**ISO/IEC 30141 20160527**

ISO/IEC JTC 1/WG 10

Secretariat: KATS

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

WD stage

**Warning for WDs and CDs**

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

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

© ISO 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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**

[1 Scope 7](#_Toc451871184)

[2 Normative references 7](#_Toc451871185)

[3 Terms and definitions 7](#_Toc451871189)

[4 Symbols and abbreviated terms 7](#_Toc451871190)

[5 IoT Reference architecture goals and objectives 8](#_Toc451871191)

[5.1 Structural overview 10](#_Toc451871192)

[6 Characteristics of IoT systems 11](#_Toc451871193)

[6.1 IoT System Characteristics 13](#_Toc451871194)

[6.2 IoT Service Characteristics 17](#_Toc451871202)

[6.3 IoT Component Characteristics 19](#_Toc451871203)

[6.4 Compatibility 23](#_Toc451871204)

[6.5 Usability 23](#_Toc451871205)

[6.6 Reliability 26](#_Toc451871206)

[6.7 Security 27](#_Toc451871207)

[6.8 Privacy 29](#_Toc451871208)

[6.9 Other Characteristics 30](#_Toc451871210)

[7 IoT Conceptual model 36](#_Toc451871211)

[7.1 Main purpose 36](#_Toc451871212)

[7.2 Interpreting model diagram 36](#_Toc451871213)

[7.3 The big picture 38](#_Toc451871214)

[7.4 Concept 39](#_Toc451871215)

[8 IoT Referencemodel and Reference architectureviews 49](#_Toc451871218)

[8.1 Relation between CM, RMs and RAs 49](#_Toc451871220)

[8.2 IoT Reference models 50](#_Toc451871221)

[8.3 IoT Reference architecture (IoT RA) views 58](#_Toc451871222)

[Annex A. 85](#_Toc451871223)

[Overall IoT infrastructure at High-level 85](#_Toc451871224)

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](http://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](http://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](http://www.iso.org/iso/home/standards_development/resources-for-technical-work/foreword.htm)

The committeeresponsiblefor this document is ISO/IEC JTC 1/WG 10.

Introduction

Internet of Things (IoT) has a 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 are adapting IoT technologytodigitize areas that were not possible a few years ago. Several forecasts indicate that IoT will connect 50 billion devices worldwide by the year 2020. There are a number of possible applications such as; smart city, smart grid, smart home/building, digital agriculture, smart manufacturing, intelligent transport system, e-Health, etc.IoT is an enabling technology that consists of many supporting technologies, for example, different types of communication networking technologies, information technologies, sensing and control technologies, software technologies, device/hardware technologies. This international standard is based onworking, and widely used enabling technologies that are defined in standards from several organizations such as ISO, IEC, ITU, IETF, IEEE, ETSI, 3GPP, W3C, etc.

This standard covers the generalized Reference architecture of IoT, which is to serve as base on which to develop (specify) specific IoT applications.

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

# Scope

This International Standard specifies the general IoT Reference Architecture in terms of defining System Characteristics, the Conceptual Model, Reference Model and Architecture Views for IoT.

# 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*

*ISO/IEC 20924 - Terms and Definitions*

# Terms and definitions

**Editor’s Note:** Terms and definitions have been processed by ISO/IEC 20924. Following terms are considered as RA specific. Comments shall also indicate placement of the definition. If the definition is considered to be “general”, it will be moved to 20924.

# Symbols and abbreviated terms

Editors’ Note: we will make a search when all the clases is updated and seek for abbriviations that exists or not.

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

6LoWPAN IPv6 over Low power Wireless Personal Area Network

ASD Application Service Domain

CM Conceptual Model

DHCP Dynamic Host Configuration Protocol

FQDNs Fully Qualified Domain Names

HTTP Hypertext Transfer Protocol

IoT Internet of Things

LAN Local Area Network

OMD Operation & Management Domain

PAN Personal Area Network

PED Physical Entity Domain

PII Personally Identifiable Information

QoS Quality of Service

RA Reference Architecture

RID Resource &Interchange Domain

RM Reference Model

SAP Session Announcement Protocol

SCD Sensing & Controlling Domain

TCP/IP Transmission Control Protocol/Internet Protocol

UML Universal Modelling Language

UD User Domain

URI Uniform Resource Identifier

VPN Virtual Private Network

WAN Wide Area Network

WLAN Wireless Local Area Network

# IoT Reference architecture goals and objectives

IoT is defined as an infrastructure of interconnected objects, people, systems and information resources together with the 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 IoTsystems 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 IoT system architecture.

The IoT RA serves the following goals:

* to describe the characteristics and general requirements of IoT systems;
* to define the IoTsystem’s domains;
* to describe the conceptual model (CM),reference model (RM) of IoT systems; IoT architecture views, and
* to describe interoperability of IoTsystem’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 astarting point with the same rules and guidance when the developers reuse the IoT RA.

The IoT RA supports the following important standardization objectives:

* to enable the production of a coherent set of international standards for IoT;
* to provide a technology-neutral reference point for defining standards for IoT; and
* to encourage openness and transparency in thedevelopment of a target IoT system architecture development and in the implementation of the IoT system.

The IoT RA is also intended to:

* facilitate the understanding of the overall intricacies of IoT systems;
* illustrate and provide understanding of IoT reference architectures from different architectural views;
* provide a technical reference to enable the international community to understand, discuss, categorize and compare IoT systems;
* facilitate the analysis of candidate use cases/applications including data/information flows; and
* facilitate the identifyingofgaps in IoT-relatedstandardsinorder to initiate the standardization projects.

## Structural overview

The IoT Reference Architecture (IoT RA) represented in this International Standard provides:

* a conceptual model containing common entities and their relations, and
* a reference models and different architecture views

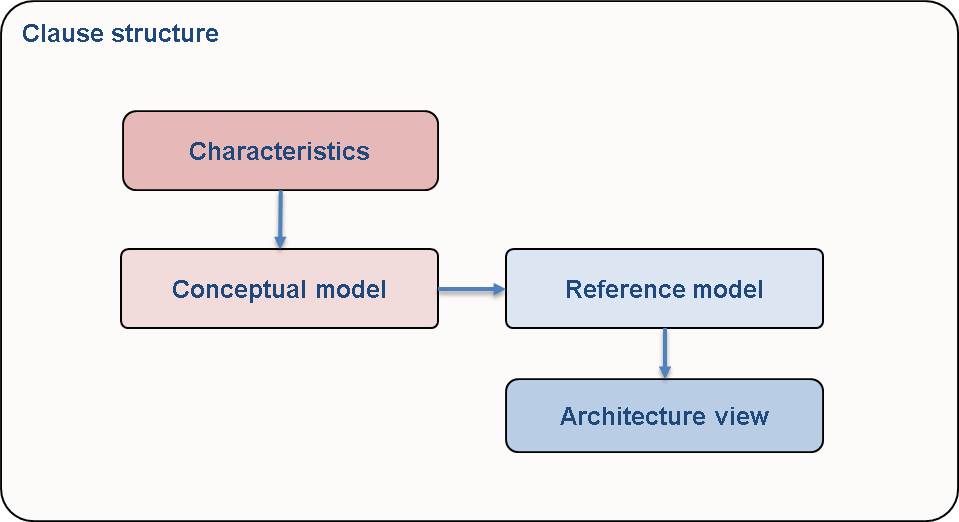


Figure 1 - IoT RA structure

### Conceptual model

The conceptual model contains the following elements:

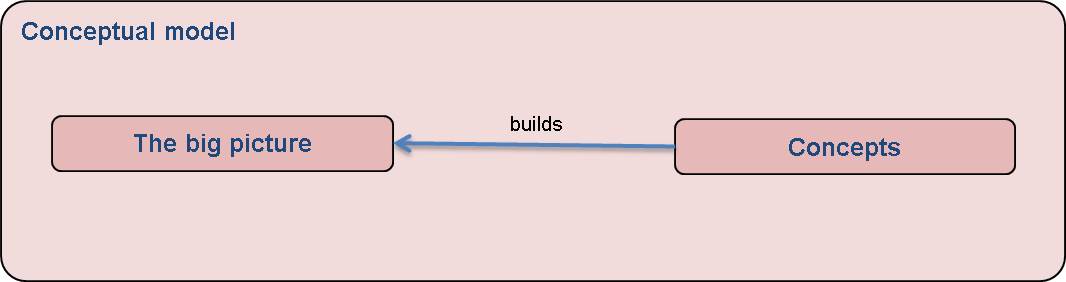


Figure 2 - Conceptual model structure

### Reference modeland architecture views

The reference model contains the following parts:

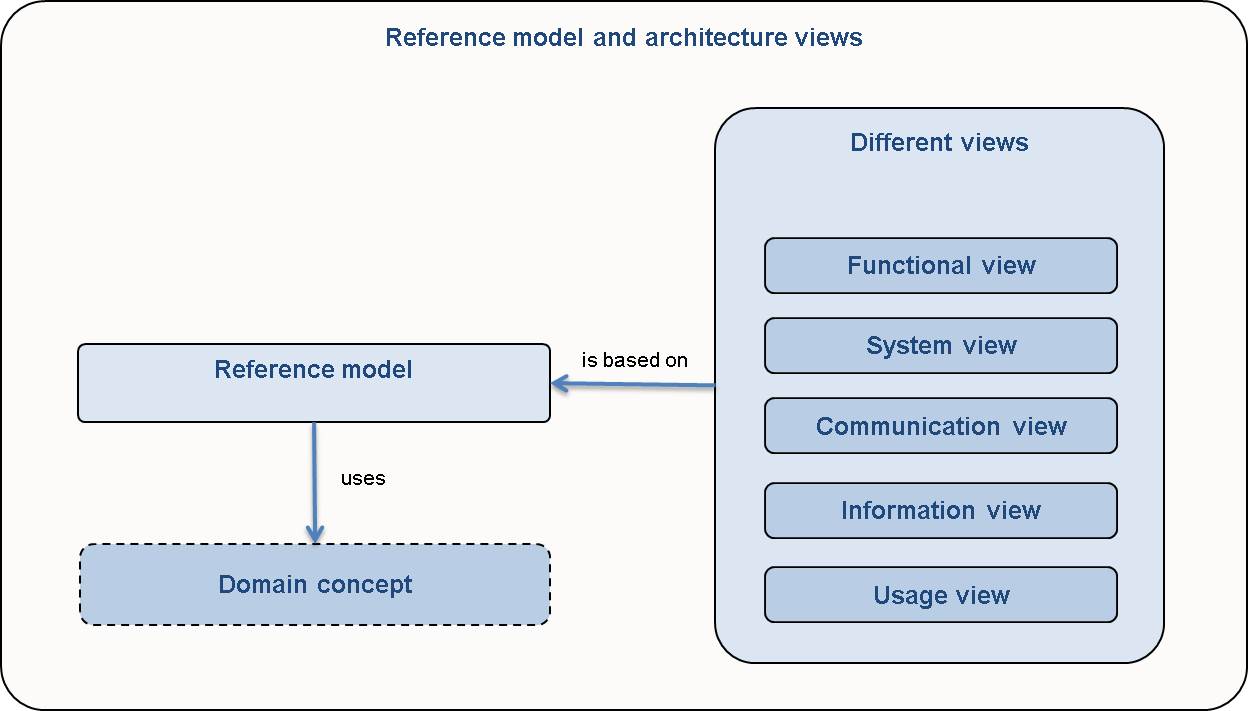


Figure 3 - Refernce model and architecture views

The respective views are described in clause 8.

# 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.

This clause provides characteristics of IoT systems. Functions based on all or a part of these characteristics can be implemented in IoT systems according to services and operations.

|  |  |
| --- | --- |
| Grouping | 1st Level |
| 6.1 IoT System Characteristics | 6.1.1 Auto-configuration  (including autonomic networking, autonomic service capabilities, plug and play) |
| 6.1.2 System configuration |
| 6.1.3 Network communication |
| 6.1.4 Network management and operation |
| 6.1.5 Service provisioning |
| 6.1.6 Self-description |
| 6.1.7 Data/Control separation |
| 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 |
| 6.4.2 Well defined components |
| 6.5 Usability | 6.5.1 Manageability |
| 6.5.2 Flexibility |
| 6.6 Reliability | 6.6.1 Reliability |
| 6.6.2 Resilience |
| 6.6.3 Availability |
| 6.7 Security | 6.7.1 Confidentiality |
| 6.7.2 Integrity |
| 6.7.3Safety |
| 6.8 Privacy | 6.8.1 Privacy |
| 6.9 Other Characteristics | 6.9.1 Data 5Vs – volume, velocity, veracity, variability and variety |
| 6.9.2 Heterogeneity |
| 6.9.3 Scalability |
| 6.9.4 Regulation compliance |
| 6.9.5 Consumer protection |
| 6.9.6 Trust/trustworthiness |

## IoT System Characteristics

### Auto-configuration

#### Description

Auto-configuration is the automatic configuration of devices based on the interworking of predefined rules (associated algorithms based on data inputs). Auto-configuration includes automatic networking, automatic service provisioning and plug & play. Auto-configuration allows an IoT system to react on conditions and add and remove components such as devices and networks. Auto-configuration needs security and authentication mechanisms to make sure that only authorised components can be auto-configured into the system. Security and authentication mechanism shall be arranged appropriately for each market segment.

#### Relevance to IoT systems

Auto-configuration is needed for various IoTsystems and benefits those users who expect robust systemsbecause auto-configuration can allow automatic elimination of faulty components and maintenance of a working system. It can be set up with hardware stand by or manually introduced.

#### Examples

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

**Editor’s Note:** Action point for comment issuer JP05, content needs to be reworked and described details in three parts Description, Relevance to IoT systems and Example to fit current structure

### System-configurations

#### Description

It is summarized that IoT systems consist of networked devices, network, information processing, services on configuration. Then, network types are introduced as follows; area networks, dedicated wide area networks, and general purpose wide area networks including Internet.

#### Relevance to IoT systems

IoT devices are connected by several types of communication networks. Information between IoT devices and Information processing platform are transferred across communication networks. Communication networks shall have abilities which comply with requirements on service, such as QoS control, network security, resilience and some management features. Information processing platforms configure data base and analysis information from IoT devices to provide services.

#### Examples

According to services, communication networks and Information processing platforms are configured. For example, in a factory automation system, IoT devices distributed in small areas are connected to LAN. Information from these devices is transferred to Information processing platform located in the same area. On the other hand, in a monitoring system of disasters and an energy management system using smart meters, IoT devices distributed in wide area are connected by some kinds of wide area networks. Information is transferred to Information processing platforms located in far end.

