



BSI Standards Publication

Internet of things (IoT) — Reference architecture

National foreword

This British Standard is the UK implementation of ISO/IEC 30141:2024. It supersedes BS ISO/IEC 30141:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IOT/1, Internet of Things and Digital Twin.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 20480 3
ICS 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2024.

Amendments/corrigenda issued since publication

Date	Text affected



ISO/IEC 30141

Edition 2.0 2024-08

INTERNATIONAL STANDARD



Internet of things (IoT) – Reference architecture

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020

ISBN 978-2-8322-9193-1

Warning! Make sure that you obtained this publication from an authorized distributor.

AVA Documents
Document Sharing Hub

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
0.1 General.....	7
0.2 About Internet of Things (IoT)	7
0.3 IoT sources of information.....	7
0.4 General principles of a reference architecture	8
1 Scope.....	9
2 Normative references	9
3 Terms and definitions	9
4 Abbreviated terms	9
5 IoT RA context.....	10
5.1 Overview.....	10
5.2 Stakeholders and concerns.....	11
6 IoT RA viewpoints and views	12
6.1 Overview.....	12
6.2 Foundational IoT viewpoint and views	13
6.2.1 Foundational IoT viewpoint.....	13
6.2.2 Foundational IoT view.....	13
6.3 Business viewpoint and view.....	19
6.3.1 Business viewpoint	19
6.3.2 Business view.....	19
6.4 Usage viewpoint and view.....	21
6.4.1 Usage viewpoint	21
6.4.2 Usage view.....	21
6.5 Functional viewpoint and view.....	22
6.5.1 Functional viewpoint	22
6.5.2 Functional view.....	23
6.6 Trustworthiness viewpoint and view	25
6.6.1 Trustworthiness viewpoint.....	25
6.6.2 Trustworthiness view	26
6.7 Construction viewpoint and views	29
6.7.1 Construction viewpoint.....	29
6.7.2 Construction view	31
6.7.3 IoT component pattern.....	32
Annex A (normative) Additional IoT construction patterns	38
A.1 General.....	38
A.2 Reference Architecture Model Industrie 4.0 (RAMI 4.0) pattern.....	38
A.3 Dynamic IoT system pattern.....	40
A.4 IoT enterprise system pattern.....	43
A.5 IoT enterprise networking pattern.....	45
A.6 IoT enterprise usage pattern	47
Annex B (informative) Guidance on the use of ISO/IEC/IEEE 42010:2022.....	53
B.1 Overview.....	53
B.2 Systems and architectures	53
B.3 Elements in ISO/IEC/IEEE 42010:2022 used in ISO/IEC 30141 IoT reference architecture description.....	53

B.3.1	Overview	53
B.3.2	Stakeholders, perspective, and concerns	54
B.4	Viewpoints, model kinds, legends, correspondences, and correspondence methods	55
B.5	Views and models	55
B.6	Correspondences	55
Annex C (informative)	Characteristics for IoT systems in particular contexts	56
C.1	Common characteristics	56
C.1.1	Legacy support	56
C.1.2	Network connectivity	56
C.1.3	Unique identification	56
C.1.4	Well-defined components	57
C.1.5	Auto-configuration	57
C.1.6	Content-awareness	57
C.1.7	Context-awareness	57
C.1.8	Discoverability	57
C.1.9	Manageability	58
C.1.10	Network management and operation	58
C.1.11	Real-time capability	58
C.1.12	Self-description	59
C.1.13	Service subscription	59
C.2	Characteristics related to trustworthiness	59
C.2.1	Data characteristics – volume, velocity, veracity, variability, and variety	59
C.2.2	Protection of personally identifiable information (PII)	60
C.2.3	Flexibility	60
Bibliography		61
Figure 1	– Using the IoT RA standard	8
Figure 2	– Relationship between IoT component, IoT system and IoT environment	14
Figure 3	– Example of IoT environment	16
Figure 4	– External facing functions	21
Figure 5	– Internal model of abstract function classes	23
Figure 6	– Legend used in the trustworthiness view	26
Figure 7	– IoT architecture construction view	31
Figure 8	– Capabilities of an IoT component	32
Figure A.1	– RAMI 4.0	39
Figure A.2	– DSC components	41
Figure A.3	– Message flow in DSC	42
Figure A.4	– Home smart air cleaning service	42
Figure A.5	– Example system deployment model	43
Figure A.6	– Networking model	45
Figure A.7	– Roles present when the system is in use	48
Figure A.8	– IoT service provider subroles and activities	48
Figure A.9	– IoT service developer subroles and activities	49
Figure A.10	– IoT subroles and activities	50
Figure A.11	– Activities of device and application development	50

