Here is recognized that with respect to collect, use, EDI of personal information, many of the legal/regulatory requirements pertaining to consumer protection are similar in nature to those of privacy protection requirements, there are differences (However these are beyond the scope of this IoT standard.)

Nevertheless there are consumer protection issues which an IoT must be able to address Examples here include whether or not a consumer agrees to the activation/use of an IoT

device imbedded in the product purchased, whether or not having / using an thing in IoT and allowing it to be connected to the product/service provider is a condition or sale or lease, etc.

6.8.5.3 Examples

An individual purchases a (high-end) refrigerator/ freezer. It includes an imbedded chip with Wi-Fi capabilities and which is automatically activated when the fridge is turned one. The customer is informed that its purpose is to monitor the effective functioning of the fridge which in turn is linked to the warranty & maintenance contract associated with the purchase of the fridge. If the customer wishes he/she can link this "thing" to the home Wi-Fi network in order to establish a direct Internet connection between the fridge operation and the manufacturer (or warranty/maintenance service provider).

However, the customer needs to be fully informed of this service before agreeing that this device in its home is linked to IoT. A customer may refuse to have one or more of its devices to be linked to an IoT. Many other examples of a similar nature can be provided.

7 IoT Conceptual model

Editors' note: all diagrams and texts have been updated based on the discussion and consensus made at meeting in shanghai. WG10 decided to move security related description to entity based reference model in architecture chapter. Further contributions or suggestions of proposed change are required

7.1 Main purpose

The conceptual model (CM) provides common structure and definitions for describing the concepts of and relationships among 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 is the big picture of the overall IoT entities and their relationships?
2. What are the key concepts in a typical IoT system?
3. What is the relationship between the entities, especially between digital entities and their physical entities?
4. Who and where are the actors?
5. How the things and services are collaborated through network?

The following clauses describe the conceptual reference model focusing on above five points. The models presented here use simplified Unified Modelling Language™ (UML®, hereafter "UML"). Clause 7.2 provides a short description of the simplified UML in order to help readers to better understand CRM diagrams presented in this standard.

7.2 Interpreting model diagram

In this standard, UML[1] Class diagrams have the following restrictions:

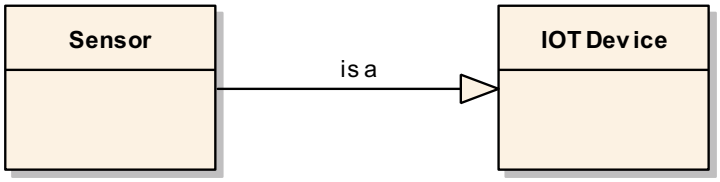
— Concepts are represented as UML Classes with no attributes.

— 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 IoT device. This generalization relationship can be expressed as shown in Figure7-1:

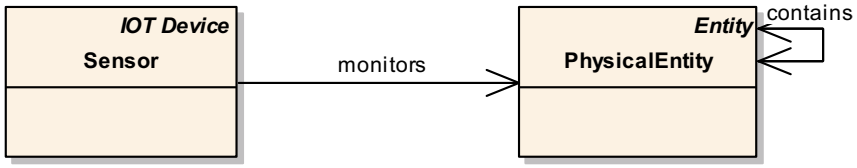
[1] ISO/IEC 19501:2005(en) Information technology — Open Distributed Processing — Unified Modeling Language (UML)



694

695 **Figure7-1. Generalization.**

696 2. Directed association (expresses relationship between concepts. These
697 association names are verbs.). Figure 7-2 expresses the association relationship
698 that Sensor monitors Physical Entity (the thing).



699

700 **Figure 7-2. Association.**

701 Cardinality constrains on association ends are not shown. They vary from one kind of
702 association to another, but can be inferred from the Descriptions in following clauses.

703 If a concept, which is a generalization of a concept on the diagram, is not itself shown on
704 the diagram, the name of that generalized concept appears in italics at the top right
705 corner of the box as shown in Figure7-1("*Physical Entity*") and Figure 7-2 ("*IoT device*").

7.3 The big picture

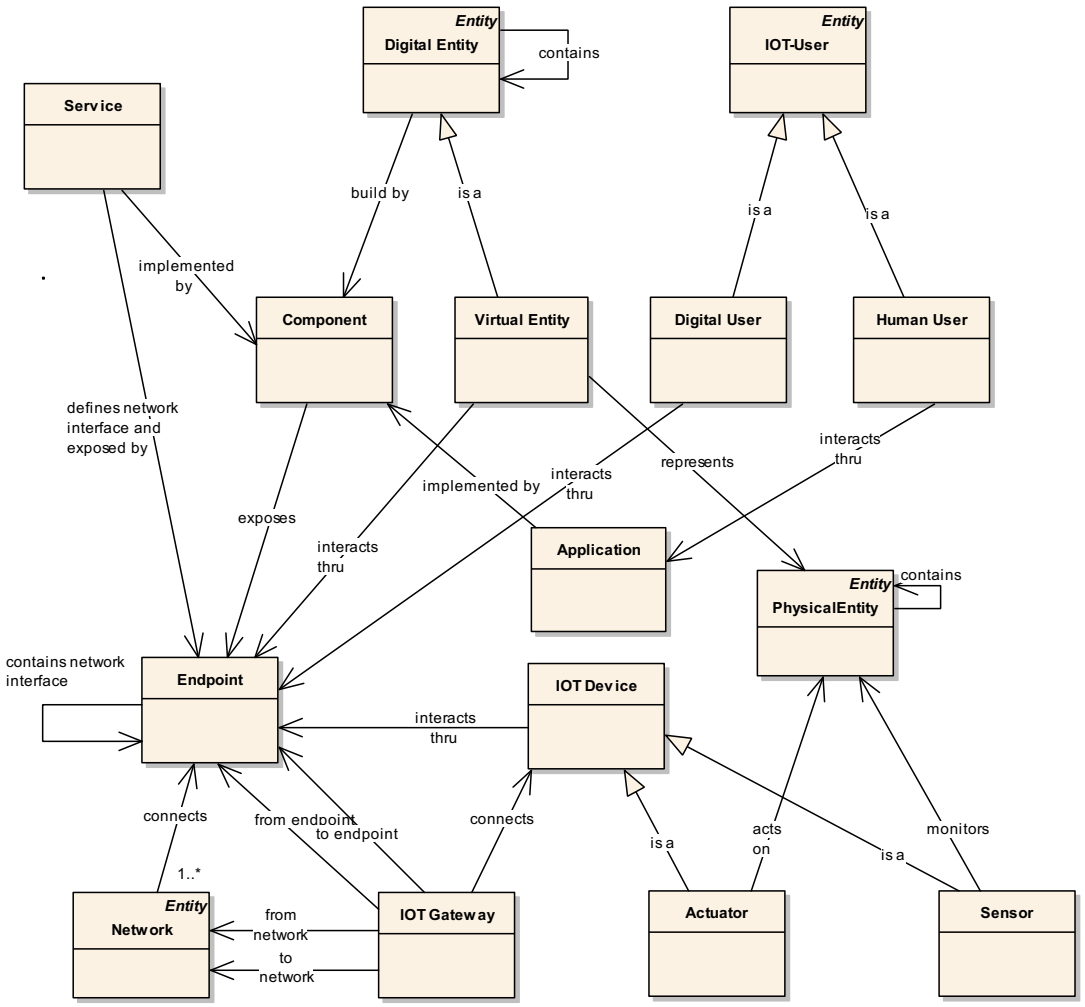


Figure 7-3. Big Picture for IoT Concepts of the CM.

The model diagram in Figure 7-3**Error! Reference source not found.** provides the big picture of all key IoT entities defined in this CM, their relationships and their interactions. IoT-User can be human (human user) or non-human (digital user) such as roboter or automation services, which act on behalf of human user. Digital user consumes remote services through endpoint, which is attached to the communication network, while human user interacts through applications, which can communicate with services via network. Physical entity here is the thing which is to be controlled or monitored by actuator and sensor. Virtual entity represents physical entity in IT world. Both actuator and sensor are kind of IoT device. IoT devices may interacts through endpoint to have network communicate directly or needs to be connected with IoT gateway first if itself does not have communication capabilities. Services are implemented by components and they can be located everywhere. Services can be discovered and consumed via different types of networks through endpoint.

The following clauses describe more details of entity and its relationship with focus on its key concepts.

7.4 Concept

7.4.1 IoT Entities and domains

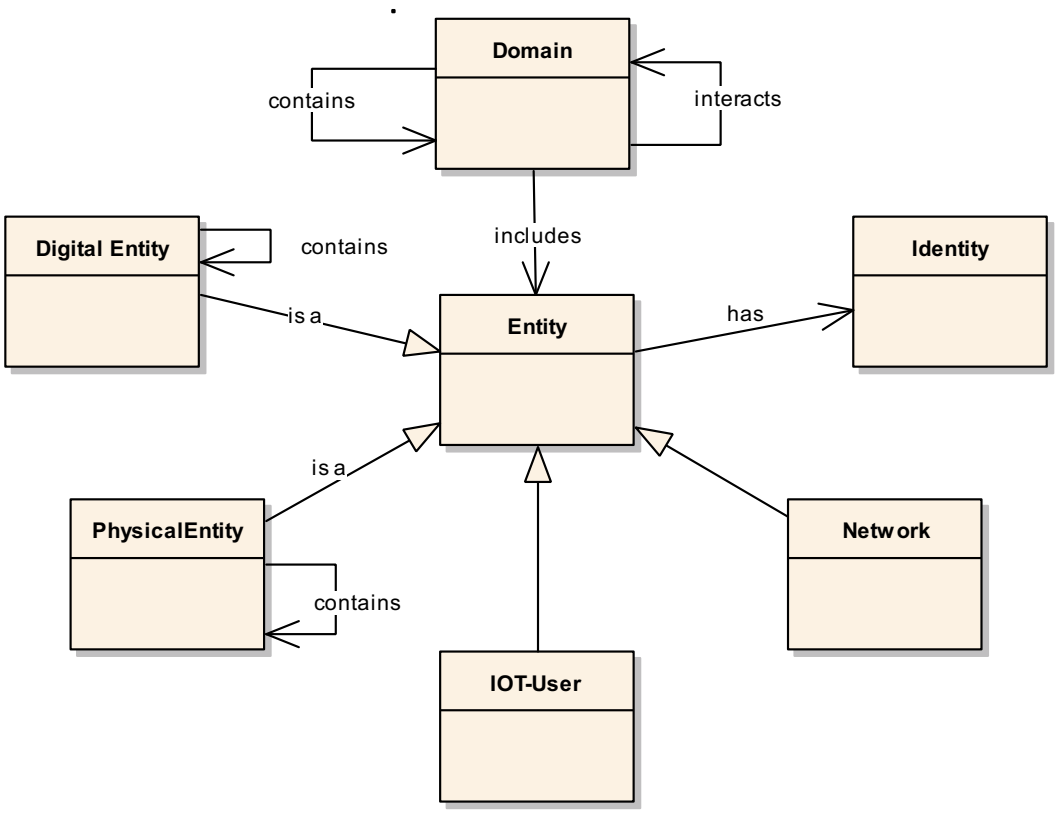


Figure 7-4. Entity and Domain Concepts of the CM.