### Network communication

#### Description

Physical network configurations to connectIoT devices depend on network types such as area networks, dedicated wide area networks and general purpose wide area networks. Communication protocols in each layer, e.g., Physical, Data link, Network, Transport or Application layer, are specified according to these network types. Logically, information between IoT devices and Information processing platforms are transferred by IP and its related technologies including optimization for IoT.

#### 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 types with the IoT devices when one device is able to exchange information with the other device whether or not they have a direct connection to each other. Some Gateways are located in edges and borders of networks. Network structure can/should be able to be static/dynamic at any time of its existence, and (consider) structural elements like: QoS, resilience, network security and some management features.

#### Examples

In an area network, IoT devices are connected by wireless technology, e.g., IEEE802.15.4 and IEEE802.11 in communication protocols on Physical and Data link layers. They are transported by 6LowPAN which is IoT specific IP and UDP. IoT devices are connected to a dedicated or general purpose wide area network directory or via area networks through a Gateway.

### Network management and operation

#### Description

Network management and operation depend on services, network type and network ownership. They include in-service management, e.g., QoS, fault and security managements, and pre-service management, e.g., device, static profiles and resources of facilities managements.

#### Relevance to IoT systems

In some services, IoT devices and communication networks are managed strictly. On the other hand, if users deploy IoT systems, all of IoT devices and communication networks are not managed. If IoT services are overlaid on conventional communication networks, their management and operation can be applied.

#### Examples

One of strict operation and management case is energy monitoring by smart meters. In this case, all of IoT devices and facilities of communication networks and information processing platform are managed. On the other hand, in case of home energy management, it is not necessary that all of them are managed strictly.

### Service provisioning

#### Description

If a user subscribes some services provided by service providers, some procedures including payment are required. Moreover, governance for their services is specified. On the other hand, if a user installs some services by himself, he burdens all of responsibilities on their services.

#### Relevance to IoT systems

It depends on provided services and business models.

#### Examples

When service provides of IoT receives request from users for service subscription, they shall provide services according to agreement with users and claim payment. In this case, they protect privacy of their users in addition to service quality.

### Self-description

#### Description

Self-description is the description about IoT system itself in order to inform other IoT system about itself for interoperability. Self-description includes interface specification, capability of IoT system, number of IoT system which are connected to itself, what types of devices can be connected to itself, how many IoT system can be connected to itself, what kinds of service are possible by itself, and current state of interconnected IoT systems.

#### Relevance to IoT systems

Self-description is needed for interoperability among IoT system/devices and benefits those users who expect to interconnect his IoT systems/devices to other IoT systems/devices to extract more useful result.

#### Examples

Example of self-descriptionIoT system and protocols: The system which usesbluetooth provide device name and supported service list to each other when connecting. Access point broadcast SSID and WiFi device sends password and MAC address to access point when it is connecting to access point.

### Data/Control separation

#### Description

Separation of data from control is the condition where a different processor, communications channel, protocol or interface is used to transmit, process or store control signals and data signals.

#### Relevance to IoT systems

Data and control flows are bits and bytes with logically distinctively different

* purposes (execution/action vs information/description),
* user roles (control and modify behavior vs transfer or consume facts and information),
* classification/types of data (technical or system specific vs personal/sensitive/public),
* access (e.g. an operator may access system configuration, but not gathered personal data; and vice versa for the user, whom the personal data belongs to)
* protocols, formats and lifecycle (e.g. support multiple control protocols vs metadata/structure of the transferred information, which is particularly important considering interoperability and co-existence of multiple versions and variants of both data and control planes)

Usually, the aforementioned differences bear specific risks and require special security (and other) controls, e.g. retention policy is applicable while dealing with personal data, but not the control one; access control may be weaker for a user and stronger for an administrator).

Ubiquitous penetration of IoT into virtually all areas of life increases the attack surface, multiplying the number of potential attack targets by an order of magnitude (at least), increasing the availability of the attackable targets to the threats, and often making ineffective alternative measures such as physical security controls.

Ironically, the key value of IoT – the connection of numerous edge components to each other and/or other new or legacy systems – increases the security concerns, since adding a weak link makes whole chain weak. That ultimately means making insecure the entire interconnected and interdependent digital world first and immediately the tightly coupled with it physical world! Applications and systems previously running in well-protected data centers may suddenly become exposed to numerous threats.

In that way, IoT significantly increases the risk exposure (which is [increased] value at risk x [increased] probability of attack). Separation of data and control planes allows introduction of better fitted and as strong as required security controls for each plane accordingly, thus increasing security in general without unnecessary complications where it is not desired.

Separation of Data and Control enables or strengthens the ability to apply different authorization, authentication and protection mechanisms or constraints to data flows as opposed to control flows. Broad sharing of data from an IoT system might be useful or desirable, and yet there are many circumstances where one might wish to limit control of an IoT system or component to only a subset of the entities with which the data from that IoT system is allowed to be shared.

#### Examples

If an IoT system is used to provide sensors and data for HVAC or other building control, it might be desirable to share data with other inter-related systems (alarms, access control, power management or auxiliary power, etc.), while still retaining control of the system strictly within the system boundaries.

## IoT Service Characteristics

### Content-Awareness

#### Description

Content-Awareness is 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.

#### 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.

#### 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.

### Context-Awareness (location awareness, time awareness)

#### Description

Context-Awareness is 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.

#### 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 effect an action, this understanding is critical.

#### Examples

An example of location-based services which provides different services according to the location a user.

In cases of an emergency like afire 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.

### Timeliness

#### Description

Timeliness is the property of performing an action, function, or service within a specified period of time.

#### 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 other aspects such as jitter, frequency/sampling rate, and phase.

#### Examples

IoT system for smart meter needs to collect energy consumption data withinspecific 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 interactionamong them is critical is critical to prevent accidents. Where IoT entities are part of any kind of controlloop. The total latency around the loop is critical.

## IoT Component Characteristics

### Composability

#### Description

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

#### Relevance to IoT systems

System integration, interoperability and composability deal with how the functional building blocks are assembled to form a complete system and how the functional building blocks interface with each other, andvia 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 withother building blocks of the same kind that share the same set of characteristics and properties such as 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.

#### Examples

An example of composability might be the ability to swap out sensor or control components from one vendor to replace legacy components that are part or a system produced by a different vendor. In this example, there might be two levels of composability. First would be complete interchangeability of “commodity” functionality, such as an IoT device from Vendor A being fully swappable with one from Vendor B.

A second level of composability (or possibly interoperability) might be an IoT control that is vendor-specific at the interface between the IoT component and a physical process device being controlled (a valve, motor, switch, pump or fan, for example) , but is still fully interchangeable at the interface between the IoT device and the rest of the IoT ecosystem. In this sort of example, the IoT device would serve as the “middleware” between the vendor-agnostic IoT infrastructure, and the vendor-specific physical devices or mechanisms being controlled.

### Discoverability

#### 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.

#### 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 segment. Discovery and lookup service of IoT systems allow to locate physical entities based on geographical parameters and the dynamic discovery of relevant virtual and physical entities and their related services based on respective specifications.

#### Example

Network mapping discovers the devices on the network and their connectivity. It is not to be confused with network discovery or [network enumerating](https://en.wikipedia.org/wiki/Network_enumerating)which discovers devices on the network and their characteristics such as [operating system](https://en.wikipedia.org/wiki/Operating_system), open [ports](https://en.wikipedia.org/wiki/Computer_port_(software)), listening [network services](https://en.wikipedia.org/wiki/Network_service), etc. Examples such as DHCP, Bonjour, SAP (Session Announcement Protocol).

### Modularity

#### Description

Modularity is the property of a component to be a distinct unit that can be combined with other components.

#### 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.

#### Examples

An example of Modularity in an IoT system might be a smart thermostat. Because the interface to the HVAC system and the interface to a larger IoT infrastructure could both be defined in compliance with non-proprietary interface standards, there is nothing to prevent a thermostat from Vendor A being replaced by one from Vendor B.

Further, it doesn’t matter how the functionality might be implemented. Vendor A might provide the capability in the form of an ASIC-based state machine, while Vendor B’s design might be based on a microcontroller. As long as both perform the same functions in response to the same inputs, and they are both compliant with open standard interfaces without imposing any proprietary constraints, there is nothing to prevent one from being replaced by the other.

### Network connectivity

#### 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 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 device (objects/things).

#### Relevance to IoT systems

IoT systems rely on the ability to exchange information units in a structured manner based upon different but interoperable 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 devices (objects/things), whether or not they have a direct connection to each other. IoT Network structure can be be static or dynamic at any time of its existence, and structural elements like: QoS, resilience, encryption, authentication and authorisation.

#### Examples

IoT networks consist of physical layers defined by standards such as IEEE 802.1, 802.3, 802.11, 802.15, ZigBee, 6LoWPAN, SmartBAN and with elements such as repeaters, hubs, bridges, switches routers, modems and firewalls. Topologies can be: Mesh, Ring, Star, Fully connected, Line, Tree, Bus.

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

Organisational IoTnetwork can be: inter- and intra-network, internetwork (in the meaning of networks of different kind of an architecture/structure connecting together).

### Shareability

#### Description

Shareability is the ability to use individual components in multiple interconnected systems.

#### Relevance to IoT systems

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

Temperature sensing for heating control could be used by the security system for fire detection.

#### Examples

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

### Unique identification

#### Description

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

#### Relevance to IoT systems

It is essential that the entities in an IoT system such as the devices, physical and virtual objects and end-users can be distinguished from each other. This enables interoperability and global services across heterogeneous IoT systems.

Its unique identification is a universal property of 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.

#### Examples

IPv4, IPv6, URI, and Fully Qualified Domain Names (FQDNs) are used as unique, unambiguous identification in the Internet applications. Individual hardware devices, software etc. may have unique manufacturer’s IDs, OIDs, UUIDs or other identifiers. 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.

## Compatibility

### Legacy support

#### Description

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

#### Relevance to IoT systems

Support of legacy component integration and migration can be important, although when supporting legacy components it is also important to ensure that the design of new components and systems does 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.

#### Examples

Railway signalling systems are typically maintained for many decades.

One example of transition from legacy to future compatibility is the current slow rollover from IPv4 compliance to IPv6 compliance. The limits of the IPv4 address space and of the IPv4 protocol are known, and the transition to IPv6 is clearly the way of the future, but the varying pace of the transition, depending on the context, makes it a topic which can be very complex.

Many existing standards and application environments still assume and depend on IPv4, and yet it’s clear that sticking with IPv4 forever is not a viable strategy., Deciding how and when to make the transition, however, is a topic that nobody has a universal answer to.

The end result is different market segments, vendors and communities of interest are each pursuing their own strategies for the v4 to v6 transition, and anybody whose activities straddles several of these different transition strategy enclaves has an additional layer of complexity draped over the individual transition strategies.

## Usability

### Manageability

#### Description

Manageability addressing aspects such as device management, network management, system management, and interface maintenance and alerts is important to meet IoT system requirements. Components capable of monitoring the system and changing configurations are needed for manageability of the IoT device, network and system.

#### Relevance to IoT systems

ManyIoT 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.

#### 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. Additionally, software updates are necessary to ensure that devices and systems maintain functionality and the latest security vulnerabilities are patched. The configured manageability component may include device state monitoring component, the link monitoring component, the calibration component, etc.

### Well-defined components

#### Description

Well-defined components are the components for which an accurate description of their capabilities including associated uncertainties is available. Capability information includes not only information about the specific component functionality, but configuration, communication, security, reliability and other relevant information.

#### 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.

#### Examples

MIB objects that link to datasheets.

An example of an implementation of a well-defined component might be as follows: A particular IoT component is available with varying amounts of memory or support for various RF frequencies, waveforms and protocols. Such a device might have a baseline handshake protocol which all the variants make use of to inform other IoT components of the list of capabilities possessed by each device. Once the devices’ respective configurations have been exchanged, each device’s software or applications can then self-adjust to take into account the capabilities of the other devices.

### Flexibility

#### Description

At its most basic level, flexibility is the capability of an IoT system, service or device to provide a varied range of functionality, depending on need or context.

#### Relevance to IoT systems

History and experience tell us that while there are exceptions, the economic and functional sweet spot for flexibility is usually somewhere in the middle, between the extremes of a dedicated single purpose device on one end of the spectrum, and a massively capable, programmable, extensible, “all things to all people” general purpose device.

One might conceivably break down the general concept of flexibility into different sub-categories or dimensions.

One dimension of flexibility might be the distinction between IoT capabilities hosted on a platform powered by a general purpose computing core and a similar capability implemented in the form of state machines implemented using discrete components, programmable FPGAs, or a purpose-specific ASIC. The state machine versions will tend to be smaller, faster, more power efficient, and more secure (due to a more limited range of capability). The general purpose version will trade off speed, size, power draw and other traits to gain more generalized capabilities, and a greater ability to be adapted to meet unanticipated future requirements.

A second continuum or dimension of flexibility might be the distinction between the following:

1. A device which has fixed, nonprogrammable, non-extensible functionality – “hard wired, single purpose”
2. A device which has fixed H/W capability, but which provides some amount of configurability within the single available format
3. A device which is both programmable and expandable in the hardware domain – adding memory, adding more computational capability, adding RF channel capability, etc.
4. A family of devices, each of which might fall into categories 1-3, from which an integrator can select the one(s) which are appropriate for a given context
5. A family of devices such as in 4, where some of the options provide different amounts of composability or modularity, at different levels of abstraction.

A third dimension of flexibility might involve the range of standards, protocols, formats, and interfaces which an IoT device is designed to support, where that support might then be designed and implemented taking the factors above into account.

A fourth dimension might be the ability to emulate or host non-native capability, such as a Mac running a virtual machine to emulate a PC, or a PC hosting an expansion board which is itself a self-contained computer or other device.

Aside from the device or platform, there is also a fifth dimension of flexibility that involves the overall design and marketing philosophy underlying the IoT product, system or environment. As in other domains, there will likely be open IoT ecosystems, and proprietary IoT ecosystems, with varying amounts of overlap between the two.

#### Examples

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

## Reliability

### Reliability

#### Description

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

#### 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.

#### Examples

Data reliability is of utmost importance for the decision-making processes of IoT systems. Communication reliability is important for ensuring the availability and correct operation of data/devices, particularly in mission-critical systems.

### Resilience

#### Description

Resilience is the ability of the system or its components to recover from faults and failures within a timeframe that meets system requirements.

#### Relevance to IoT systems

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

#### Examples

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

In a master-slave system if the master unit fails then an alternative device must assume the master role. In a mesh network if one link fails then data can still flow from source to sink through an alternative route.