Figure A.12 – Using device data for security-related analytics and operations.	51
Figure B.1 – Conceptual model of an architecture description	54
Table 1 – List of viewpoints, stakeholders, and concerns	11
Table 2 – Foundational IoT viewpoint.....	13
Table 3 – Business viewpoint.....	19
Table 4 – Usage viewpoint.....	21
Table 5 – Functional viewpoint.....	23
Table 6 – Trustworthiness viewpoint	26
Table 7 – Construction viewpoint	30
Table 8 – Construction pattern legend	30
Table 9 – IoT component pattern	32
Table 10 – Additional information on IoT component capabilities	33
Table 11 – Key capability transformations.....	35
Table 12 – IoT system pattern.....	36
Table A.1 – RAMI 4.0 pattern.....	38
Table A.2 – Dynamic IoT system pattern.....	40
Table A.3 – IoT enterprise system pattern.....	43
Table A.4 – IoT enterprise networking system.....	45
Table A.5 – IoT enterprise usage pattern	47
Table A.6 – Overview of activities and roles.....	51
Table A.7 – Overview of enterprise activities and roles	52

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

FOREWORD

- 1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
- 2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
- 3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this document.
- 7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
- 8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
- 9) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity, or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch> and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 30141 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

This second edition cancels and replaces the first edition published in 2018. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) conformance with ISO/IEC/IEEE 42010:2022;
- b) improved usability;
- c) implementation pattern support.

The text of this International Standard is based on the following documents:

Draft	Report on voting
JTC1-SC41/417/FDIS	JTC1-SC41/431/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, and the ISO/IEC Directives, JTC 1 Supplement available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

0.1 General

This document is the second edition of the Internet of Things reference architecture (IoT RA). This document is in conformance with ISO/IEC/IEEE 42010:2022 requirements on architecture descriptions that are described in Annex B except for aspects, perspectives, decisions and rationale.

The IoT RA addresses systems that:

- use technology for sensing and operating on physical world entities;
- have components that interact through a digital network.

The IoT RA deals with related issues, like trustworthiness functions regarding both the physical and digital worlds.

This document can be used as a generic normative part of IoT domain-specific reference architectures (DSRAs). IoT DSRAs are in conformance with ISO/IEC/IEEE 42010:2022 requirements on architecture descriptions and enable consistency and alignment with other reference architectures within ISO/IEC JTC 1.

0.2 About Internet of Things (IoT)

IoT has broad implications in industry and society today and is likely to continue to have an impact on many aspects of our lives for many years to come. Various IoT applications and services have adopted IoT techniques to provide capabilities that were not possible earlier. IoT is one of the most dynamic areas of information and communication technologies.

Fundamental to IoT are devices that interact with the physical world. Sensors collect the information about the physical world, while actuators can act upon the physical world. These field devices are connected to the digital world through network connections. Both sensors and actuators can be in many forms such as thermometers, accelerometers, video cameras, microphones, relays, heaters or industrial equipment for manufacturing or process control.

IoT is the base for new business models or offerings and new working methods in industry and in the public sector. IoT is an essential enabler for other computing areas such as digital twins, artificial intelligence, cloud computing, big data, data analysis and more. Many application areas called "smart xxx" such as smart grid, smart cities, and even smart cars use IoT as an important technology capability.