Figure 7-4 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. Actually every entity is physical. In order to have a simple concept about IoT entities and its relationship, four fundamental entities are defined here, the thing (Physical Entity), the user (IoT-User), IT systems (Digital Entity) and the networks (Network).

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. IoT-User is an entity which can be human or non-human, while physical entity is discrete, identifiable and observable, which is interested by IoT-User. 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 7-5shows that one IoT domain A interacts with another IoT domain B. Of course, one IoT domain can also interact with multiple IoT domains.

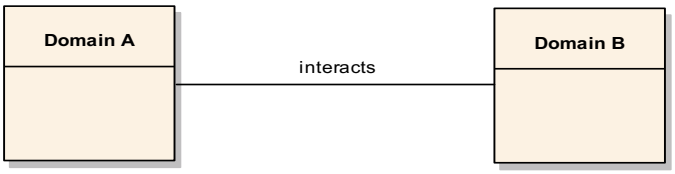


Figure 7-5. Domain Interactions of the CM.

Domain is composed of various types of entity. Sometimes one large domain can be segmented into more sub-domains. Figure 7-6shows that Domain A contains two sub domains, Domain C and Domain D.

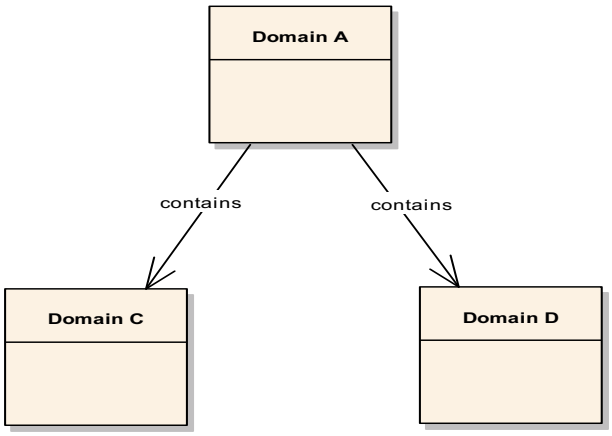


Figure 7-6. Domain Composition of the CM.

Following sub clauses 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.

7.4.1.1 Entity

The Conceptual Model defines the following relationships from this concept.

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

7.4.1.2 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

765

766 #### 7.4.1.3 Digital entity

767 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.
2	Association	Digital Entity	A Digital Entity may contains other Digital Entities

768

769 #### 7.4.1.4 Physical entity

770 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

771

772 #### 7.4.1.5 IoT-User

773 The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Generalization	Entity	An IoT-User is specialization of Entity representing a human user or digital user.

774

775 #### 7.4.1.6 Network

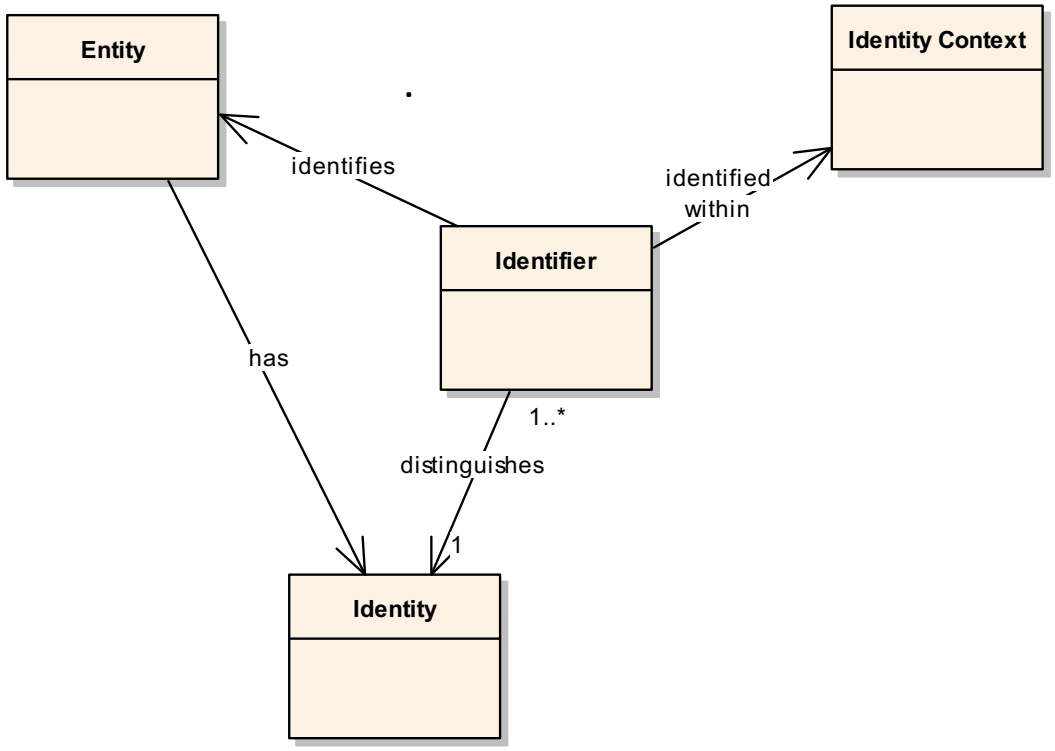
776 The Conceptual Model defines the following relationships from this concept.

Nr	Relationship	Related Concept	Description

	Type		
1	Generalization	Entity	A Network is a specialization of Entity.

777

778 ### 7.4.2 Identity



779

780 **Figure 7-7.Identity Concept of the CM**

781 Figure 7-7 shows the identity concept. Most entities in IoT especially physical entity
782 ("Thing") need identity. Identifiers can be understood as a dedicated, publicly known
783 attribute or name for an identity, a person or a device. Typically, identifiers are valid
784 within a specific context. Thing can have more than one identifier, but it requires at least
785 one unique identifier within any environment or context through which it can be
786 accessed. For example, identity information from a Tag can be used as Identifier to
787 identify the Physical Entity to which it is attached.

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

792 #### 7.4.2.1 Identifier

793 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. Identity may have more than one identifiers
3	Association	Identity Context	Identifier identified with a given identity context

7.4.3 Services, components, and endpoints

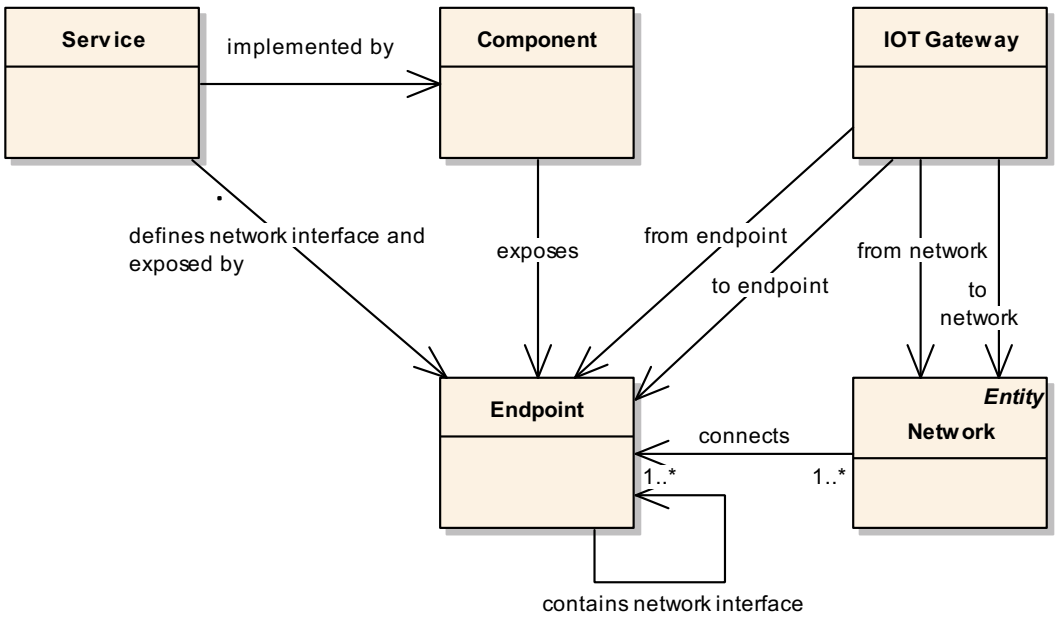


Figure 7-8. Service, Component, and Endpoint Concepts of the CM.

Figure 7-8 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 exposes zero or more endpoints by which they can be invoked. An Endpoint has one or more network interfaces. Services, which are located remotely, can be reached by endpoint through network interface across the communication network. 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.

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.

7.4.3.1 Components

The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Association	Endpoint	A Component exposes endpoint.

813

814 **7.4.3.2 Endpoint**

815 The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Association	Endpoint	An Endpoint may contain more than one network Interface.