### Availability

#### Description

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

#### 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 lifetime and the reliable connectivity of the devices. Availability of the data is related to the ability of the system to get the requested data from a system component. Availability of services is related to the ability of the system to provide the requested service to users with a pre-defined QoS.

#### Examples

In some critical applications, e.g. 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.

## Security

### Confidentiality

#### Description

Confidentiality is the property, that information is not madeavailable or disclosed to unauthorized individuals,entities, or processes. (Excerpt from ISO27000)

Incorporate the principle of purpose limitation: data can only be collected for specific and legitimate purposes.

Incorporate the principle of data minimization: data collected should be strictly necessary for the specific purposes identified.

#### Relevance to IoT systems

In an IoT system the confidentiality protection is responsible for prohibiting other network participants from reading 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 assured by protecting it before sending it over potentially insecure channels (many IoT communications are done wirelessly or over the Internet) so that it only reaches the intended recipient.

#### Examples

The neighbour or a burglar is not able to read the actual value of the room motion detectionsensors 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).

With a smart meter system the frequency of messages must not depend on the rate of consumption of electricity.

### Integrity

#### Description

Data integrity is the property that data has not been altered or destroyed in an unauthorized manner [ISO\_27040:2015--3.9]

#### Relevance to IoT systems

Data integrity is highly related to IoT systems to ensure that the data used for decision-making processes in the system and executable software has not been altered by faulty or unauthorized devices or by malicious users.. The protection of the integrity of the data is a key requirement to ensure the security of the IoT system.

#### 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 and this must not cause the air-conditioning system to increase the amount of cooling.

### Safety

#### Description

Safety is the property of being designed to prevent damage or harm due to malfunction, failure, or accident. While prior traits describe the desired behavior of the system when operating correctly, Safety includes the consideration of failure modes with the intent of preventing, reducing or mitigating the potential for undesired outcomes; specifically damage, harm or loss.

#### Relevance to IoT systems

Many IoT systems will be deployed in contexts or operational environments where damage, loss, injury or death might result if failure modes are not adequately addressed. In many operational contexts, approval to operate or approval to connect will not be granted if safety requirements are not met.

Even in contexts where compliance with safety standards is optional or voluntary rather mandatory, proper consideration of safety factors might have significant impact on continuity of operations, reduction of loss, prevention of injury or death, insurance premiums, torts and liability, and other issues.

#### Examples

(Examples given below are from a U.S. context – similar international examples might be more appropriate, both here and elsewhere in the document)

IoT contexts where safety standards or requirements might need to be considered include medical or health care applications (FDA oversight), Aviation (FAA and DoD) consumer products (Underwriter’s Labs, Consumer Product Safety Commission), automotive application (NTSB), workplace (OSHA), housing (building codes, fire codes) etc.

## Privacy

### Privacy

#### Description

Privacy 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, machines and processes. It is advisable that the quantity of PII be the minimal necessary to support the application. The PII which is necessarily present should be securely deleted when no longer needed. This protects the individual and minimizes legal risk to the entity using the customer PII. If PII is disclosed it must be based on prior informed consent given by the PII principalfor the intended purpose.

#### 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 administration) where the latter collects, receives, exchanges, processes etc.personal information. From an international common requirements perspective there are eleven (11) common privacy protection principles. 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 constitutes each individual’s privacy might be different among individuals. It might be different due to legal, social or cultural norms. However, when end-users provide data about themselves and it is used for a different purpose than that for which they understood it would be used at the time of release, this is a breach of privacy..

Being able to fully respect the privacy of individuals is essential for the societal and legal acceptation of IoT systems by the public. Therefore the user’s location should be anonymized in the traffic data base.

#### 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) by an individual represent a keyexample. 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 the organization (public and private sector) wanting access to 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 IoTRA is designed to be able to support the 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 collected by separate services and would come with different access control policies due to different consents given by the PII principal.

For a different example, the end-user wants to participate in sensing traffic jams; obviously he does not want the IoT system to disclose his whereabouts in more detail than is necessary for the application to work.

## Other Characteristics

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

#### Description

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

#### Relevance to IoT systems

IoT Systems 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.

#### Examples

A logistic company usesbig 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.

### Heterogeneity

#### Description

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

#### Relevance to IoT systems

IoT is cross-system, cross-product, and cross-domain. Realizing the full potentialofIoT 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.

#### Examples

A smart container using RFID tags and sensors needs interworkingof RFID systems and sensor network systems.

### Scalability

#### 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.

#### 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.

#### 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, and in the number of temperature readings processed by services and applications.

### Regulation Compliance

#### Description

IoT systems, services, components and applications will quite often be deployed in circumstances which require adherence to a variety of laws, policies or regulations. Such support might be inherent in the IoT device or system, or might require specific configuration, programming, modification or extension to ensure compliance.

Additionally, there might be a range of different granularity or levels of abstraction at which the regulations are applied or enforced.

#### Relevance to IoT systems

Regulations of interest to IoT systems might take many forms, including the following:

Regulations to assure interoperability,

Regulations to mandate or constrain functionality or capability,

Regulations to assess the ability of the IoT device or system to inhabit a certain usage context without causing damage,

Regulations to impose at least minimal balance between contribution to the collective good and self-interest on the part of system owners or operators.

#### Examples

(the examples provided are from a U.S. context, and might need to be replaced with examples which are more familiar to an international audience)

Regulations which might apply to an IoT context include one or more of the following categories:

Safety regulations – These might include FAA or DoD flight safety standards for IoT devices operating in aircraft, or Commerce Department regulations covering the manufacture and sale of devices intended for consumer use in the home, NHTSB regulations for automotive systems, or FDA regulations for devices or systems used in a medical context.

RF related regulations – This category might include regulations imposed by the FCC or ITU governing RF emanations, adherence to frequency band restrictions, signal strength, spurious signals (such as side channels, noise, or harmonics produced outside of the device’s nominal frequency allocation), etc.

In some IoT contexts, such as home automation, HVAC, etc. another layer of regulations might be imposed in the form of building codes in various jurisdictions.

While the area is still developing, it is quite possible that at some point, there will be regulations imposed or referenced by insurance companies as part of their risk models for pricing coverage of structures, vehicles, systems, or businesses incorporating IoT systems and devices.

### Consumer protection

#### Description

“Consumer protection” pertains to the need to support applicable legal/regulatory requirements whenever an IoT system (or an IoT system to which it is connected) involves a consumer anywhere in its operation.

NOTE 1: In many jurisdictions consumer protection requirements apply only to individuals. In some jurisdictions “consumer protection “also applies toorganizations, i.e., legal or artificial Persons.

NOTE 2: In those jurisdictions which define consumer protection focussed on individuals, there is an overlap between consumer protection and privacy protection requirements with respect to personal information or PII.

#### 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 embedding “things” with Internet WiFi capability to connect via an IoT system in the products which they sell.

Such 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 it is recognized that with respect to collection, use and EDI of personal information, many of the legal or regulatory requirements pertaining to consumer protection are similar in nature to those of privacy protection.

It is generally advisable that customers are provided with the ability to opt-in or opt out of sharing of customer-related data. Additionally, this option should be offered in a way that is defensible as reasonable, based on national legal standards. The choice of whether to use an opt-in model or an opt-out model is one which needs to be carefully considered.

Nevertheless there are consumer protection issues which an IoT must be able to address Examples include whether or not a consumer agrees to the activation/use of an IoTdevice embedded in the product purchased, whether or not having or using a thing in IoT and allowing it to be connected to the product or service provider is a condition of sale or lease.

#### Examples

An individual purchases a (high-end) refrigerator/ freezer. It includes an embedded chip with Wi-Fi capabilities 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.

### Trust/trustworthiness

#### Description

Trustworthiness is the 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].

#### Relevance to IoT systems

Device, data and service trustworthiness is of utmost importance for IoT systems to ensure that only trusted devices participate in the decision-making process of the system, resulting in the provision of trustworthy applications. Device executable processes and data must be trusted to ensure that the device/system operates as intended.

#### Examples

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.

# 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

## Main purpose

The conceptual model (CM) provides a 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 fundamentals of the IoT systems by asking the 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 are the relationshipsbetween the entities, especially between digital entities and their physical entities?
4. Who and where are the actors?
5. How the things and services collaborate via the network?

The following clauses describe the conceptual reference model focusing on the above five points. The models presented here use simplified Unified Modelling LanguageTM (UML®, hereafter “UML”). Subclause7.2 provides a short description of the simplified UML[[1]](#footnote-2) in order to help readers to better understand CMdiagrams presented in this standard.

## Interpreting model diagram

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

* Concepts are represented as UML Classes with no attributes.
* The documentation for each concept is the definition of the concept.

Only two kinds of associations are used:

1. Generalization (an “is-a” relationship): For example, a sensor is anIoT device. This generalization relationship can be expressed as shown in Figure 4:



Figure 4 - Generalization.

1. Directed association (expresses relationship between concepts. These association names are verbs.). Figure 5expresses the association relationship that the Sensor monitors the Physical Entity (the thing).



Figure 5 - Association.

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

If a concept, which is a generalization of a concept on the diagram, is not itself shown on the diagram, the name of that generalized concept appears in italics at the top right corner of the box as shown in Figure 5(“*Entity*” and “*IoT device*”).

## The big picture



Figure 6 -Big Picture for IoT Concepts of the CM.

The model diagram in Figure 6provides the big picture of all key IoT entities defined in this CM, their relationships and their interactions. The IoT-User can be human (human user) or non-human (digital user) such as robots or automation services, which act on behalf of human users. Digital user consumes remote services through endpoint, which is attached to the communication network, while a human user interacts through applications, which are implemented by a set of components. Some of the components of application can communicate with remote services via network using exposed endpoint..Physical entity here is the thing which is to be controlled by an actuator or monitored by a sensor. A virtual entity represents a physical entity in the IT world. Both actuators and sensors are kinds of IoT device. IoT devices may interacts through an endpoint to have network communicate directly or connected with an IoT gateway first if itself does not itself have communication capabilities. Services are implemented by components and they can be located anywhere. Services can be discovered and consumed via different types of networks through endpoint.

The following clauses provide more details of entities and their relationship with a focus on their key concepts.

## Concept

### IoT Entities and domains



Figure 7 - Entity and Domain Concepts of the CM.

Figure 7shows the whole IoT family of entities. A thing with distinct and independent existence is called an 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. In order to have a simple concept about IoT entities and their relationship, four fundamental entities are defined here, the thing (Physical Entity), the user (IoT-User), IT systems (Digital Entity) and the networks (Network).

A 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. An IoT-User is an entity which can be human or non-human, while a physical entity is discrete, identifiable and observable.A network is another important entity in the IoT world, through which other entities can be communicated with each other.Any entity may have an identity, and identifiers are one way for an entity to get into communication with other entities 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 characteristics into a specific domain. Each domain has its own boundary. Showing interaction between domains instead of between all the entities in a system can provide a simpler high level view of how the complex system works. Figure 8shows that one IoT domain A interacts with another IoT domain B. Of course, one IoT domain can also interact with multiple IoT domains.

Domain interaction.emf

Figure 8 - Domain interactions of the CM.

Domains are composed of various types of entity. Sometimes one large domain can be segmented into more sub-domains. Figure 9shows that Domain A contains two sub domains, Domain C and Domain D.

Sub Domains.emf

Figure 9 - Domain composition of the CM.

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

#### Entity

The Conceptual Model defines the following relationship from this concept.

Table 1 - Entity

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Identity | Entity has identity. |

#### Domain

The Conceptual Model defines the following relationships from this concept.

Table 2 - Domain

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **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 |

#### Digital entity

The Conceptual Model defines the following relationship from this concept.

Table 3 - Digital entity

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | Entity | A Digital Entity is a specialization of Entity. |
| **2** | Association | Digital Entity | A Digital Entity may contain other Digital Entities |

#### Physical entity

The Conceptual Model defines the following relationships from this concept.

Table 4 - Physical entity

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | Entity | A Physical Entity is a specialization of Entity. |
| **2** | Association | Physical Entity | A Physical Entity may contain other Physical Entities |

#### IoT-User

The Conceptual Model defines the following relationships from this concept.

Table 5 - IoT-User

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | Entity | An IoT-User is a specialization of Entity representing a human user or digital user. |

#### Network

The Conceptual Model defines the following relationship from this concept.

Table 6 - Network

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | Entity | A Network is a specialization of Entity. |

### Identity



Figure 10 - Identity concept of the CM

Figure 10shows the identity concept. Most entities in IoT especially physical entity (“Thing”) need an identity. An identifier can be understood as a dedicated, publicly known attribute or name for an identity, a person or a device. Typically, identifiers are valid within a specific context. A thing can have more than one identifier, but it requires at least one unique identifier within any environment or context through which it can be accessed. For example, the identity information from a Tag can be used as an Identifier to identify the Physical Entity to which it is attached.

The following subclauses provide a short text description in table form regarding the corresponding associations shown in Figure 10. In the description of the relationship between two entities, only entities with outgoing relationships are described.

#### Identifier

The Conceptual Model defines the following relationships from this concept.

Table 7 - Identifier

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Entity | Identifier identifies Entity. |
| **2** | Association | Identity | Identifier distinguishesidentity. Identity may have more than one identifiers |
| **3** | Association | Identity Context | Identifier identified within a given identity context |

### Services, components, and endpoints



Figure 11 - Service, component, and endpoint concepts of the CM.

Figure 11shows how services and components are connectedthrough 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. AnEndpoint has one or more network interfaces. Services, which are located remotely, can be reached by endpoints through network interfaces across a 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.

The following subclauses provide a short text description in table form regarding the corresponding associations shown in Figure 11. In the description of the relationship between two entities, only entities with outgoing relationships are described.

#### Component

The Conceptual Model defines the following relationship from this concept.

Table 8 - Component

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Endpoint | A Component exposes an Endpoint. |

#### Endpoint

The Conceptual Model defines the following relationship from this concept.

Table 9 - Endpoint

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Endpoint | An Endpoint may contain more than oneNetworkInterface. |

#### IoT Gateway

The Conceptual Model defines the following relationships from this concept.

Table 10 - IoT Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Network | The Network from which interactions are forwarded. |
| **2** | Association | Network | The Network to whichinteractions are forwarded to |
| **3** | Association | Endpoint | An Endpoint from which interactions are forwarded |
| **4** | Association | Endpoint | An Endpoint to which interactions are forwarded to |

#### Service

The Conceptual Model defines the following relationships from this concept.

Table 11 - Service

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **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 and exposed by an Endpoint. |

### IoT User



Figure 12 - IoT User concepts of the CM.