IoT can be combined with other technologies to address complex requirements. For example, IoT can leverage cloud computing, including private cloud, public cloud, hybrid cloud, and multi-cloud, for resource provisioning and management. IoT can benefit from machine learning and big data for the analysis of sensor data to enable rapid decisions for improved control and efficiency. IoT with distributed ledger technology can ensure traceability in applications. IoT can take advantage of edge computing to distribute computing resources near the convergence of information technology and operational technology, where they are needed most. The IoT area continues to grow rapidly, and new IoT application areas continue to be found and invented. This document can serve these new technology and application areas.

0.3 IoT sources of information

For a given application field and purpose, the many IoT standards, guidelines, and initiatives in existence today work well on their own and are used by various IoT stakeholders. As a result, heterogeneity is a prominent aspect of IoT. However, support for the combination and interaction of these heterogeneous resources to enable interoperability and convergence between IoT standards and guidelines is necessary.

Stakeholder decisions about both a foundation for long-term investments and durable protection of current cornerstones is more difficult because of uncertainty about resource compatibility.

This document serves as a foundation for creating interoperability and alignment between IoT initiatives. The aim of this document is to bring different views together.

0.4 General principles of a reference architecture

This document is positioned as a reference architecture for IoT systems. It utilizes the terms, definitions, and relationships for best practices in architecture descriptions as outlined in ISO/IEC/IEEE 42010:2022 to:

- establish vocabulary, principles, guidance; and
- provide a description of IoT principles, capabilities, and interactions with the physical and digital worlds.

One of the primary purposes of the IoT RA is to support architects that want to design architectures or reference architectures for IoT systems. Normative parts of the IoT RA can then be included in an architecture closer to the realization of IoT systems.

Figure 1 shows how this document has been specified and how it will be used.

- This document conforms to ISO/IEC/IEEE 42010:2022 requirements for architecture descriptions [1]¹ and uses guidelines from the "Best practices and guidelines for RA standards" standing document [2].
- Users of this document apply it to specify an IoT architecture that guides the implementation of an IoT system.

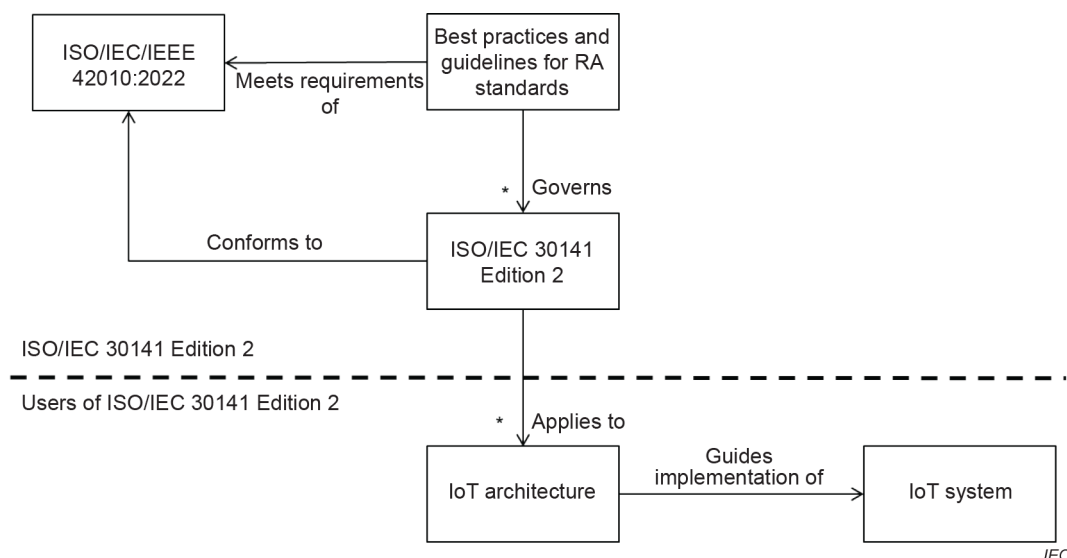


Figure 1 – Using the IoT RA standard

¹ Numbers in square brackets refer to the Bibliography.