816

817 **7.4.3.3 IoT Gateway**

818 The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Association	Network	The network from which interactions are forwarded.
2	Association	Network	The network that interactions are forwarded to
3	Association	Endpoint	An Endpoint from which interactions are forwarded
4	Association	Endpoint	An Endpoint that interactions are forwarded to

819

820 **7.4.3.4 Service**

821 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.

822

7.4.4 IoT User

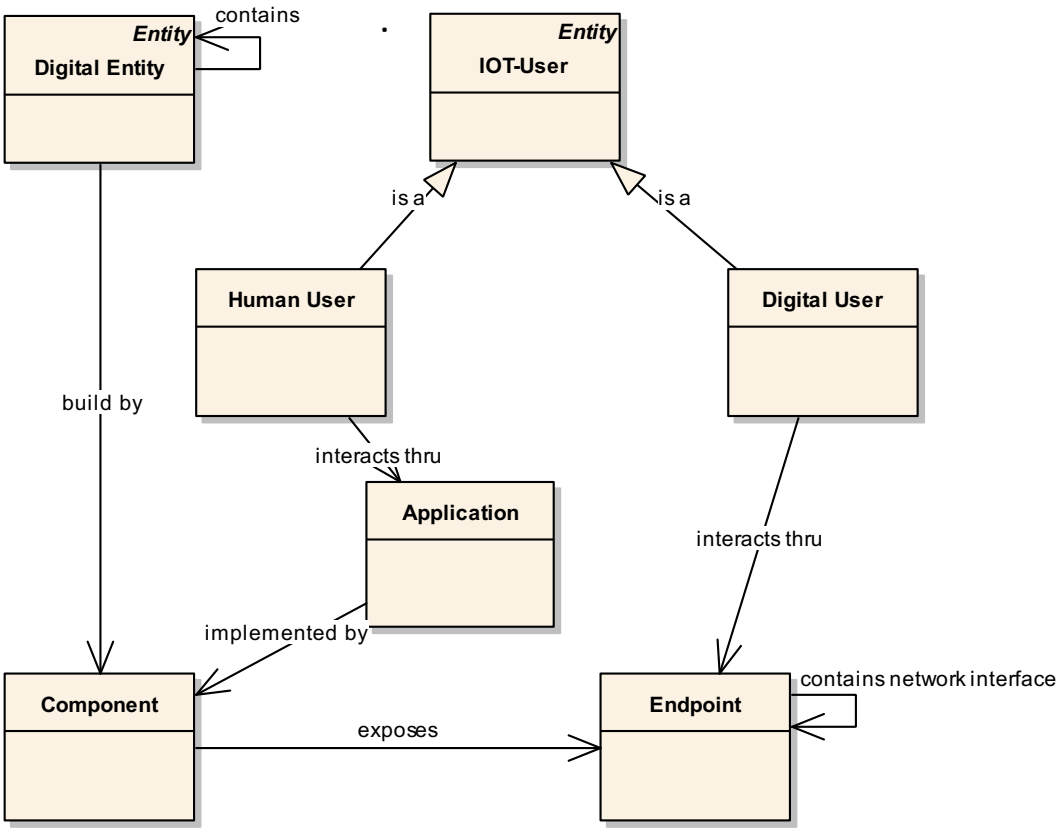


Figure 7-9. IoT User Concepts of the CM.

As shown in Figure 7-9, 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. Digital user interacts with a physical entity directly or indirectly through the endpoint. IoT user also uses endpoint to communicate with other IoT user or services in the network.

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.

7.4.4.1 Human user

The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Generalization	IoT User	A Human User is also a specialization of an IoT user
2	Association	Application	A Human User interacts across the

			Network thru an application.

838

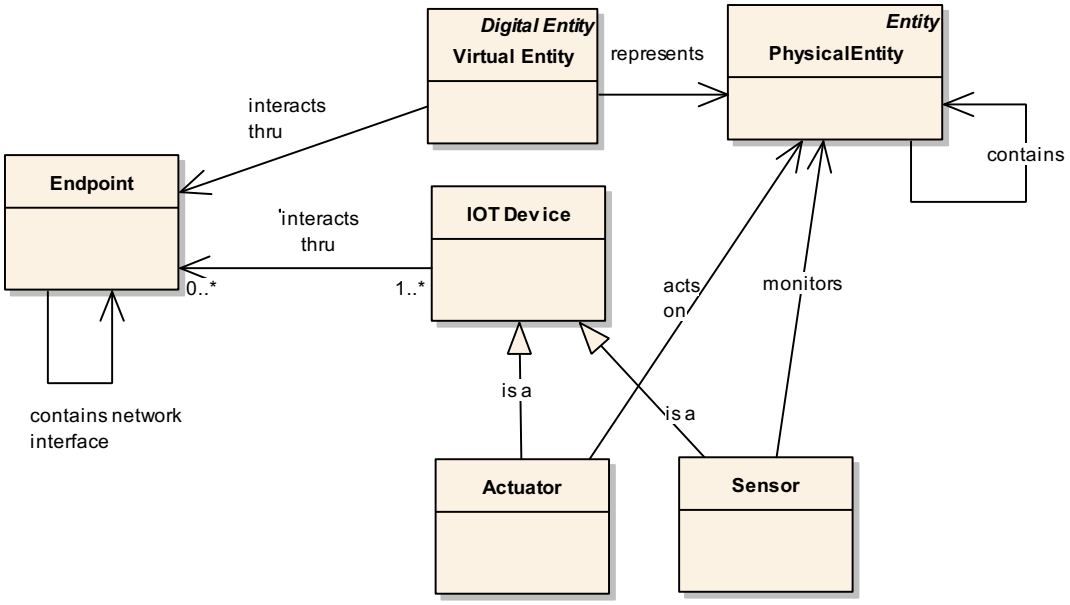
839 ### 7.4.4.2 Digital user

840 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	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.

841

842 ## 7.4.5 Virtual entities, digital entities, and IoT devices



843

844 **Figure 7-10. Virtual Entity, Digital Entity, and IoT device Concepts of the CM.**

845 Figure 7-10 shows the relationship between virtual entity, physical entity and IoT
846 device. Digital entity can be considered as an assembly of certain components. Actuator
847 and Sensor are the components which have direct or indirect contact with Physical
848 Entity. Actuator executes digital information to alter some property of a physical entity.
849 Sensor perceives certain characteristics of the real world and transfers them into a
850 digital representation. Actuator and Sensor are kind of IoT device, which converts
851 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 smartphone 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 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.

7.4.5.1 IoT device

The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Association	Endpoint	A IoT device 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 IoT device capabilities.

7.4.5.2 Sensor

The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Generalization	IoT device	a Sensor is a specialization of IoT device
2	Association	Physical Entity	A Sensor monitors a Physical Entity

7.4.5.3 Actuator

The Conceptual Model defines the following relationships from this concept.

Nr	Relationship Type	Related Concept	Description
1	Generalization	IoT device	An Actuator is a specialization of IoT device
2	Association	Physical Entity	An Actuator acts on a Physical Entity.

8 Internet of Things reference models (IoT RM) and reference architectures views (IoT RA)

Editor Notes: The text has been discussed and updated in Shanghai meeting based on the disposition of comments. Continue to call for the new contribution and comments.

Editor's Note: Recommendation 65 from WG10 4th Meeting in Shanghai, ISO/IEC JTC 1/WG 10 approves the establishment of an ad-hoc group for reviewing the different views of RA on IoT based on the new revised WD of ISO/IEC 30141. The Terms of Reference of ad-hoc group are to determine the number of views, purpose and contents.

8.1 Relation between CM, RMs and RAs

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 or domains (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 connections, interrelations and interactions with each other and with functions located outside of predefined architecture patterns representing the entities and functions.[2]

Figure 8-1 shows the architecture continuum from the CM, entity-based RM, domain-based RM, finally to a number of different views of RA. The consistent architecture continuum should be maintained not only in this hierarchy (e.g., CM → RM → RA) but also in evolutionary updates over time and it should be clearly understood through effective way of documenting the architecture descriptions.

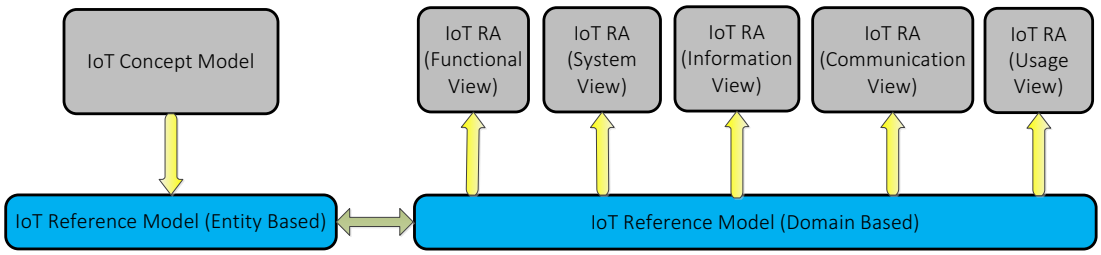


Figure 8-1. Relation between IoT concept model, reference model, and reference architectures.

In this standard, after examining various kinds of deployed IoT systems and developed 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 domains provides an effective and representative Reference Model (RM) of the IoT systems for the various purposes and uses of the RM.

8.2 IoT Reference models

8.2.1 Entity-based reference model

A composite entity-based reference model of IoT systems is shown in Figure 8-2. This figure illustrates the activity interaction using arrowhead lines between the entities. Each arrowhead line is described with a concise, representative activity description to convey the activity relationships in Figure 8-2.

[2] 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.