As shown in Figure 12, actors of IoT systems are IoT-Users. An 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 in machine to machine interactions.A digital user interacts with a physical entity directly or indirectly through the endpoint. A Human User interacts with entities via Applications. IoT user also uses endpoint to communicate with other IoT user or services in the network.

The following subclauses provide a short text description in table form regarding the corresponding associations shown in Figure 12. In the description of the relationship between two entities, only entities with outgoing relationships are described.

#### Human user

The Conceptual Model defines the following relationships from this concept.

Table 12 - Human user

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | IoT User | A Human User is a specialization of an IoT-User. |
| **2** | Association | Application | A Human User interacts across the Network via an Application. |

#### Digital user

The Conceptual Model defines the following relationships from this concept.

Table 13 - Digital user

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | IoT-User | A Digital User is a specialization of IoT-User |
| **2** | Association | Endpoint | A Digital User interacts with an Endpoint through local (non-networked) interfaces to usefunctions offered by the IoT system across the network. A component implementation could combine the endpoint capabilities with the Digital user capabilities. |

#### Application

The Conceptual Model defines the following relationship from this concept.

Table 14 - Application

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Component | AnApplication is implemented by a Component |

### Virtual Entity, Physical Entity and IoT Device



Figure 13 - Virtual entity, physical entity, and IoT device concepts of the CM.

Figure 13shows the relationship between virtual entity, physical entity and IoT device. Actuator and Sensor areIoT Devices which have direct or indirect contact with Physical Entity. An actuator executes digital information to alter some property of a physical entity. A Sensor perceives certain characteristics of a Physical Entity and transforms them into a digital representation.. Actuator and Sensor are kinds of IoT Device, which converts variations in one physical quantity, quantitatively into variations in another.

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

The following subclauses provide a short text description in table form regarding the corresponding associations shown in Figure 13. In the description of the relationship between two entities, only entities with outgoing relationships are described.

#### IoT device

The Conceptual Model defines the following relationship from this concept.

Table 15 - IoT device

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Endpoint | AnIoTDeviceinteracts on the network, through an Endpoint with which it interacts using local (non-networked) interfaces. A component implementation could combine the endpoint capabilities with the IoT device capabilities. |

#### Sensor

The Conceptual Model defines the following relationships from this concept.

Table 16 - Sensor

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | IoT Device | A Sensor is a specialization of an IoT Device |
| **2** | Association | Physical Entity | A Sensor monitors a Physical Entity |

#### Actuator

The Conceptual Model defines the following relationships from this concept.

Table 17 - Actuator

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Generalization | IoT Device | An Actuator is a specialization of an IoT Device |
| **2** | Association | Physical Entity | An Actuator acts on a Physical Entity. |

#### Virtual Entity

The Conceptual Model defines the following relationships from this concept.

Table 18 - Virtual entity

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Relationship Type** | **Related Concept** | **Description** |
| **1** | Association | Endpoint | A Virtual Entity interacts through an Endpoint |
| **2** | Association | Physical Entity | A Virtual Entity represents a Physical Entity |

# IoT Reference model and Reference architecture views

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

## Relation between CM, RMs and RAs

A reference model (RM) is an abstract framework for understanding significant relationships among the entities of anenvironment, 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 common semantics that can be used unambiguously across and between different implementations.

There are a number of concepts rolled up into that of a reference model. TheRM 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 another, and exhibit joint properties). A list of entities, 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 the problem to be 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 of a class of problems, not to provide specific solutions for those problems. With respect to this, it must aid the process of inventingand evaluating a variety of potential solutions in order to assist the practitioner. The RM is useful: (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 entities.

The reference architecture (RA)can be understood as contexts provided with common features, vocabulary, and requirements, together with supporting artefacts to enabletheir use.The artefacts are the description of the major foundational architecture components, which provide guidelines and constrain for instantiating solution architectures.The solution architectures can be defined not only from differentemphases or viewpoints but also at many different levels of detail and abstraction; they consist of a list ofentities and functions and some indication of their connections, interrelations and interactions with each other andwith functions located outside of predefined architecture patterns representing the entities and functions.[[2]](#footnote-3)

Figure 14shows the architecture continuum from the CM through the entity-based RManddomain-based RM to a number of different views of the 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 clear documentation ofthe architecture descriptions.



Figure 14 - Relation betweenIoTconcept model, reference model, and reference architectures.

In this standard, after examining various kinds of deployed IoT systems and developingthe IoT Conceptual Model 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 of the IoT systems for the various purposes and uses of the RM.

## IoT Reference models

### Entity-based reference model

Based on the previous high level IoT conceptual model, a composite entity based reference model of system level can be developed. The digital entity from conceptual model can be categorised into three groups of basic systems: IoTdevices,IoT gateway and IoT enabled systems.A composite entity-based reference model of IoT systems is shown in Figure 15. This figure illustrates the interactions between the entities using arrowhead lines.



Figure 15 - IoT reference model (Entity-based).

From Figure 15, the physical entities are the “Things” that are to be monitored and controlled by IoT devices directly. IoT devices may contain sensors or scanners to retrieve some information from the physical entities, and it may also have actuators to control the physical entities. Data exchanging between IoT Devices and Backend can be achieved through different ways based on the capabilities of different IoT Devices. Some IoT Devices can be connected to the network directly, some must use IoT Gateway for communicationswith Networks, and some can be connected with local systems immediately without usingNetworks. IoT Gateway is another important entity, which provides a secure and reliable communication between IoT Devices and the Cloud or Enterprises through the entire Networks. In addition, IoT gateway also has local data processing capability, which enables preprocessing and filtering of data locally to increase data delivery and control efficiency.

A large number of IoT related data, service and applications can be hosted by IoT Enabled System. Typical IoT related services and applications can be:

IoT Device management (attach, collect & organizes, configuration, secure connectivity, visualization, firmware update),

IoT related information management which deals with the large number of data from IoT Devices and other sources (storage, archive, metadata management, reporting, data streaming, data parsing and transformation, management of unstructured data),

IoT related analytics services for improving business performance (predictive, cognitive, real-time and contextual),

IoT related risk management services (security analytics, data protection, auditing/logging, key/certification management and org specific security) etc.

IoT users (including human or digital application) are the actors in this reference model. They consume IoT services by connecting to IoT Enabled System directly or via Networks, and in some cases they communicate with IoT Devices without Networks or IoT Enabled Systems.

“Security & privacy" and "operation & management" are two important elements for IoT, which need to be considered as end to end solutions across all entities.

Based on astudy of the decomposition of variousIoT systems in different application scenarios, Figure 16extracts theIoT entities found in most of the IoT systems. Additionally, this figure provides a very high level relationship between Domain and Entity.



Figure 16 - Domain and entity relationship, and representative conceptual entities in the IoT systems.

#### IoT Device

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

An IoTDevice is the technical artefactfor bridging the real world of Physical Entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, processing, storage, communicationcapabilities. An IoTDevice is attached to or in proximity to Physical Entity. In certain situations, IoTDevices can be structurally embedded in Physical Entities. In other situations, IoTDevices, especially Sensors, can be located away from the Physical Entitiesandmonitor the Physical Entities from a distance.

In IoT systems there are some key types of IoTDeviceswhich takeavital role in the IoT systems,providing the technological connection for interacting with, or gaining information about,the physical entity; thisenhancesthe physical entity and allowsit to be a part of the digital world. The IoTDevicecan be an aggregation of several devices of different types.Figure 17shows the key IoTDevices in an IoTSystem,andTable 19provides the description for each type of IoT Device.



Figure 17 - The key IoTDevices.

**Table 19 - Description of IoT Devices shown in** Figure 17**.**

| **IoT Device** | **Description** |
| --- | --- |
| Sensor | Sensors provide the 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 to 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. This can include adjusting Sensors (sensitivity), or platforms, on which Sensors are mounted, e.g. pan, tilt and zoom for a camera, or engaging thrusters in a satellite. Some Actuators can activate or deactivate functionalities of a Physical Entity or a group of Physical Entities. |

#### 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 infrastructurethat provide connectivity from one network to another network, from one domain to another domain, and so on. Network can be wired or wireless using different kinds of communication protocols.

The communication connectivity of Networks 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, personal area network body area network, etc.).

#### IoT Gateway

An IoT Gateway is a forwarding device enabling aconnection between the sensing or actuating subsystem and other subsystems.

#### Physical Entity (Things)

A Physical Entity whichis part of an IoTsystem isan element in the environment for which the IoT system is responsible and whose characteristics, function, status, or behavior is sensed, monitored or controlled by the IoT system.

#### Operations & Management System

The Operations & Management Systemobserves, operates, maintains, and manages all IoT system assets including, but not limited to, Networks, IoT environments, IoT Devices, etc.

#### Resource & Interchange System

The Resource & Interchange System supports IoT system’s connectivity with other external IoT or non-IoT systems.

#### Application Service System

The Application Service System has various applications which provide IoT services to the IoT User.

#### IoT User

The IoT User is an individual human user or non-human user, or an organization, which requests IoT services and is provided the requested service by a service provider in an IoT system.

### Domain-based reference model

#### Introduction

Figure 18shows the domain representation of the IoTreference 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).Each identified domain is mutually exclusive from the other domains.



Figure 18 - IoT reference model (Domain-based).

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) which appear in the domains other than the PED and the SCDsupport functions and capabilities 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 links, which can be point-to-point links) in IoT systems (both 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 communication and data/information exchange activities and interactions. The 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.

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 local area network, Internet, Intranet, enterprise backbone network, wide area network, etc. Business-to-business (B2B) networks are also considered as inter-domain communication/data network.

##### The User Domain (UD)

Usersare the stakeholders and actors of the User Domain (UD).A usercan be an individual person, a group of persons (e.g., a household or a company) or local/state/provincial/federal governmentdepartment.

##### The Physical EntityDomain (PED)

The Physical EntityDomain (PED) consistsofphysical entities that are “the things within the ambitof an IoT system.” Therefore, the PED is the primary environment within whichan IoT system is responsible for tasks or functions such as monitoring, sensing, and controlling. The objects in the PED can be a myriad of different kinds of physical entities and virtual entities. The owner of the PED is a stakeholder. However, this stakeholder may not show up as an entity in the PED. A person or persons can be one of the entitiesin the PED.

##### The Sensing &Controlling Domain (SCD)

Sensing and controlling domain (SCD) is the most essential domain of an IoT system because the SCD provides critical information about an environment (i.e. PED) to all the other domains of an IoT system. In addition, the SCD can manipulate the state of physical entities in the IoT system environment through actuation.

##### The Operations &Management Domain (OMD)

System operators and managers are the actors of the OMD. The operators and managers maintain the overall health of IoT systems.The OMD represents the collection of functions responsible for provisioning, managing, monitoring and optimizationof the systems’ operational performance in real-time.

##### The Resource & Interchange Domain (RID)

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 source can be physical, monetary, ordigital (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 play its role, the RID needs access to the digital resourcesby permission of other domains (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 data after processing arestored in the service providers’ database. In the RID, additional data processing may beperformed, if required, to accommodate the external organizations. Thisadditional processing may include data quality ensurance, data transformation, distribution and storage.

##### The Application Service Domain (ASD)

Application service providers are the actors of the ASD. Application service provider organizations provide service to the IoT-Usersin the UD. The ASD has a set of applications that form an application domain within the ASD.

The ASD contains 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 theirrequestsbut also with entities in the SCD (i.e. sensors and actuators) to gain data from Physical Entities 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 platforms, law enforcement, utilities, financial institutions, governments, 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.

### Relation between the two reference models

Based on the entity-based RM in Figure 15and the domain-based RM inFigure 18, a mapping relation between thetwo RMs can be achieved as shown inFigure 19, wherethese two RMs are consistent with each other.



Figure 19- Relation between the concept model and the reference model.

Following Figure 19, the corresponding relationship between the entities in the entity-based RM and the domains in the domain-based RM is listed inTable 20.

Table 20- 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 (UD) |
| Application Service System | Application Service Domain (ASD) |
| Operations & Management System | Operations & Management Domain (OMD) |
| Resource & Interchange System | Resource & Interchange Domain (RID) |
| IoT Device | Sensing &Controlling Domain (SCD) |
| IoT Gateway |
| Physical entity | Physical Entity Domain (PED) |
| Networks | Communication and interactions among the domains |

## IoT Reference architecture (IoT RA) views

### General description

**Editor’s Note:** The text of the different views is updated based on the output from Ad hoc group for architecture views, and reach the consensus in Berlin meeting.

The IoT RA is describedby the following five reference architecture views:

1. IoT RA Functional View
2. IoT RA System View
3. IoT RA Communications View
4. IoT RA Information View
5. IoT RA User View

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.

### IoT RA Functional view

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

* Functions in each domain; and
* Cross-domain functions.

Each functional component is realized by one or more implementations of actual system components, which may be deployed to form a working system.Figure 20shows the decomposition of the IoT RAfunctional components. In this figure, there are two parts: inside-domain functions and cross-domain functions. The functional components are very general and optional based on specific applications. For a specific IoT system, some components may not exist at all.

#### Inside-Domain Functions

As shown at left side of the figure, the inside-domain functions are depicted as follows:



Figure 20– IoT RA Functional View –Decomposition of IoT RA Functional Components.

##### The Sensing &Controlling Domain (SCD)

The SCD is comprised of a set of common functional components whose implementation complexity depends on the infrastructure of IoT systems.

* 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 has a tighter 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 effect the actuation. Its implementation may span hardware, firmware, device drivers and software elements.
* Executor is the functional component that executes logic which controls states, conditions, and behaviour of the system and its environment, in accordance with control objectives.
* Identification is essential for a system to enable the entities to be identifiable and traceable, so that the system can distinguish an entity from others.
* Network Access is for connecting between sensors, actuators, controllers, gateways, and other edge systems. Access mechanisms take different forms, such as a bus (local to an underlying system platform or remote), or networked architecture (hierarchical, hubs and spokes, meshed, point-to-point), some statically configured, and others dynamically. Quality of Service (QoS) characteristics such as latency, bandwidth, jitter, reliability, and resilience must be taken into account.
* Local Modeling deals with understanding the states, conditions and behaviors of the systems under control and those of peer systems by interpreting and correlating data gathered from sensors and peer systems.
* Asset Management enables operations management of the control systems including system onboarding, configuration, policy, system, software/firmware updates and other lifecycle management operations. Note that it is subservient to the executor so as to ensure that policies (such as safety and security) are always under the responsibility and authority of the edge entity.

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 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).

##### 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.

##### The Operation &Management Domain (OMD)

The OMD represents the collection of functions responsible for life cycle management, business support, security & safety management, and regulation management. Management functional component consists of a set of functions that enable management centres to issue a suite of management commands to the control systems or the corresponding devices. The life cycle management provides several types of functional components for the IoT system operations: provisioning, deployment, monitoring, maintenance, prognostics, diagnostics, optimization, billing, etc..

* 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.
* Monitoring and Diagnostics functional component consists of functions that enable detection and identification of problems when orafterthey occur.
* Prognostics functional component consists of a set of functions that serve 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 improve asset reliability and performance, reduce energy consumption, and increase availability and output in correspondence to how the assets are used.

##### The Resource & Interchange Domain (RID)

The main functional components are resource management, analytics, resource interchange, access control, and so on. The IoT resource, which can be shared within an IoT system or with other IoT systems, could be intelligence, knowledge, information, data, etc. The IoT resource & interchange domain performs interchange of the IoTresource for the whole IoT system with other systems. Moreover, stakeholders in the RID need to provide data of the IoT system, give analytics about the resource data, and use cloud for data storage.

##### The user domain (UD)

The main function for the UD is how to use the IoT service. Here the functional components are users and HMI (human machine interface) which provides the interface for user to access, subscribe and receive the services provided by the application service domain.

##### The Physical Entity Domain (PED)

There is no function in thePED.

#### Cross-Domain Functions

As shown at right side of Figure 20, it is an overview of the cross-domain functions. The cross-domain functions are the functions exist all over the six domains as described in the IoT Reference Model (Domain Based), which include security, safety resilience, trust & privacy, connectivity, interoperability, dynamic composition & automated interoperability, etc.. All these cross-domain functions are common, essential and implemented through the union of some functional components in the six domains. Each function can be expanded in the functional domain decomposition. For example, function of privacyis realized through the data privacy protection in the sensing and transmission, API & Portals, Monitoring, information resource interchange and HMI etc.

* The security function refers to the ability of IoT system to ensure the confidentiality, integrity, authenticity and confirmation of the exchanged information. The IoT RA integrates security policies for IoT components as core to system design. For example, Asset Management in the SCD enables operations management including system onboarding, configuration, policy, system, software/firmware updates and other lifecycle management operations. In the RID, Access Control and the Resource Management are responsible for data security, data access control and data rights management.
* The safety & resilience functionis a superset of fault tolerance and very much related to autonomic computing notions of self- healing, self-configuring, self-organizing and self-protecting, e.g., the IoT component can take advantage of the hierarchical network to do self-optimization.
* The trust & privacy functionis to distinguish different levels of trust for a party (e.g., application, system, network, etc.) during data transmission or exchange procedure in order to protect the confidentiality of data. Usually, validation is required before the trust is established and trust can be enhanced by reputation-based approaches. Privacy is achieved mostly via authentication. In addition, in order to prevent leaking of confidential data to meet privacy requirements, data access rules may be used for data requisition, removal, encryption, etc.
* The connectivity functionprovides the capability of heterogeneous integration for IoT components, either belonging to different networks or using different technologies, to achieve seamless connection of each “thing” in the world.
* The interoperability functionshows the capability to exchange information of an IoT system based on common interpretation of information in context. Basically, two levels of data interoperability are considered. Syntactic interoperability is to exchange information in a common data format with a common protocol to structure the data. Semantics interoperability is to get the meaning of the symbols in the messages in the right way.
* The dynamic composition & automated interoperability functionprovides a flexible method of composing services so that the IoT components can be dynamically integrated at run-time to enable adaptable services. Semantic interoperability is required to support the dynamic composition.

### IoT RA System View

The system view describes the generic components (such as devices, sub-systems, networks, etc.) in each domain to form an IoT system. Different from the functional view which describes an IoT system from the perspective of logical functional block, the system view is from the perspective of physical components. More specifically, the system view describes the following issues:

* Key physical components (e.g. sub-systems, devices, networks) of an IoT system.
* The general architecture of an IoT system, includingthe structure of an IoT system, the distribution of components, and the topology that how components are interconnected.
* A technical description of its components, including behaviors and other properties.



Figure 21-IoT RA System View.

In Figure 21, IoT RA system view is shown along with all the entities involved in each domain and the connections among them from the viewpoint of system composition. The entities in each domain are very general and optional based on specific applications. There are four different kinds of networks to connect the physical components in the six domains of anIoT system: proximity network, access network, services network, and user network. More detailed description about these four networks will be introduced in 8.3.4.

#### Physical Entity Domain (PED)

In the PED, there are no devices or sub-systems. Instead, itmainly consists of sensed physical objects and controlled physical objects, which are related to IoT application and interested by users. Sensed physical object is a physical entity that is acquired information by sensing equipments, while controlled physical object is a physical entity controlled by controlling equipments.

#### Sensing & Controlling Domain (SCD)

In the SCD, generally there are sensors, actuators, and IoT gateway or endpoint. Sensors acquire information from the sensed physical object, e.g., physical, chemical, biological properties, etc. Actuators perform operations on controlled physical objects through controlling function units. Sensors and actuators sense and control physical objects independently or collaboratively. IoT Gateway is the device to connect SCD with other domains. IoT Gateway provides functions of protocol conversion, address mapping, data processing, information fusion, certification, equipment management, etc. IoT Gateway can either be independent equipment or be integrated with other sensing and controlling devices. The SCD might also include some local control systems such as Asset Management, Executor, etc., depending on the complexity of the IoT system infrastructure.

#### Application Service Domain (ASD)

In the ASD, generally there are basic service system and business service system. Basic service system provides fundamentaldata service, which includes data access, data processing, data fusion, data storage, identity resolution, geographic information service and user management, inventory management, etc.

Business service system is responsible for realization of traditional or new types of Internet specific business functions. The business functions include enterprise resource management (ERP), customer relationship management (CRM), asset management, service lifecycle management, billing and payment, human resource, work planning and scheduling systems.

#### Operation & Management Domain (OMD)

The OMD typically includes operation system and regulation management system. Operation system is responsible for management of IoT devices and control of the operation of the IoT system, to guarantee that the equipments and systems operate safely and reliably. Regulation management system is to guarantee that the IoT application system complies with relevant laws and regulations. It provides inquiry, supervision and execution of relevant laws and regulations.

#### User Domain (UD)

In the UD, users can be human or devices. Both of them interact with other domains via the user interface device, of which human users connects to the user interface device via the human machine interface (HMI). The devices in the UD are the HMI and the user interface device.

#### IoT Resource & Interchange Domain (RID)

In the RID, there are three major sub-systems: (1) Resource management system: store and process the resources. The resources can be divided into two purposes; one is for interior usage, the other is to be shared to and from the external systems. (2) Interchange system: execute the interchange of the resources. (3) Access management system: control access for the stored resource in RID and anything within an IoT system. Therefore, RID kindly plays a role of bridge between an IoT system with its outside world. For example, a cloud servicer can act as a physical system of RID. A cloud servicer in an IoT system can remotely store the data, and also share the data with others if needed. Certainly, the cloud servicer has access control for safety and privacy purpose.

The working procedure of the systems in the RID is described as follows.

* Case 1: When the external systems require resources from theIoT system, including data, financial transaction, etc., they first send request to Interchange Systems in RID. Then Interchange System forwards the request to Access Management System, which decides whether to accept this request. If accepted, it authorizes ASD, SCD or other domains to provide relevant resources, which is sent back to Resource Management Systems for data format conversion, data fusion, etc. Then Data Management System transmits those requested resources to Interchange System, which acts as an interface between theIoT system and external systems. If not accepted, Access Management System directly sends command "No" to Interchange System, which says "No" to the request from the external systems.
* Case 2: When theIoT system requires some resources from the external systems, it first sends request to access management system in RID for access authority. After that the access is authorized, it sends resource interchange request to the interchange system in RID, which forwards this request further to the external systems. When it gets positive response, it delivers relevant resources and and stores them in the data management system in RID. Then data management system further forwards the resources to the origin of the request in the interior IoT system, such as ASD, SCD. When interchange system receives negative response, it delivers this message to the origin of the request.

### IoT RA Communications view

The IoT RA communications view describes the principal communications networks which are involved in IoT systems and the entities which they connect. The principal communications networks are shown in Figure 22.

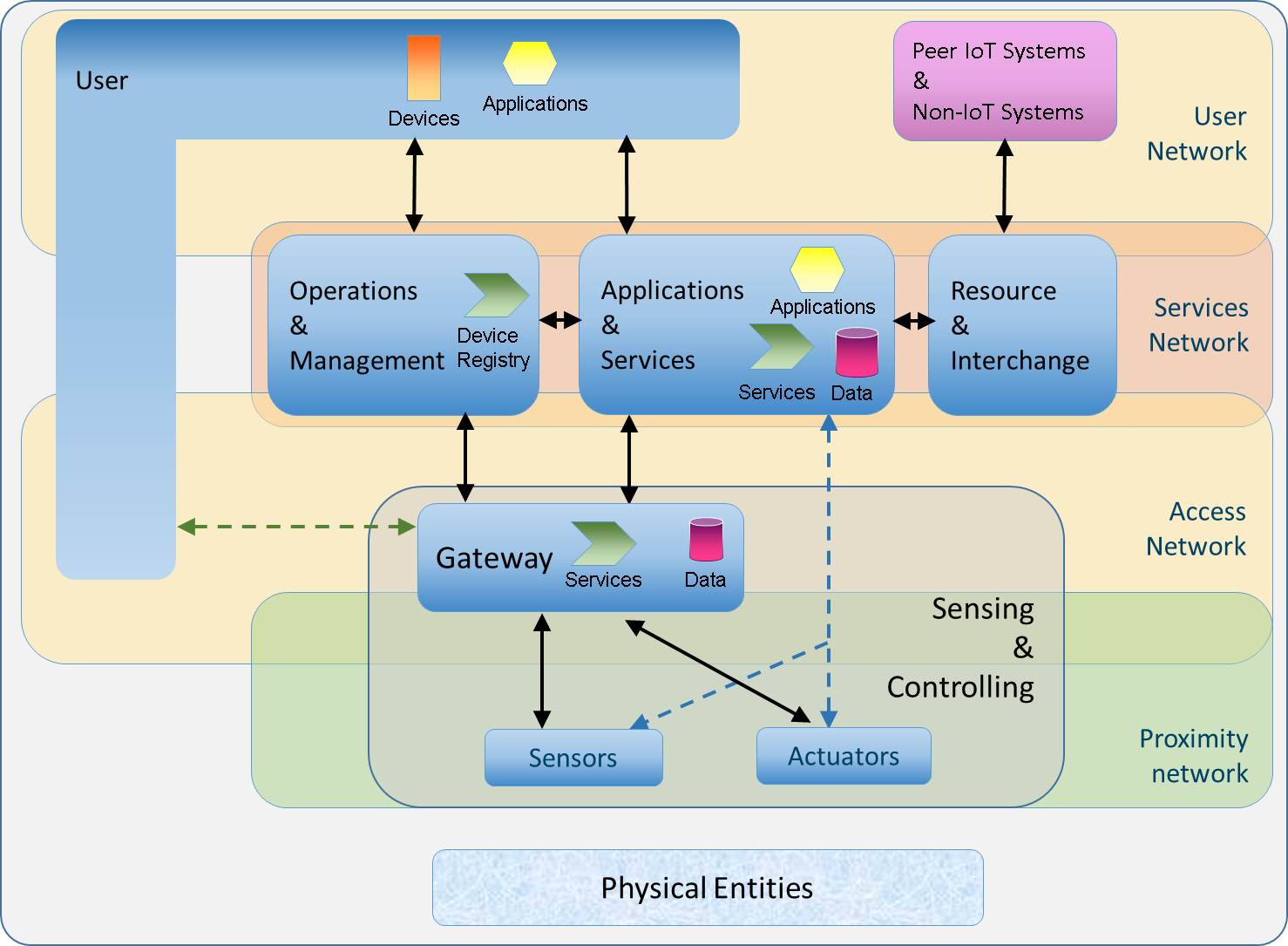


Figure 22- Principal Communication Networks of IoT Systems

The four principal communications networks are:

1. Proximity Network. This network exists within the Sensing and Controlling domain. Its main task is to connect the Sensors and Actuators to Gateway. Proximity networks are typically local and limited in range, largely necessary because Sensors and Actuators are low power, or are in locations that make wide area connections (such as the internet) difficult or impossible to provide.

Proximity networks may use specialized protocols and may not be based on the use of IP protocol.

Proximity Network often uses low power limited range wireless and wired technologies. Current examples include IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), ZigBee, Narrow-Band IoT.

The concept is that individual sensors and actuators may have limited power and limited hardware capabilities so that simple, local, low-power networks are used to connect them to gateways, which are more powerful and which can in turn connect to Access Network.

Proximity Network may involve the use of an address translation capability to translate from addressing schemes used on Access Network to local addressing schemes use on Proximity Network.

2. Access Network. This network connects the devices in the Sensing and Controlling domain to the Application Service domain, to the Operations & Management domain. Access Network is typically a wide area network, often the Internet. Access Network typically connects to gateways, but When Sensors and Actuators are more capable, they may connect directly to Access Network (dashed lines in Figure 1).

Access Network typically uses the IP protocol.

Access Network is a wide area network connecting the Sensing and Controlling domain to the other domains. A range of technologies can be used including wired connections (Broadband / ADSL / Fiber) and wireless connections including Wireless LANs ("WiFi"), Mobile (cellular) networks and Satellite links (particularly for remote locations).

Access Network may involve the use of device registry which holds data about the IoT devices associated with the IoT system and how to communicate with them.

3. Services Network. This network connects elements within and between the Application Service domain, the Resource & Interchange domain, and the Operations & Management domain. This network can include both Internet elements and also (private) intranet elements. It is typical for intranet networks to be used where the elements of the Operations & Management, Application Service and Resource & Interchange domains exist within a single datacenter.

Services Network typically uses the IP protocol.

Service Network connects the applications and services in the Application Service, the Operations & Management and the Resource & Interchange domains, which are typically wired networks within datacenters, running IP based protocols. Where communication spans multiple datacenters, a variety of network technologies may be used, including both dedicated connections and alternatively Internet connections.

4. User Network. This network connects the User domain with the Application Service domain, the Operations & Management domain. It also connects Peer IoT Systems and non-IoT Systems with the Resource & Interchange domain. This network is typically based on public Internet elements.

User Network typically uses the IP protocol.

User Network connects outwards to User devices and outwards to other ("peer"to peer) IoT systems and to other non-IoT systems, which is typically internet-based. The outward facing networks can use any of the technologies commonly used to carry internet traffic, including both wired and wireless systems.