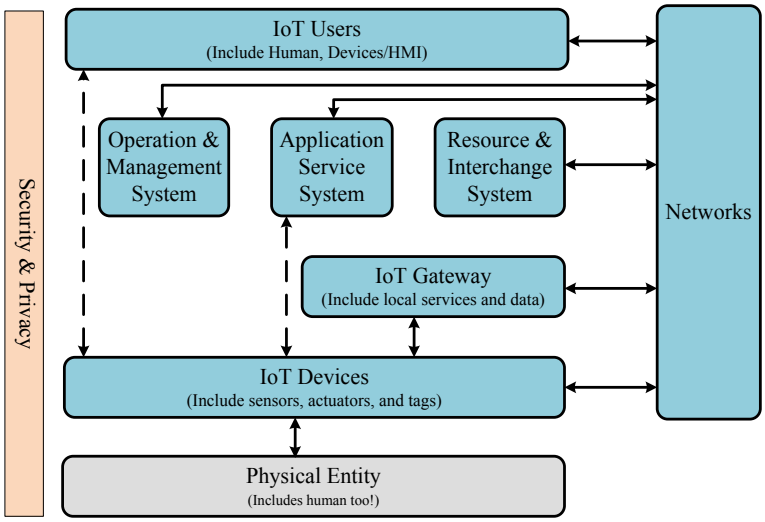


Figure 8-2. IoT reference model (Entity-based).

Based on the study of system decomposition of various IoT systems in different application scenarios, Figure 8-3 extracts 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.

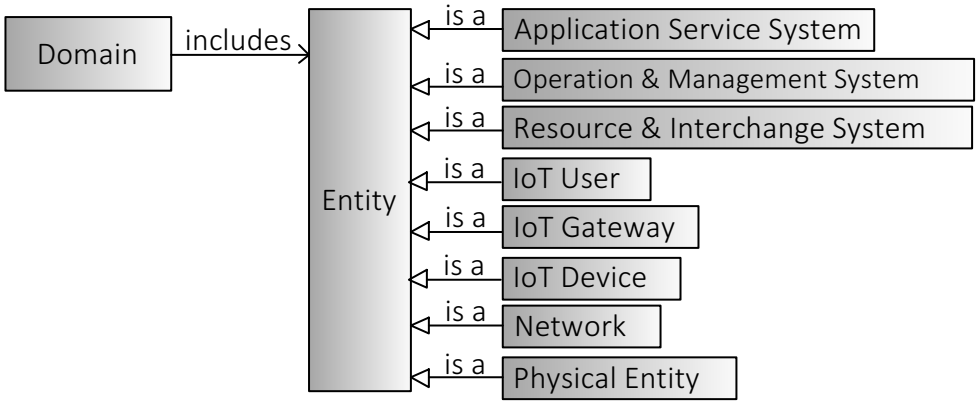


Figure 8-3. Domain and entity relationship, and representative conceptual entities in the IoT systems.

8.2.1.1 IoT device

Editor Note: Tag/Tag reader has been removed, and looking for further contribution from SC31.

An IoT device is the technical artefact for bridging the real world of physical entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, computation, storage, communicating and processing capabilities [3]. An IoT device is attached to or in proximity to physical entity. In certain situations, IoT devices can be structurally embedded in physical entity. In other situations, IoT devices, especially Sensor, can be located away from physical entity and monitoring the Physical entities from a distance.

In the IoT systems, there are some basic types of IoT devices, and they are identified in Figure 8-4. These devices take vital role in the IoT systems for providing the technological connection for interacting with, or gaining information about the physical entity, enhancing the physical entity 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 8-4 shows the key IoT devices in an IoT system. Meanwhile, Table 8-1 provides the description for each type of IoT Devices.

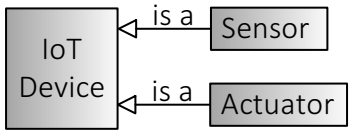


Figure 8-4. The key IoT devices.

Table 8-1. Description of the IoT devices shown in Figure 8-4.

IoT Device	Description
Sensor	Sensor provides the data and/or information about the physical entity being monitored. Information in this context ranges from the identity of the physical entity to measures of the physical state of the physical entity. Sensors can be attached or embedded in the physical structure of the physical entity. Or, sensors can be placed in the environment away from the physical entity performing non-contact or remote sensing.
Actuator	Actuators manipulate or alter physical entities' 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 engage thrusters in a satellite) or alter its environment by certain types of actuators. Some actuators can activate or deactivate functionalities of a physical entity or a group of physical entities. There are three types of actuators: (1) mechanical actuator; (2) electronic actuator; (3) virtual actuator.

8.2.1.2 Network

Various types of networks are used in the IoT systems. All types of networks are represented by the Network entity. This entity represents various types of devices that allow the connectivity from one network to another network, from one domain to another domain, and so on. The devices belonging to this entity are routers, endpoint, etc.

8.2.1.3 IoT Gateway

IoT Gateway is a forwarding device enabling the connections between the sensing or actuating subsystem in the real environment and other subsystems.

8.2.1.4 Physical Entity (Things)

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.

8.2.1.5 Operations & Management System

The Operations & Management System is an integrated physical/virtual entity system which observes, operates, maintains, and manages all IoT system assets including, but not limited to, networks, IoT environments, IoT devices, etc.

8.2.1.6 Resource & Interchange System

The Resource & Interchange System is an integrated physical/virtual entity system supporting IoT system's external connectivity with 3rd party suppliers, markets, and temporary stakeholders of the IoT system.

8.2.1.7 Application Service System

The application service system is an integrated physical/virtual entity having various applications in order to provide IoT services to IoT User.

8.2.1.8 IoT User

The IoT User is an individual human user or various sizes 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.

8.2.2 Domain-based reference model

8.2.2.1 Introduction

Figure 8-5 shows the domain representation of the IoT system reference model. The domain-based RM is composed of User Domain (UD), Operations & Management Domain (OMD), Application Service Domain (ASD), Resource & Interchange Domain (RID), Sensing & Controlling Domain (SCD), and Physical Entity Domain (PED).

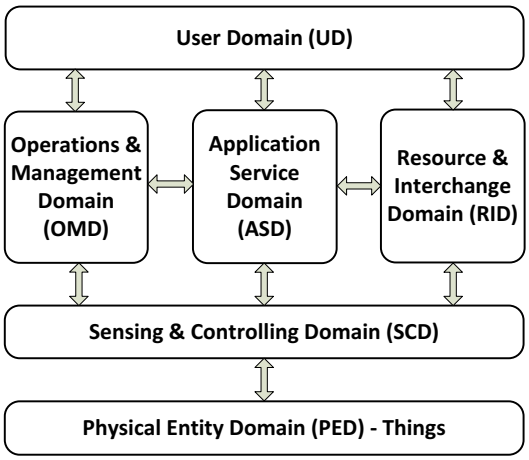


Figure 8-5. IoT reference model (Domain-based).

Each identified domain is mutually exclusive from the other domains. The IoT system's environment is mainly formed by the PED, but in certain situations, part of the SCD entities can be allotted as a part of the environment. Hardware (i.e. physical entities) and software (i.e. virtual entities) appear in the domains other than the PED and the SCD. These hardware and software in theses domains other than the PED and the SCD 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 domain-based RM 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 interoperability from one network to another.

The network mainly provides 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, domains, and IoT systems, respectively.

The networks and communication connectivity is accomplished by wire-line or 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 form the network/communication infrastructure of an IoT system.

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

8.2.2.1.1 The user domain (UD)

Users are the stakeholder/actor of the User Domain (UD). 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.).

8.2.2.1.2 The physical entity domain (PED) - Things

The physical entity domain (PED) is constituted of physical entities that are "the things within the purview of an IoT system." Therefore, the PED 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 PED can be a myriad of different kinds of physical and virtual entities.

The stakeholder is an owner or owners of the PED, yet, this stakeholder may not show up as an entity in the PED. A person or persons can be one of the objects in the PED.

8.2.2.1.3 The sensing & controlling domain (SCD)

Sensing and controlling domain (SCD) is the most essential domain of an IoT system because the SCD provides critical data and information about an environment (i.e. physical entity domain, PED) to all other domains of an IoT system.

8.2.2.1.4 The operations & management domain (OMD)

System operators and managers are the stakeholders/actors of the OMD. The operators and managers maintain overall health of IoT system(s).

The OMD represents the collection of functions responsible for the provisioning, managing, monitoring and optimizing the systems' operational performance in real-time.

The OMD includes several functional components for the IoT system operations: Provisioning and Deployment functional component consists of a set of functions required to configure, on-board, register, track assets, and to deploy and withdraw 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.

8.2.2.1.5 The 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.

The RID interacts with the external entities, applications/services, and/or systems in terms of "resources." The resource can be physical, monetary, and digital (e.g., data/information) depending on transactions executed through the RID.

From the perspective of the digital resources (e.g., data), the domain-based RM has an underlying data layer covering all six domains because the data is generated and consumed in a distributed fashion by all domains in the RM. In order to achieve its role, the RID needs access to the digital resources (e.g., data) by permission of other domains (e.g., the UD, the OMD, the ASD, and the SCD). Thus, this particular RID role can be viewed as the RID having a pseudo-information database domain. The actual data processing such as data "analytics" are performed typically in the ASD, and the results of the processing is stored in the service providers' database. In the RID, if required, additional data processing is performed to accommodate the external organizations. These additional processing may include ensuring quality of data, data transformation, distribution and storage.

8.2.2.1.6 The Application Service Domain (ASD)

Application service providers are the stakeholder/actor of the ASD. Application service provider organizations provide services to the users in the UD. The ASD has a set of applications that forms an application domain within the ASD.

The ASD 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. Users) in the UD to fulfil the users' requests, but also with the sensors/actuators/readers in the SCD to gain data from objects (i.e. environment that an IoT system is responsible for) in the PED. Additionally, the ASD interacts with the OMD if an OMD stakeholder becomes a client of a service provider in the ASD directly or indirectly (e.g., through a user's request). The service providers in the ASD are likely to interact with the external organizations (e.g., other IoT systems, IoT platform, law enforcement, utility, financial institutions, government, etc.) via the RID.

The application service providers form a business domain within the ASD. The business domain functions enable end-to-end service operations of the IoT systems by integrating those functions with traditional or new types of IoT specific business functions.

8.2.3 Relation between the two reference models

Based on the entity-based RM in Figure 8-2 and the domain-based RM in Figure 8-5, a mapping relation between these two RMs can be achieved as shown in Figure 8-6, Where these two RMs are consistent with each other.