Each of the principal communications networks can be implemented by means of a range of different network technologies, which are used depending on the particular characteristics of the IoT system. IoT system implementations may use multiple instances of each of these networks to create complete solutions.

Notable in Figure 22 is that User domain is shown spanning both the User Network and the Access network. This describes those cases where user devices and their applications connect directly to the Sensing and Controlling domain, for example when the user device is a smartphone which contains sensors.

***Operation of the Access Network: Find and Connect***

An important characteristic of the Access Network is that it involves two operations: find and connect.

IoT systems typically involve a large number of sensor and actuator devices – and their number and type can change over time. These devices also have a set of associated metadata which is necessary or useful when other components of the IoT system interact with those devices.

Information about the IoT devices in the system is held in a Device Registry, as shown in Figure 22. IoT devices that are added to the IoT system are registered into the Device Registry, including information about their network location and their associated metadata.

***Find*** operations are used by other components (such as services, applications, management systems) to query the Device Registry for information about one or more IoT devices.

***Connect*** operations involve the use of the information from the Device Registry to establish communications to the IoT devices over Access Network, which may involve communications via IoT Gateways.

The form of communications that takes place can follow any one of a variety of patterns, such as synchronous requests, asynchronous requests (potentially message based), publish/subscribe/notify messaging, broadcast or multicast.

The registration steps and the find operations may take place during deployment or may be dynamically executed at runtime of the IoT system components.

***Operation of the IoT System networks***

Some network characteristics important to IoT systems, such as end-to-end latency, may need coordinated behaviour across multiple networks within the IoT system, e.g. to ensure that an IoT application can request the correct network QoS for its particular needs. This means that networks supporting IoT traffic require interfaces that allow the operations and management capabilities to manage complete paths.

### IoT RA Information view

In IoT systems there are six domains (i.e. UD, ASD, SCD, OMD, PED, and RID) that generate and consume data and information both dependently and independently from each other.

The data/information generated by monitoring the physical entities in PED is from the IoT devices (e.g., sensors, actuators, RFID reader) and other data entry devices (e.g., SCD data entry terminals deployed in PED). The IoT devices and the other data entry devices are architecturally belong to SCD; therefore, PED does not produce any data/information within. The IoT devices and the data entry devices, which are interconnected to form various types of sensor and control networks in SCD, generate data from the physical entities in PED.

The data obtained by interacting with the PED is the initial source of data that feeds an IoT system. The types of this initial data depend on the types of IoT devices and the embedded capabilities in the IoT devices and also of sensor networks and gateways in SCD, which results in both raw data and processed data. The raw data is the output of the IoT devices without any further data manipulation. The processed data is the data resulted from processing the raw data by certain data processing algorithms (e.g., aggregation, reduction, transformation, partition, etc.). The metadata associated with the raw or the processed data is generated through an embedded capability in the SCD sensor/control network. The sensors and actuators also report its status through the sensor/control networks.

Both raw and processed data are then used by the application/service providers in ASD to serve their customers, by the operators/managers in OMD to operate, administer and maintain their business operations, and in certain cases directly by the users in UD to fulfill their needs. The application/service providers, the operators/managers, and the users use the functionality in RID to communicate and perform various types of transactions with other IoT systems and with external organizations.

Additionally, each domain also generates its own data/information to serve its own domain which is not shared with other domains. OMD generates command and control signals based on the sensor data to control the actuators deployed in PED. In certain IoT systems, command and control signals can be generated by a sensor network or a gateway by embedded control algorithms for automated control operations to immediately manipulate the PED situation/environment, especially to correct an urgent or emergency situations once detected by the sensors and recognized by the data analysis algorithms.

IoT RA Information View expresses the data and information flow as described in the above paragraph and is depicted in Figure 23.The entities in Figure 23 form the basis for the guidelines associated with Information View. The represented entities are not exhaustive of all IoT systems in their information/data flow point of view.

Figure 23 is representative for example, and it does not describe all the potential data flow or exchange between the two entities connected by the line. The entity description is found in , which describes the data flow/exchange between each pair of two entities.



Figure 23 - IoT Reference Architecture Information View.

Table21 - Description of data flow/ contents from one entity to another.

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity 1** | Data flow direction | **Data content** | **Entity 2** |
| User Interface | ► | * Data associated with requesting operational data; * User Status data; * User terminal data. | Management System |
| ◄ | * Management data. |
| User Interface | ► | * Data associated with requesting IoT services; * Data associated with requesting to use the dedicated IoT services; * Data associated with requesting to use the dedicated non-IoT services. | Business Service Systems |
| ◄ | * Data associated with access to the requested service’s data from the service requested; * Data associated with access to the requested services. |
| Basic Service System | ► | * Machine understandable messages (e.g., commands to gather certain types of sensor and/or actuator data), which are to be relayed to Sensing and Actuating entities. | IoTgateway |
| ◄ | * Raw and/or aggregate sensing data; * sensor/actuator status data, etc. |
| IoTgateway | ► | * Data associated with the messages received from Basic Service system and Business system. | Sensor |
| ◄ | * Raw and/or aggregate data, processed data from sensor; * Sensor status data. |
| IoTgateway | ► | * Data associated with the control messages from business service system to manipulate the targeted actuators. | Actuator |
| ◄ | * Data associated with the actuation task response; * Actuator status message. |
| Management System | ► | * Data associated with the actuator control messages to configure the sensor or sensor networks; * Data associated with the actuator control messages to manipulate actuators. | IoTgateway |
| ◄ | * Sensor and control networks status messages; * Specific status response message after completing the command. |
| Information Exchange | ► | * Data associated with the request of data/information packages (e.g., sensor state, aggregated sensor data, analytics, etc.) which originate from external IoT and non-IoT systems. | Management System in UD, OMD, ASD |
| ◄ | * The data exchange request command for external IoT or non-IoT system; * Data associated with the request data/information packages from other IoT or non-IoT systems. |

### IoT RA Userview

#### General description

Whereas the functional view shows the necessary functions and dependencies of the IoT system, the user view focuses on how the IoT system is developed, tested, operated and used from a user perspective. This viewaddresses the following concepts:

* Activities;
* Roles and sub-roles;
* Services and cross-cutting aspects.

#### Description of the roles, sub-roles and related activities

All IoT related activities can be categorized into three user groups as listed below:

1. IoT Service Provider
2. IoT Service Developer
3. IoT User

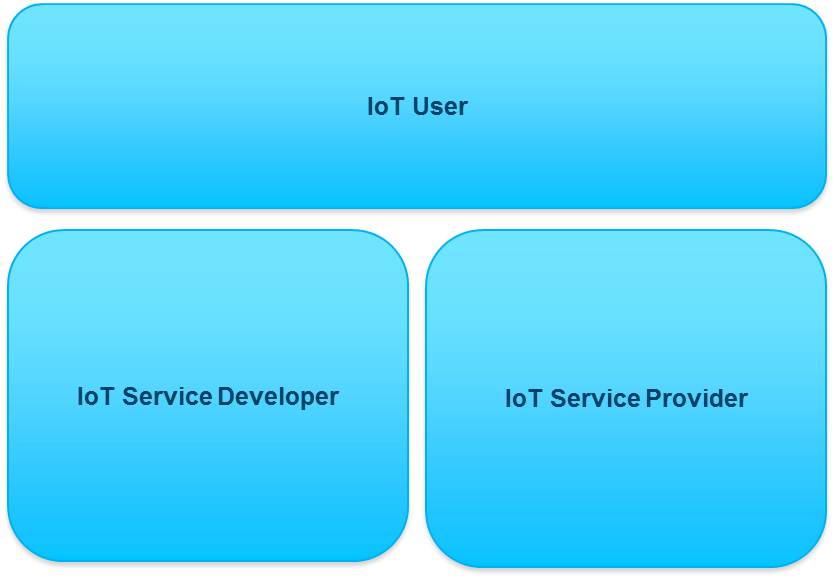


Figure 24 - IoT User Groups and Roles

#### IoT Service Provider



Figure 25 - IoT Service Provider

The role of IoT Service Provider is to manage and to operate IoT services. Following sub-roles can be identified:

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 stakeholder for IoT applications.

A **Service Delivery Manager** is responsible for a service level agreement (SLA) with a client to the line of business (LOB). He and his team of maintenance engineers are on or near the client site and the managed equipment and use the IoT enabled platform and LOB industry applications to plan, installation, monitoring and service equipment. This role ensures that the quality is within the service level agreements agreed with the client.

A **System Operator** handles the day to day system operations for a customer by enrolling new users and making sure that new device types and devices are registered, are behaving correctly, and are up to date with the current secure firmware.

A **Security Analyst** mitigates security risks by proactively creating rules that detect threats and prevent breaches. He creates automation that acts on misbehaving devices and users. And he ensures compliance through audits.

An **Operations Analyst** is responsible for the availability of specific assets in the LOB product line and uses deeper analytics provided by analytics in the IoT platform and data scientist’s algorithmic service extensions.

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.

Figure 26 shows the activities which relate to the sub-roles of IoT Service Provider

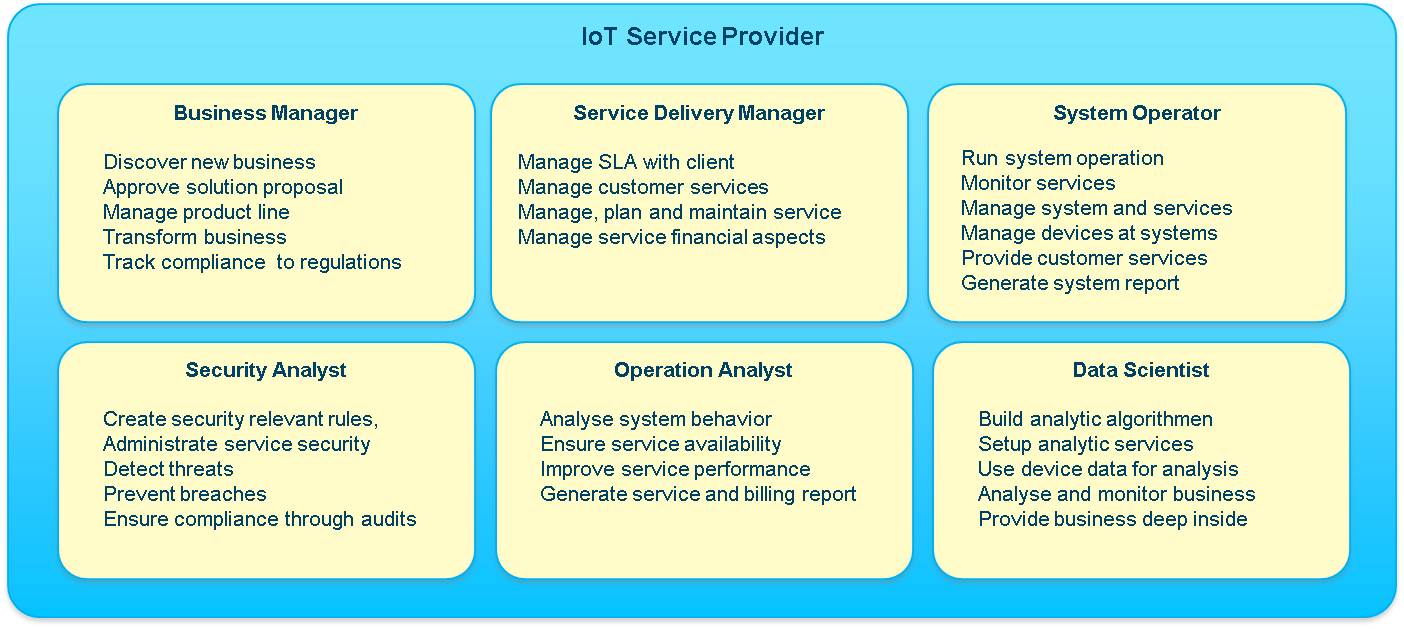


Figure 26 - IoT Service Provider sub-roles and activities

##### IoT Service Developer



Figure 27 - IoT Service Developer

The IoT Service Developer has the roles of implement, test and integrate IoT service to the platform. Sub-roles of IoT Service Developer are described as follows.

A **Solution Architect** proposes, proves and deploys the IoT enabled platform to the LOB. He decides on integration strategies and architectures for the new IoT enabled platform, existing business systems and devices in production.

A **DevOps Manager** sets up, configures and operates the IoT enabled platform, relevant services and acts as a project manager by 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 **Device Developer** integrates hardware and software into devices and applications. He develops and maintains device firmware that securely connects devices to an IoT-enabled platform.

A **System Integrator** tests and integrates IoT services into IoT enabled platform.

All sub-roles and their activities are shown in Figure 28.

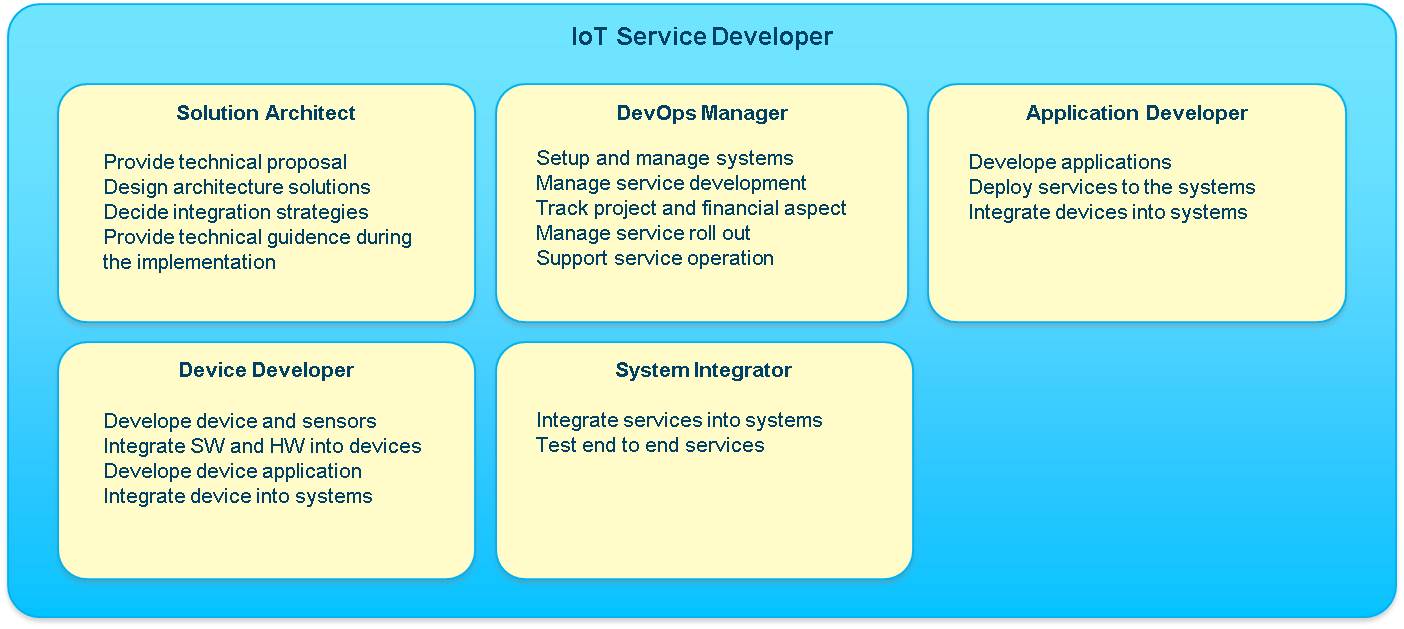


Figure 28 - IoT Service Developer sub-roles and activities

##### IoT User

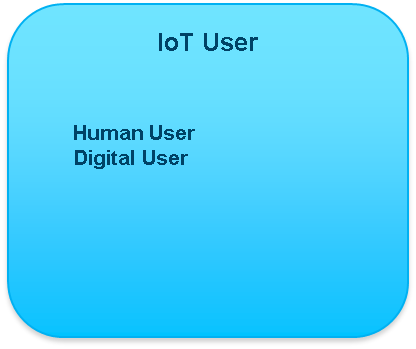


Figure 29 - IoT User

The IoT User is the end-user of IoT services. End-user can be categorized into Human User and Digital User.

**Human User** is an individual person who uses IoT services. There are different kinds of Human Users, such as Enterprise User, Public User, Government User, etc.

Enterprise User can use IoT services to improve companywide operational efficiency (for example field engineer for maintenance work, track driver at logistic company or workers at product line from manufactory industry), or to create new business model (for example company managers work at B2B or B2C area), or to design new products (engineer and designer at manufactory industry), etc.

Public User consumes IoT service for his private interest and use, e.g., for health, sport, travel, shopping, home living, media entertainment, etc.

Government User will use IoT service to improve public services, to help by political decision making for energy saving, environment protection, city infrastructure planning, etc.

**Digital User** is a non-human user of the IoT system. It can include automation services that act on behalf of human user.

All sub-roles and their activities are show in Figure 30.

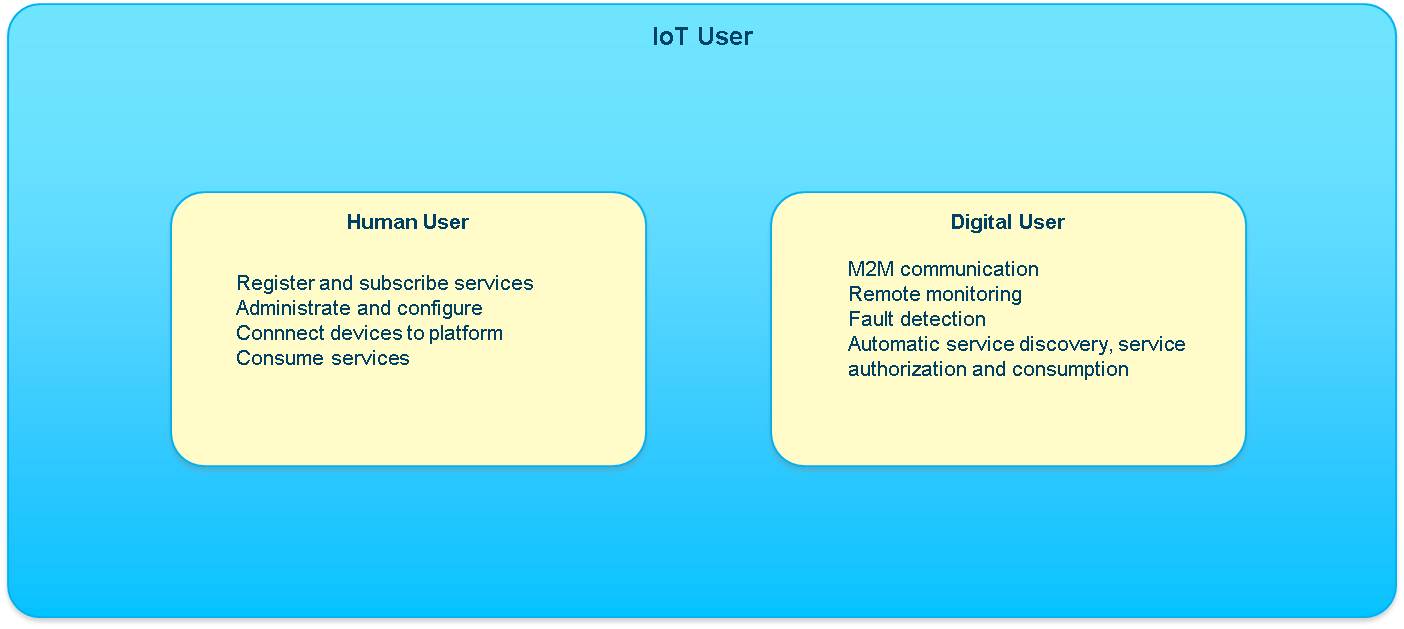


Figure 30 - IoT User sub-roles and activities

#### Mapping activities, roles and IoT systems in domains

The user view addresses the concerns of expected system usage. It typically presents roles or activities involving human or digital users that deliver its intended functionality in ultimately achieving its fundamental system capabilities. Activities for create, implement, test, integrate and operate IoT services in desired systems require cooperation among persons with different roles or skills. Figure 31 shows the roles and their co-operations during the system usage.

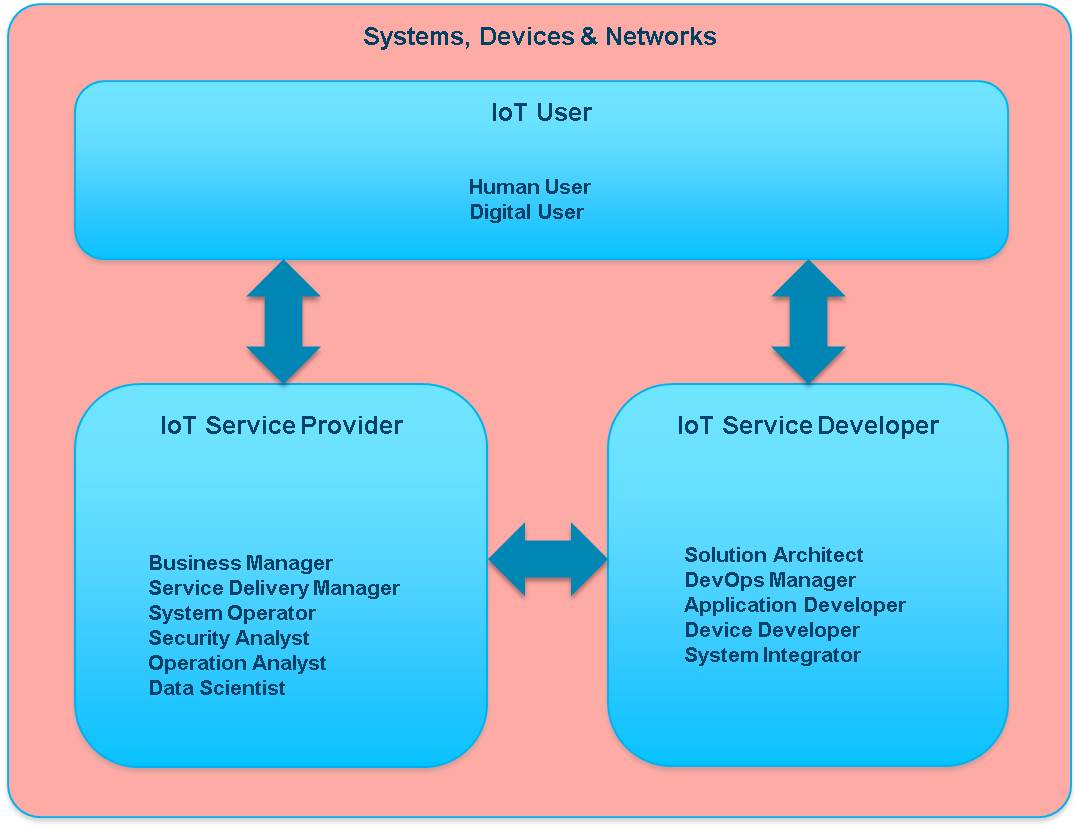


Figure 31 - Cooperation among the roles during the system usage

Table 21 gives an overview about the activities and the roles who are involved by the relevant activities

Table 21 - Overview of activities and roles

|  |  |  |
| --- | --- | --- |
| **Activities** | **Roles** | **IoT systems in domains** |
| Device and Application Development | DevOps Manager, Device Developer, Application Developer | Application Service Domain, Sensing & Controlling Domain |
| Operation of devices, connectivity and applications | System Operator, Service Delivery Manager | Operation & Management Domain, Application Service Domain |
| Use device data for analytics | Data Scientist, Security Analyst, Operation Analyst | Operation & Management Domain, Information& Interchange Domain |
| Integrate, operate and control data stores and business | Solution Architect, DevOps Manager, System Operator, System Integrator, Service Delivery Manager | Application Service Domain, Operation & Management Domain |
| Use real-time, historic and big data for applications and analytics | Data Scientist, Operation Analyst, Security Analyst, Service Delivery Manager | Application Service Domain, Operation & Management Domain, Sensing & Controlling Domain, Information& Interchange Domain |
| Make and operate analytics to run business | Data Scientist, Operation Analyst, Application Developer, DevOps Manager | Application Service Domain, Information& Interchange Domain |
| Bring in analytics to dashboard | DevOps Manager, Data Scientist, Application Developer | Application Service Domain, Operation & Management Domain, Information& Interchange Domain |
| Monitor system state, act on security risks and beaches | System Operator, Security Analyst | Operation &Management Domain |
| Track compliance to regulations | Business Manager, Security Analyst | Application Service Domain, User Domain |

Figure 32, Figure 33, and Figure 34 show some examples of using IoT systems from different activity perspectives.

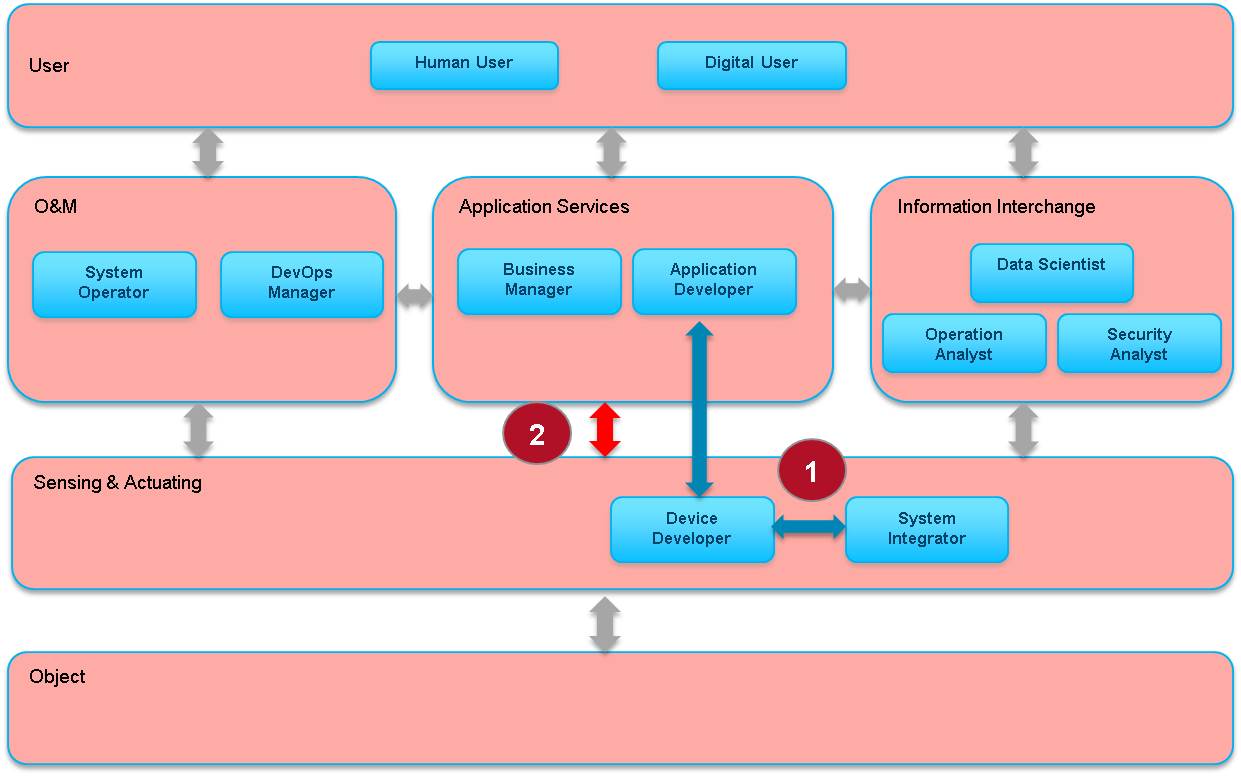


Figure 32 - Activities of device and application development

Figure 32 shows an example of activities during the device application development among device developer, system integrator and application developer. Related activities of using the system can be, for example, connecting new device to the IOT platform. The blue boxes in Figure 32 are the human users (in this case developers and operators) of IoT systems. IoT systems can be categorized into six domains in relevant pink color boxes. For this activity:

1. Device developer communicates with system integrator during the implementation phase. They discuss about API definitions and its functional behavior between the device and backend systems.
2. Application developer implements and tests APIs and its functions for device and back end together with device developer. At this step, devices at Sensing & Controlling domain will be connected to IoT systems at application service domain. End to end functions will be tested.