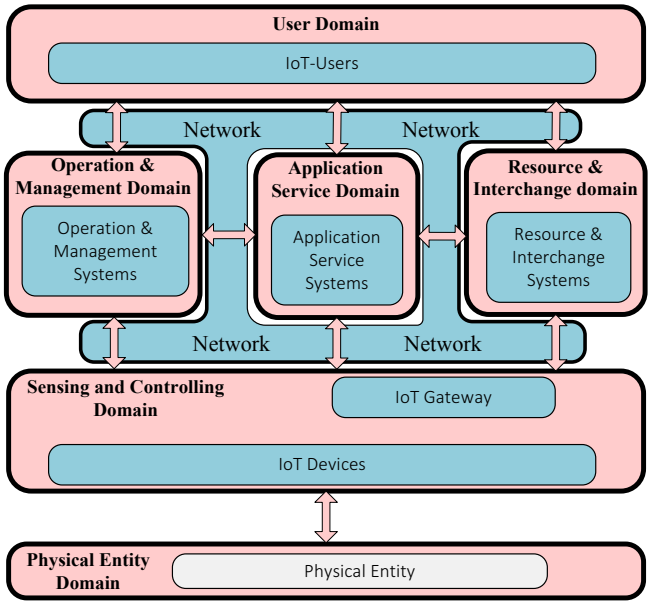


Figure 8-6. Relation between the concept model and the reference model.

Following Figure 8-6, the corresponding relationship between the entities in the entity-based RM and the domains in the domain-based RM is listed in Table 8-2.

Table 8-2. The corresponding relationship between the entities in the entity-based RM and the domains in the domain-based RM.

Entities in Entity-based RM	Domains in Domain-based RM
IoT User	User Domain (EUD)
Application Service System	Application Service Domain (APD)
Operations & Management System	Operations & Management Domain (OMD)
Resource & Interchange System	Resource & Interchange Domain (RID)
IoT Device	Sensing & Actuating Domain (SAD)
IoT Gateway	
Physical entity	Physical entity Domain (PED)
Networks	Communication and interactions among the domains

8.3 IoT Reference architecture (IoT RA) views

Editors' Note: According to the comment from WG10 4th Shanghai meeting, the simple introductions for different reference architecture views are added here. Call for comments and contribution about current five views.

Editors' Note: Call for comments to review all the views and decide which views should be included.

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

a) IoT RA Functional View. 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;

b) IoT RA System View. The system view describes the generic functional devices and systems in each domain to form an IoT ecosystem and support of functions components in the functional view. The entities in each domain can be very general and optional based on specific application;

c) IoT RA Communications View. IoT RA Communications view introduces concepts for handling the complexity of communication in heterogeneous IoT environments;

d) IoT RA Information View. IoT RA Information view describes the physical entities (data carrier) in each domain from data perspective which generate data, process data (data classification), transmit data (data source) or receive data (data destination). Beginning with this, the entities as data carrier, data classification within the entities and data transmission between entities are needed to be defined. IoT RA Information view informs the data attributes that is handled in an IoT system. It provides necessary information to various information consumers, which utilizes the communication links described by the communication view;

e) IoT RA Usage View. IoT RA Usage view provides aspects of IoT systems that are of interest to a specific user or user group together with the relevant information, represented by a corresponding collection of data. It describes from user perspective how the IoT systems or applications can be developed, tested and used;

The IoT RAs become 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.

8.3.1 IoT RA Functional view

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 for support of activities described in the usage 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.

8.3.1.1 Decomposition of the IoT RA functional domains

Figure 8-7 shows the decomposition of the IoT Functional Domains into Functional Components.

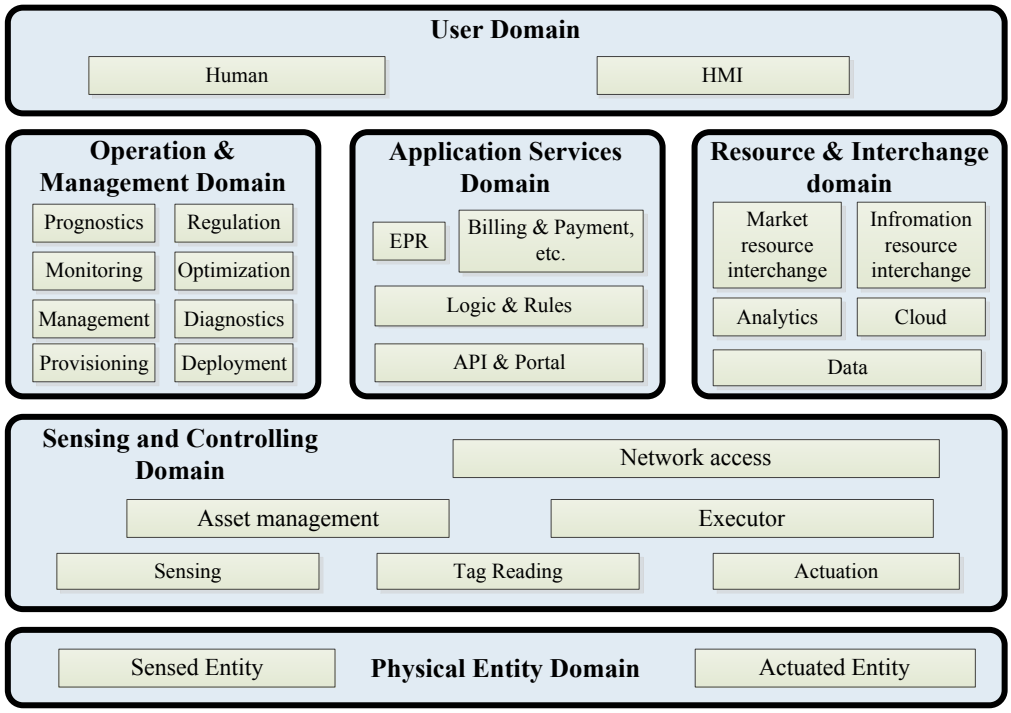


Figure 8-7. IoT Functional View - Functional Domain Decomposition.

8.3.1.1.1 The application service domain (ASD)

The ASD domain represents the collection of functions implementing application logic that realizes specific business functionalities for the service providers in the ASD. The application service domain has components such as logic and rules functional component, application programming interfaces (APIs) and portal functional component.

8.3.1.1.2 The sensing & controlling domain (SCD)

The SCD is comprised of a set of common functional components whose implementation complexity depending on the infrastructure of IoT systems. For a specific IoT system, some components may not exist at all.

Sensing is the functional component that reads sensor data from sensors. Its implementation spans hardware, firmware, device drivers and software elements. Note that recursive sensing, requires control and actuation, and thus have a more tight connection 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.

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.

The stakeholder is an owner or owners of the SCD, yet, this stakeholder may not show up as an entity in the SCD. No human type actor is expected in the SCD. The SCD 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 SCD. Thus, actors in the SCD can be physical entities (e.g., sensors, controllers, actuators, computers, etc.) or virtual entities (e.g., software).

8.3.1.1.3 The operation & management domain (OMD)

System operators and managers are the stakeholders/actors of the OMD. The operators and managers maintain the overall health of IoT system(s).

The OMD represents the collection of functions responsible for the provisioning, managing, monitoring and optimizing the systems' operational performance in real-time.

- The OMD includes several types of functional components for the IoT system operations: 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.

8.3.1.2 Cross-Domain Functions

Figure 8-8 is an overview of the IoT Functional View, showing functional domains and a high level view of cross domain functions.

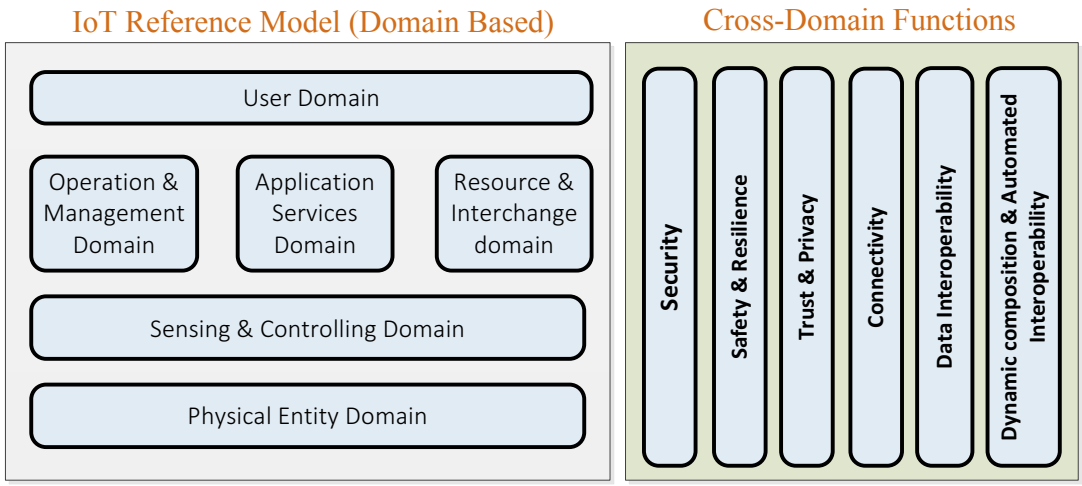


Figure 8-8. IoT Functional View – Cross-Domain Functions.

8.3.2 IoT RA System View

The system view describes the generic functional devices and systems in each domain to form an IoT ecosystem and support of functions components in the functional view. The entities in each domain can be very general and optional based on specific application. The system view addresses the following concepts:

— generic physical entities from system components;

— Connection relationships between the entities.

In Figure 8-9, IoT RA Systems view is shown along with all the entities involved in each domain and the connections among them from the viewpoint of system functional composition. It is based on IoT conceptual model and reference model.

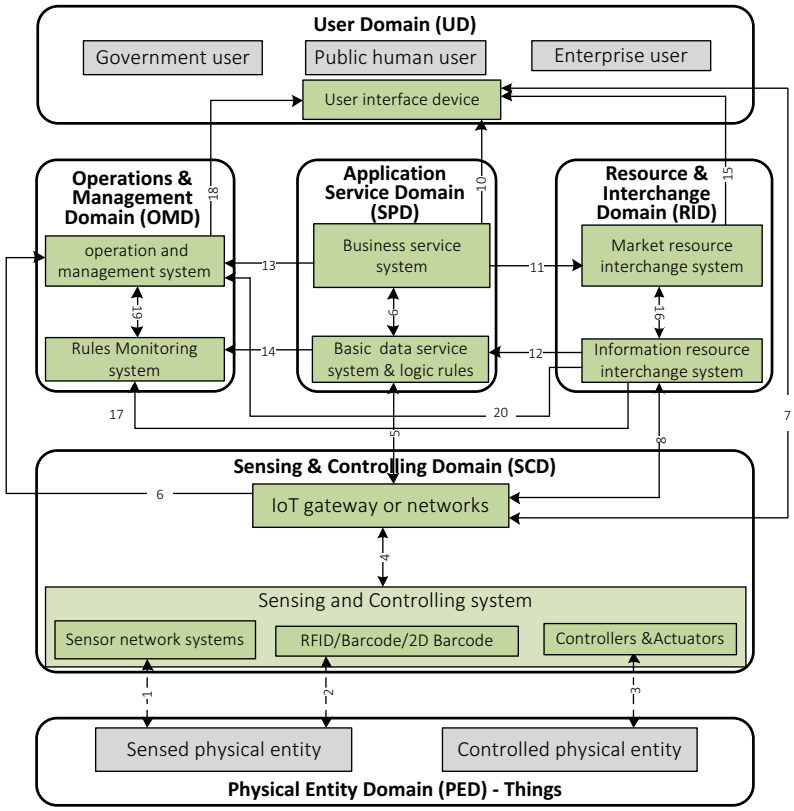


Figure 8-9. IoT RA System view.

The entity descriptions are presented in Table 8-3.

Table 8-3. Description of Entities in the IoT RA System view.

IoT Domains	Domain Entities	Entity descriptions
User Domain	User interface device	User interface device is the connection device to support user access to the Internet of things, and to use of service of the Internet of things. Form the general viewpoint the user can be classified as government user, enterprise user, the public user, etc.
Physical entity Domain	Sensed physical entity	Sensed physical entity is a physical entity which is related to IoT application, interested by users, and acquired information by sensing equipment.
	Controlled physical entity	Controlled physical entity is a physical entity which is related to IoT application, interested by users, and controlled by controlling equipment.
Sensing & controlling Domain	IoT gateway or networks	IoT gateway is the entity to support controlling system to 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 is either an independent equipment or it can be integrated with other with sensing and controlling devices. Networks include kinds of communication networks to enable the IoT device accessible for other system.
	Sensing & Controlling	Sensing and Controlling system can acquire information and perform operations on related objects through different sensing and controlling

	System	function units which achieves a certain local data processing and data fusion. Sensing and controlling system includes sensor network system, label automatic identification system, position information system, audio and video system and intelligent device connection system, etc. It senses and controls objects independently or collaboratively. Meanwhile, it may hold the capabilities of local data acquisition, local data processing, local data analysing, local data storage, etc.
Application Service Domain	Business service system	Business service system provides IoT business services according to the requirement of a particular user. Business service includes information query, analysis and comparison, alarm warning, operation control, joint coordination, etc. Moreover, this system may have functions such as services creation, services execution, service orchestration, service monitoring, etc.
	Basic data service system & logic rules	Basic service system provides foundational service for business service system, which includes data access, data processing, data fusion, data storage, identity resolution, geographic information service and user management, inventory management, etc.
Operation & Management Domain	Operation & Management system	Operation and Management system is to guarantee the equipment and systems to operate safely and reliably. It includes system access management, system security management, system operation and system maintenance, etc.
	Rules monitoring system	Rules monitoring system is to guarantee the IoT application system in line with relevant laws 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 users. 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 for IoT application system. It achieves the exchange of information flow, service flow, and capital flow.

The connections are listed in Table 8-4 below according to the connection numbers found in Figure 8-9 above. These connections are generic and optional.

Table 8-4. Description of the connections between the entities in the IoT RA System view.

#	Entity 1	Entity 2	Descriptions
01	Sensed physical entity	Sensor Network System	Sensor node acquired physical, chemical, biological properties of Sensed physical entity through this connection.
02	Sensed physical entity	RFID/Barcode/2D barcode	This connection is the binding relationship between tag and object. The tag reader can automatically read and write the content related to particular physical entities through the label attached on the target object. Existing label system generally includes RFID, bar code and 2D

			barcode, etc.
03	Controlled physical entity	Controllers& Actuators	The controllers generate control command and let the actuator act on the controlled physical entity.
04	Sensing and controlling system	IoT gateway	IoT gateway adapts and connect to different sensing and controlling systems through this connection, which realizes information interaction and system management, etc.
05	IoT gateway	Basic data service system & logic rules	Basic data service system can connect to IoT gateway through this connection, which realizes sharing and interacting of sensing object information and control command information s under permissions.
06	IoT gateway	Operation and management system	Operation and management system obtains the IoT gateway operation and management state, and sends system and equipment control command, etc.
07	IoT gateway	User interface device	User interface device obtains local service of sensing and controlling domain.
08	IoT Gateway	Information Resource & Interchange system	Information of sensing data can be interchanged with external information systems.
09	Basic data service system & logic rules	Business service system	The processed data in basic data service system and relevant logic rules are delivered to business service system.
10	Business service system	User interface device	User interface device obtains the relevant IoT services through this connection.
11	Business service system	Market Resource & Interchange system	Business service is traded through this connection
12	Information Resource & Interchange system	Basic data service system & logic rules	The information from external system can be transmitted and used.
13	Business service system	Operation and management system	Business service can be operated and managed such as service provision, monitoring, diagnostics, and optimization.
14	Basic data service system & logic rules	Rules monitoring system	Rules monitoring system monitors and controls the running state of the basic service system through this connection, which ensures that the operation of basic service system is in compliance with relevant laws and regulations.
15	Market Resource & Interchange system	User interface device	User interface device obtains information on market resource and interchange information.
16	Information Resource & Interchange system	Market Resource & Interchange system	Information Resource & Interchange and monetization.

17	Information Resource & Interchange system	Rules monitoring system	The interchanging data is stored and monitored to ensure obedience of the regulations.
18	Operation and management system	User interface device	Some manage user accesses service in operation and management system.
19	Rules monitoring system	Operation and Management system	Rules monitoring system monitors all the management data and ensures obedience of the regulations.
20	Information Resource & Interchange system	Operation and Management system	Operation and management system can monitors and controls the running state of the Resource & Interchange system, and ensures that the operation of Resource & Interchange system is in compliance with relevant laws and regulations.

8.3.3 IoT RA Communications view

IoT RA Communications view utilized by the IoT system links the entities for data/information transmission.

IoT RA communications describes the communication relation of each entity of IoT system, to provide the communication support and guarantee for IoT service, such as information collection, information aggregation, information processing, information resource sharing, information service and system operation and control.

IoT RA Communications view addresses following concepts:

— Generic physical entity (device or infrastructure network) capable of building communication links and communication networks;

— Communication relation between these physical entities, which might be physical communication link.

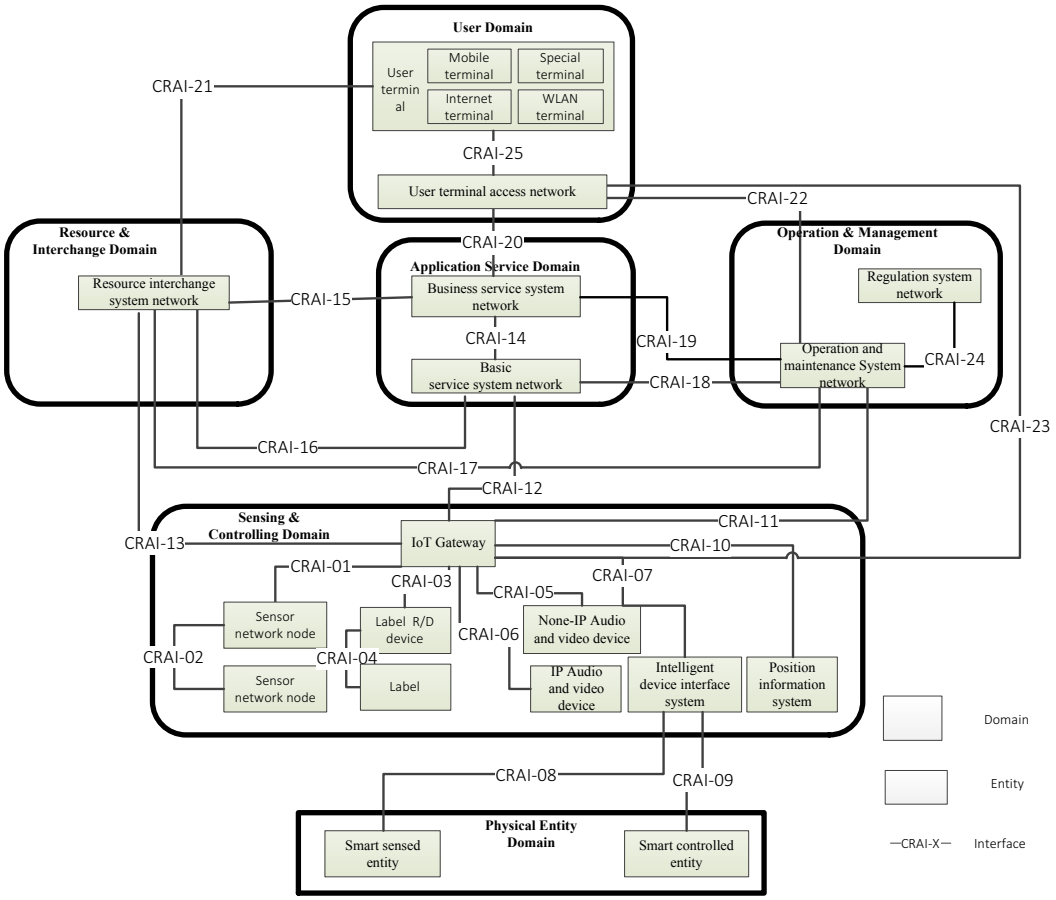


Figure 8-10. IoT RA Communications view.