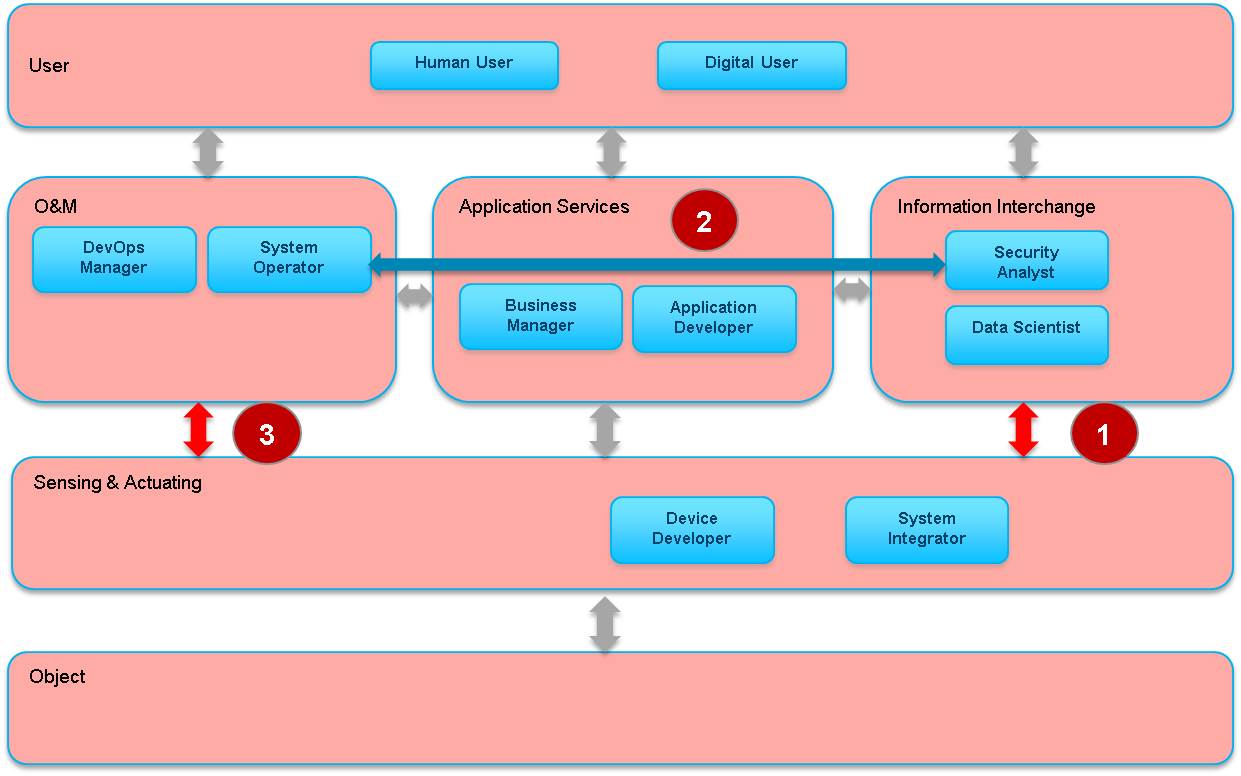


Figure 33 - Activities of using device data for security related analytics and operations

Figure 34 shows the activities of using device data for security related analytics and operations. In this case the user of the IoT systems are the data analyst and security operator. Activities are:

1. After device is successfully configured and connected,usage data will be sending to the IoT systems at Resource & Interchange domain. Security Analyst and Data Scientist can use the collected device usage data to perform security related analyses.
2. Security Analyst communicates with System Operator about the analytic result and findings
3. Security Analyst together with System Operator proactively creates rules to protect systems and to prevent breaches.

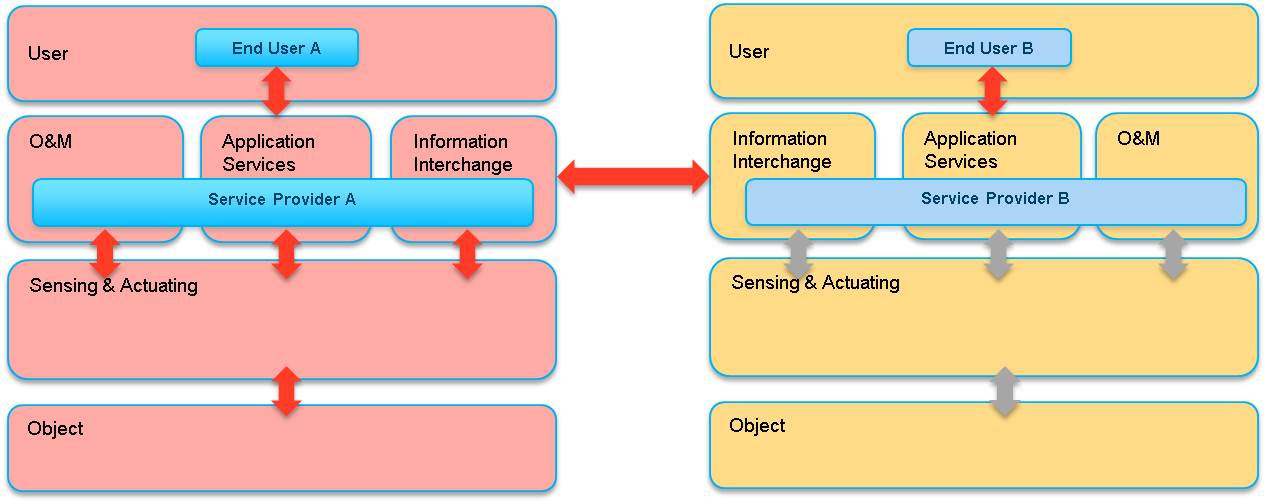


Figure 34 - Activities of using IoT services across vertical sectors

Figure 34 shows another example of using IoT service across vertical sectors. This example is related to consumer and product manufacturing industry (Vehicle manufacturing). The End User A could be the customer who is the owner of a new car.

1. Sensors installed at the car can deliver the vehicle run time status data.
2. IoT services perform the analytics and inform the customer or driver in case of defects or need for inspection.
3. Such customer car usage data together with millions of other customer’s car usage data can be sent to vehicle sensor data market place for car manufactory through Resource & Interchange interface.
4. End User B could be an engineer or designer at the vehicle manufactory industry. Based on the data collected from customer side he can get real-time information of car usage, and identify which mechanical or electrical part will be frequently maintained, replaced or cause errors during the usage. Together with other information, he can further analyze what could be the reasons of the problem. He might also use such information to improve the designs or design new cars with better quality.

#### Roles and activities during the IoT product life cycle (can be moved into Annex later)

IoT services can be used by all vertical sectors to transform every part of business. Generally they can be considered as a kind of enablement platform, which improves operations, or lowers the cost, or creates new products and business models, or drives engagement and customer experiences.

Figure 35 shows roles and activities involved by using existing system to create, develop and operate IoT services.

**Editors’ Note**: the diagram needs some modification based on new comments and suggestions of next review cycle

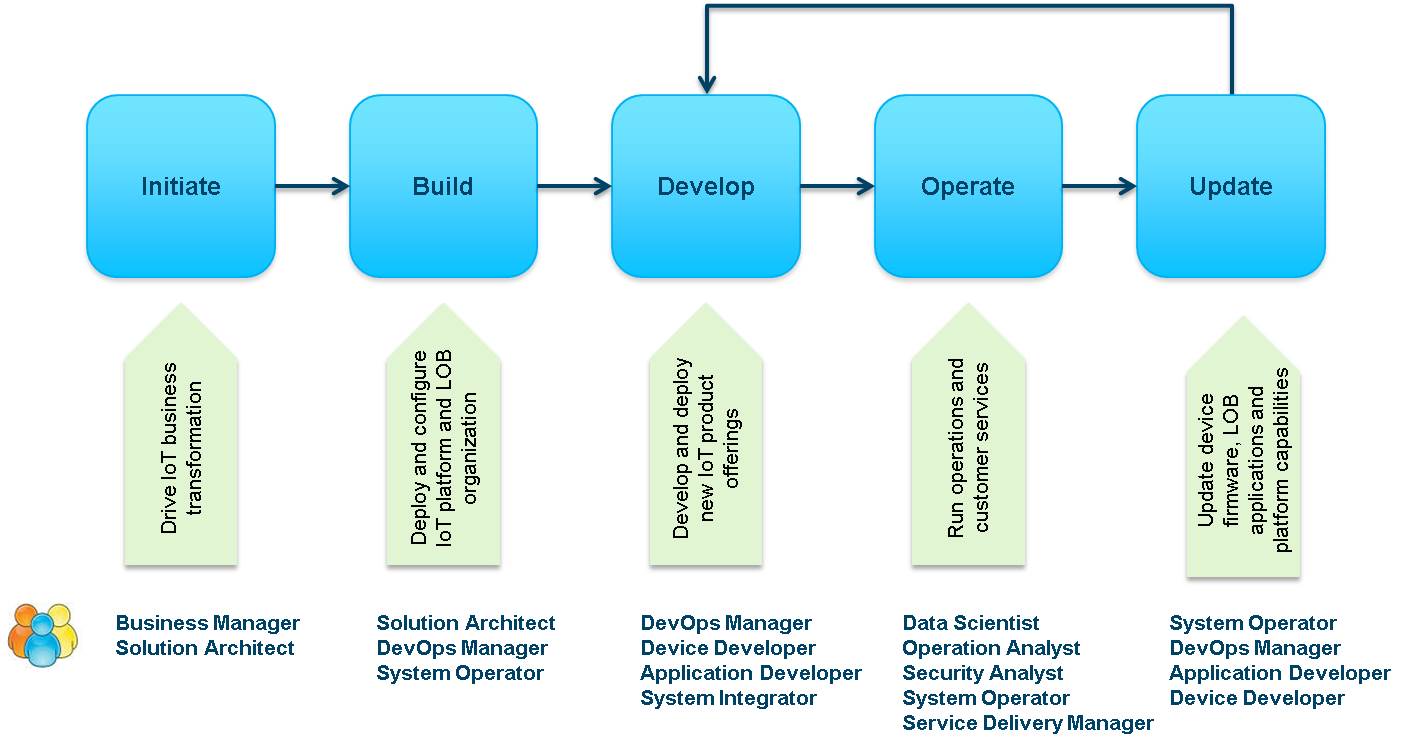


Figure 35 - Roles and Activities during the IoT product life cycle

# Annex A.

## Overall IoT infrastructure at High-level

Figure Annex-1 shows the way of combining one IoT system with 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 shown with an IoT System connecting to another IoT system, e.g., IoT System A and IoT System B and System C in Figure Annex-1.



Figure Annex-1. Integration types of one IoT system to the others.

In Figure Annex-2, an overall IoT infrastructure is presented from a system point of view. It 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 access services implemented on external, third party, systems such as banking and financial services, medical services, billing services, etc. The lines in Figure Annex-2 represent network connectivity, and the grey circles represent interoperable access points (e.g., IoT gateways).

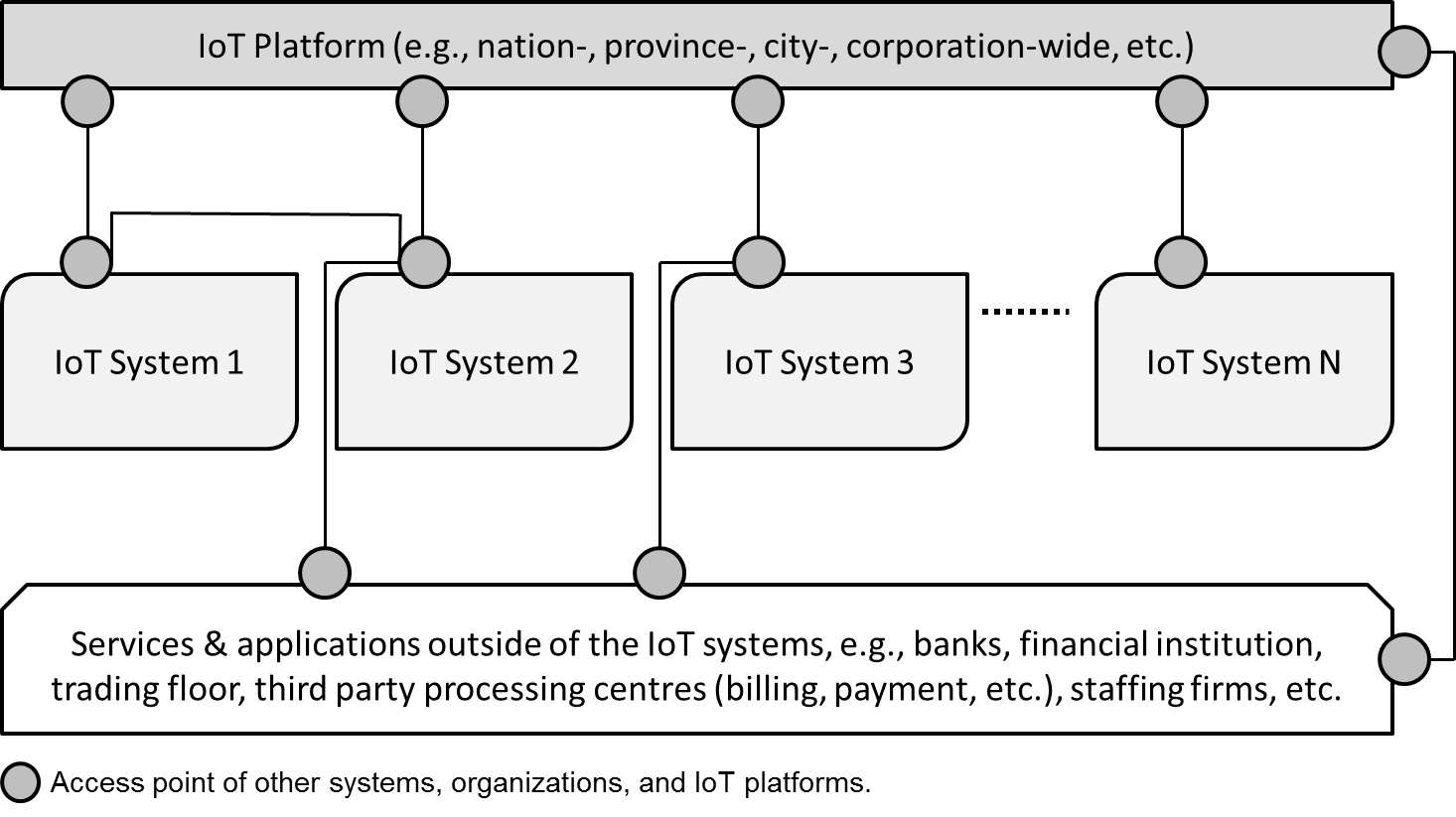


Figure Annex-2. An overall IoT Infrastructure.

1. ISO/IEC 19501:2005(en) Information technology — Open Distributed Processing — Unified Modeling Language (UML) [↑](#footnote-ref-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; andThe introduction to the IBM’s Master Data Management Reference Architecture. [↑](#footnote-ref-3)