The entities related to the Internet of things communications reference architecture as shown in Table 8-5. These connections are optional.

Table 8-5. Descriptions of entities in the IoT RA Communication view.

IoT Domains	Domain Entities	Entity descriptions
User domain	User terminal	User terminal is the interactive device to support the user access and use IoT services. From the communication access method point of view, the user terminal includes mobile terminal, internet terminal, WLAN terminal and special terminal.
	User terminal access network	For user terminal to access the network that provides IoT services.
Physical Entity domain	Smart sensed entity	Smart sensed entity is a physical entity relating to the IoT application, and users' interest, which obtains relevant information through digital or analogue connection. The sensed entity have direct communication connection with intelligent device interface system.
	Smart controlled entity	Smart controlled entity is a physical entity relating to the IoT application and users interest, which obtains relevant information through digital connection. The smart controlled entity has direct communication connection with intelligent device interface system.

Sensing & 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 protocol translation, 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 coordinates and manages different sensing control systems. When the sensing control system uses the IP address, IoT gateway can be designed as an application logic device.
	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 completes the information collection and controlling, information processing, network communication and network management.
	Label R/D device	Label R/D device is an electronic equipment to access data and (or) write data to label.
	Label	The label has information storage and read/write functions, which is used to identify and describe the characteristics of an object. It mainly includes RFID, bar code, two-dimensional code label.
	IP audio and video system	IP audio and video system is to get audio and video information of object based on IP network device.
	Non-IP audio and video system	Non-IP audio and video system is to get audio and video information of object based on non-IP network device.
	Intelligent device connection system	Intelligent device connection system is used to connect smart sensing entity and smart control entity, and implement data interaction. It provides network communication, data processing and protocol transition function.
	Position information system	Position information system obtains sensing object position information based on the localization technologies.
Application service domain	Basic service system network	Basic service system network is a communication network to support interconnection and interworking between entities in the basic service system and interaction with other external entities. Generally it adopts local area network construction and implements interconnection and interworking with external network according to some level of security.
	Business service system network	Business service system network is a communication network to support interconnection and interworking between entities in the business service system and interaction with other external entities. It supports multi-communication access method for different terminals.
Operation & Managemen t domain	Operation and maintenance system network	Operation and maintenance system network is a communication network to support interconnection and interworking between the entities in operation and maintenance system and interaction with other external entities. Generally it adopts local area network construction and implements interconnection and interworking with external network according to some level of security.

	Regulation system network	Regulation system is a communication network to support interconnection and interworking between entities in the regulation system and interaction with other external entities. Generally it adopts local area network construction and implements interconnection and interworking with external network according to some level of security.
Resource & Interchange domain	Resource & Interchange system network	Resource & interchange system network is a communication network to support interconnection and interworking between entities in the resource & interchange system and interaction with other external entities. Resource & interchange system also provides the interconnection and interworking between the IoT application systems with other IoT application systems or information resource networks.

Table 8-5 provides the connection descriptions for IoT RA Communication technology view.

8.3.4 IoT RA Information view

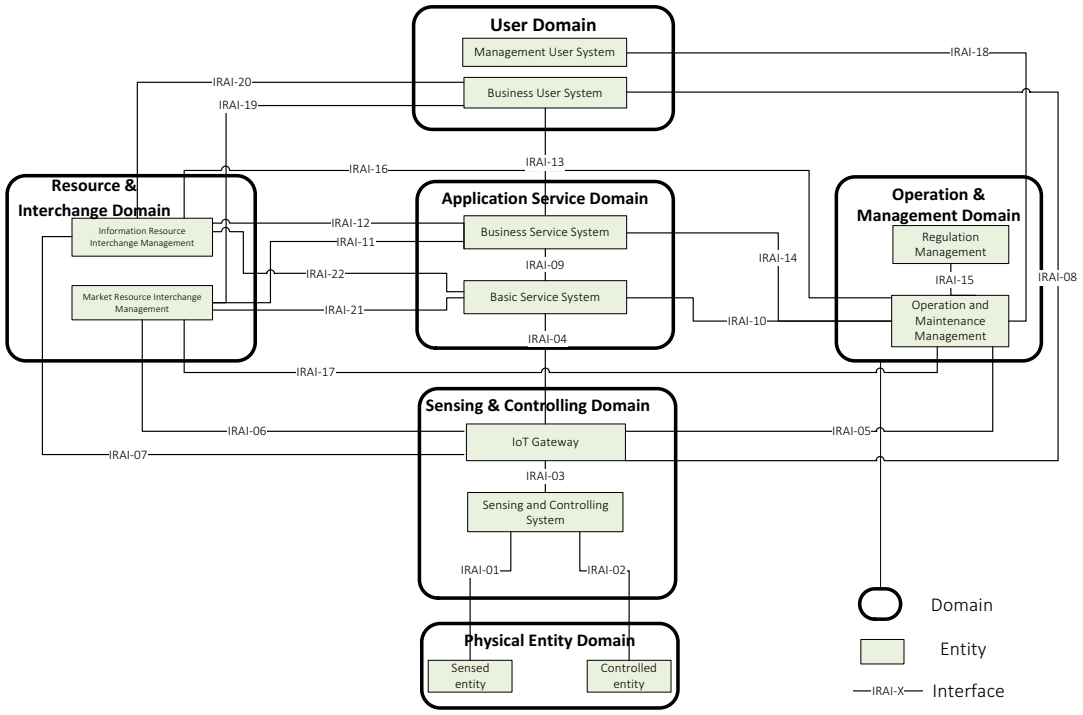
IoT RA Information view describes the physical entities (data carrier) in each domain from data perspective, which generate data, process data (data classification), transmit data (data source) or receive data (data destination). Beginning with this, the entities as data carrier, data classification within the entities and data transmission between entities are needed to be defined. IoT RA Information view informs the data attributes that is handled in an IoT system. It provides necessary information to various information consumers, which utilizes the communication links described by the communication view.

IoT RA Information view addresses the following concepts:

— Generic physical entities that from data perspective which generate data, process data (data classification), transmit data (data source) or receive data (data destination);

— Data transmission relations between these physical entities, which emphasize data transmission types, such as business data, management data, etc.

In Figure 8-11, IoT RA information view is shown with the generic, representative entities involved and the connections between them.



1276

1277 **Figure 8-11. IoT RA Information view.**

1278 The entities found in IoT RA information view are described in Table 8-6 below. The
1279 connections between them are optional.

1280 **Table 8-6 Descriptions of the entities in the IoT RA information view.**

IoT Domains	Domain Entities	Entity descriptions
User Domain	Business User System	Business User System is a system of end users to invoke or request IoT services. Users also receive the service results through this system, e.g., data or information.
	Management User System	Management User System is for the end users to inquire, obtain, and manage devices of an IoT system and system operating status.
Physical Entity Domain	Sensed entity	Sensed entities, e.g., sensors, are physical entities related to IoT applications which acquire data by sensing equipment. Smart sensed entities generate, store and process local object information.
	Controlled entity	Controlled entities are entities related to IoT applications and they are manipulated by controlling equipment which receives control signals from Sensing and Controlling System.
Sensing & Controlling Domain	Sensing and Controlling System	Sensing and Controlling System performs information collection, information processing, information transmission, and object control. From the information point of view, it generates sensing data and/or information about the object of interest. It also generates or receives control data and performs control operations.
	IoT Gateway	IoT Gateway achieves the collection, processing, and encapsulation of the sensing data, including format and application conversion of heterogeneous sensing data along with protocol translation for

IoT Domains	Domain Entities	Entity descriptions
		interoperability in a heterogeneous device and network environment.
Application Service Domain	Basic Service System	Basic Service System performs basic service and supports the services provided by Business Service System. For example, the basic services include data processing, data sharing, data storage, identity resolution, geographic information, etc.
	Business Service System	Business Service System achieves IoT application service by calling basic service and external data and provides IoT service for end users.
Operation &Management Domain	Operation and Maintenance Management	Operation and Maintenance Management is to guarantee the reliability and security of IoT systems via management and maintenance of the devices and system data. From the information point of view, it detects the system failure so as to guarantee the stability, reliability, and security of the information transmission for each communication/data link in the IoT systems.
	Regulation Management	Regulation Management provides the data connection for the data storage, sort management, and quick reference of relevant laws and regulations. It performs supervision to check if the data from the IoT systems and their business services comply with regulations. Regulation Management also provides comparison analysis of the information data between the IoT application systems and the relevant regulations so that any regulatory violation can be prevented, or if the violation occurs, it can be properly handled.
Resource & Interchange Domain	Information Resource & Interchange Management	Information Resource & Interchange System is to manage resource sharing and interchange between the IoT system and other systems. Its realizable functions include, but not limited to, information classification management, information interchange security certification, and information interchange mode management.
	Market Resource & Interchange Management	Market Resource & Interchange Management is to manage the shared information and service transaction relevant to the IoT systems so as to achieve the transaction information generation, transaction information management, and transaction user management.

8.3.5 IoT RA Usage view

During the functional view shows the necessary function and dependency of the IoT system, the usage view sets the focus on how the IoT system being developed, tested, operated and used from user perspective. This view addresses the following concepts:

— activities;

— roles and sub-roles;

— parties;

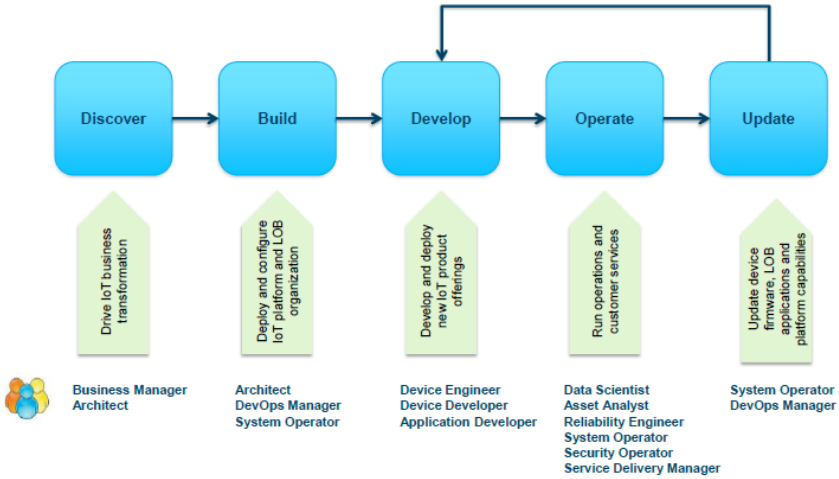
— services; and

— cross-cutting aspects.

8.3.5.1 Description of the Roles

- A Business Manager is leading a business of existing and new products, who wants to understand how to leverage the data and connectivity of devices to create new streams of revenue. He will discover industry content on company web site and act on solution proposals from Architect. Business manager is generally a funder for IoT applications.
- A Solution Architect proposes, proves and deploys the IoT enabled platform to the LOB. He decides in integration strategies and architectures for the new IoT enabled platform, existing business systems and devices in production.
- A DevOps Manager configures and operates the IoT enabled platform, relevant services and supporting IT services for LOB operations and development.
- An Application Developer works in the LOB, in IT or with a 3rd party. He develops IoT industry applications for the LOB. He uses DevOps capabilities to develop, deploy and fix applications that integrate IoT device data and services.
- A Chip Engineer develops silicon devices and sensors. He delivers chips, devices and boards for industry and consumer products.
- A Device Developer integrates HW and SW into devices and appliances. He develops and maintains
- device firmware that securely connects devices to IoT enabled platform.
- A Systems Engineer with the chip provider integration partner works with Device Developer to integrate chips and sensors into the product line.
- A System Operator handles the day to day system operations on customer by on-boarding new users, and makes sure that new device types and devices are registered, are behaving, and are up to date with recent secure firmware.
- A Security Analyst ensures security by proactively by creating rules that detects threats and prevents breaches. He creates automation that acts on misbehaving devices and users. And he ensures compliance through audits.
- A Data Scientist knows all about the industry data delivered from devices and the algorithms that provide meaningful analytics. He implements advanced algorithms as services to be used by the LOB analysts and LOB industry applications.
- An Operations Analyst is responsible for the availability of specific assets in the LOB product line and uses deeper analytics provides by Analytics in the IoT Foundation platform and Ryan's algorithmic service extensions.
- A Service Delivery Manager is responsible for a SLA with a client to the LOB. He and his team of maintenance engineers are on or near the client site and managed equipment and uses the IoT enabled platform and LOB industry applications to monitor, plan and service equipment.

8.3.5.2 Roles and activities during the product life cycle



8.3.5.3 Roles & Sub-Roles for IoT Service Development and Operations

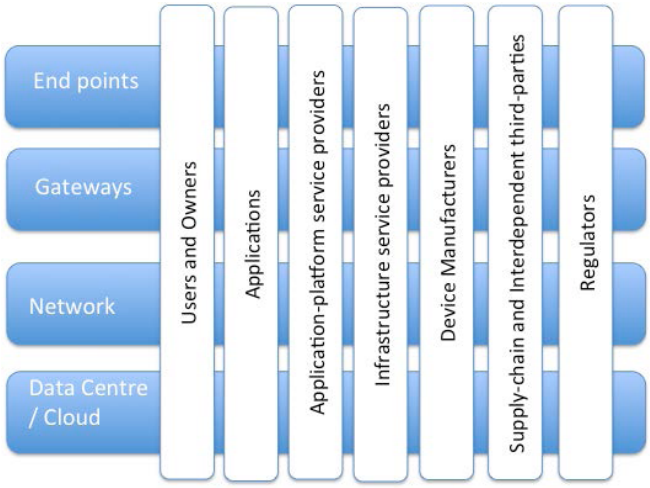
Roles	Sub-Roles
Product Development	Device Developer, Application Developer
Product Line Management	Business Manager, Data Scientist, Asset Analyst, Security Operator, System Operator
Production & Operation	Service Delivery Manager, Reliability Engineer
IoT DevOps and IT Platforms	Architect, DevOps Manager
Device & Product Engineering	Device Architect, System Engineer, Device Developer, Application Developer
End Users	End User, Advanced End User

Activities	Roles
Device and Application Development	Device Developer, Device Partner, Application Developer
Operation of devices, connectivity and applications	System Operator, Maintenance Manager
Use device data for analytics	Data Scientist, Data Analyst, Security Operator
Integrate, operate and control data stores and business	Architect, DevOps Manager, System Operator
Use real-time, historian and big data for applications and analytics	Device Developer, Application Developer, Data Scientist, Data Analyst, Security Operator, Maintenance Manager
Make and operate analytics to run business	Data Scientist, Data Analyst, Application Developer, Maintenance Manager
Bring in analytics to dashboard	DevOps Manager, Systems Operator, Security Operator
Monitor system state, act security risks and beaches	System Operator, Security Operator
Track compliance to regulations	Business Manager, CISO

8.3.6 IoT Business view

Editors' Note: The text for IoT business view is not updated since the initial contribution from Canadian expert. It should be determined whether deleted or not in the ad hoc group for RA views which is established after Shanghai meeting.

1339 The following business model reflects the emerging division of service providers and
1340 stakeholders found in the business ecosystem of the IoT.



1341

1342 **Figure 8-13. IoT Business Model.**

1343 **Table 8-7. Horizontal layers in the IoT business model in Figure 8-13.**

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.

1344

1345 **Table 8-8. Vertical IoT stakeholders in the business model in Figure 8-13.**

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 connection 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? Who is providing critical inputs to the critical inputs? (Secondary dependencies / cascade dependencies?) For instance: public security and emergency services, utilities, shipping and logistics, out-of-band communications and networking? Who is depending on the Users, and their ability within the IoT and the given IoT system under assessment? 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?

1346

1347

1348

1349

1350

1351

1352

Annex A.

Editor's Note: Comments from WG10 4th meeting in Shanghai, the description of 'overall IoT infrastructure at high-level' is moved from clause 8 to Annex A.

Overall IoT infrastructure at High-level

Figure Annex-1 shows the way of combining one IoT system to another IoT system. The arrows in the figure represent the communication and data exchange between the IoT systems, which is enabled by the Resource & Interchange domain (RID) in each IoT systems. The combining approaches are show with an IoT System connecting to another IoT system, e.g., IoT System A and IoT System B and System C in figure 8-6.

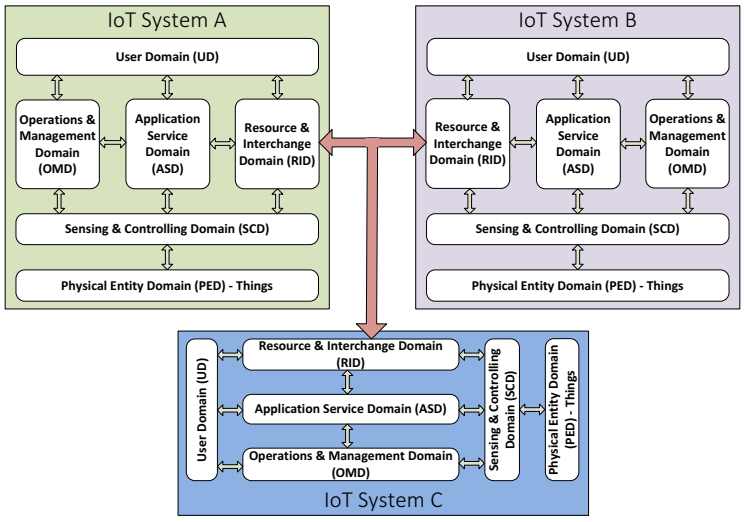
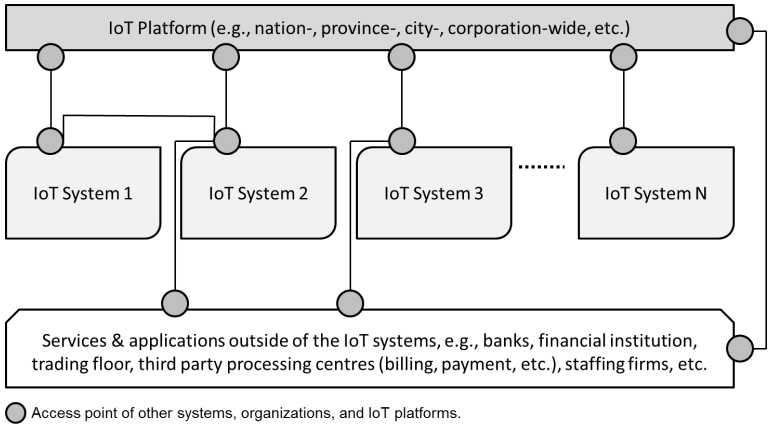


Figure Annex-1. IoT system to IoT system integration types.

In Figure Annex-1, an overall IoT infrastructure from systems point of view which illustrates how various types of IoT systems in vertical application/service domains are integrated for interoperability through the IoT platform(s) at different organizational levels (e.g. national, provincial, corporation/enterprise-wide, etc.). Additionally, one IoT system can also directly interact with other IoT systems when both IoT systems mutually benefit from the direct interaction. Furthermore, an IoT system can have the third party organization supports which are not within its IoT system such as banking/financial service, medical service, billing service, etc. The lines in Figure Annex-1 represent network connectivity, and the grey circles represent interoperable access points (e.g. IoT gateways).



1373

1374 Figure Annex-2. An overall IoT Infrastructure.