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

1 Scope

This document specifies an Internet of Things (IoT) reference architecture (IoT RA). The IoT RA is a generalization of existing practice including the distinguishing characteristics of IoT systems and other fundamental characteristics exhibited by IoT systems. The IoT RA addresses stakeholder concerns related to the business value of IoT systems. The IoT RA also addresses the interactions between the IoT system, the users, and the physical environment. Implementation of IoT systems is also addressed in this document. Among the characteristics specified in the IoT RA are abstract functions within IoT systems and a variety of structures that are used to construct IoT systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20924, *Internet of Things (IoT) and digital twin – Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org>

4 Abbreviated terms

AI	artificial intelligence
API	application programming interface
ASD	application and service domain
BSS	business support systems
CM	conceptual model
CPS	cyber physical system
CPO	chief privacy officer
DPO	data protection officer
DSC	dynamic service composition
DSRA	domain specific reference architecture
ETL	extract, transform, load
HMI	human machine interface
HTTP	Hypertext Transfer Protocol
ICT	information and communication technologies

IoT	Internet of Things
IT	information technology
LAN	local area network
LoB	line of business
OMD	operation and management domain
OSS	operational support systems
OT	operational technology
PED	physical entity domain
PII	personally identifiable information
RA	reference architecture
RAID	resource access and interchange domain
SCD	sensing and controlling domain

5 IoT RA context

5.1 Overview

This document specifies a reference architecture for the Internet of Things using the ISO/IEC/IEEE 42010:2022 requirements for architecture descriptions. While this document is intended to be used in many situations and by many different stakeholders, the focus is on the needs of architecture developers of an IoT system description, their perspectives, concerns, and the architecture views they most likely encounter. In particular, it focuses on those involved in creating a specific IoT reference or solution architecture that depends on IoT.

This document is interesting and educational for anyone with interest in IoT. However, the document is of special interest for those people looking to:

- harmonize standards or reference architectures of other IT and OT domains with this generic IoT RA;
- develop either IoT software, or IoT hardware, or both;
- provide services involving IoT;
- procure or implement IoT systems;
- integrate IoT with other IT technology.

For all the interests mentioned above, applying parts of this document to develop or implement IoT domain-specific architecture (DSRA) is a useful approach. These descriptions can be either standalone or integrated with other IoT related architecture descriptions.

Further, depending on the interest, different sections of the document have more relevancy. While some parts provide an overview, some parts provide more information regarding different aspects of IoT.

This document can also be used as normative reference in a DSRA. The document can then serve as a base for the IoT part of that DSRA, leaving application concerns, use cases and so forth to the DSRA. The DSRA can specify how the IoT RA is intended to be used for the specific domain. A DSRA can also specify conformance to parts of this document.

This document conforms to ISO/IEC/IEEE 42010:2022 requirements on architecture descriptions [1], which is described in Annex B. This ensures that the IoT RA aligns with other RAs that conform to ISO/IEC/IEEE 42010:2022 requirements on architecture descriptions. The IoT RA is intended to be used with one or more architecture description frameworks (in accordance with ISO/IEC/IEEE 42010:2022) to create an architecture description for a system of interest.

ISO/IEC/IEEE 42010:2022 provides terms, definitions, and relationships for best practices in architecture descriptions of the architecture of a system of interest. Consequently, all conforming architecture descriptions can be interpreted in a consistent way. Conformance to ISO/IEC/IEEE 42010:2022 requirements for architecture descriptions makes this document a vital part of a cohesive family of standards, including those standards dealing with interoperability.

5.2 Stakeholders and concerns

Table 1 shows a list of viewpoints, stakeholders, and concerns.

Table 1 – List of viewpoints, stakeholders, and concerns

Viewpoint	Stakeholders	Concerns
Foundational IoT viewpoint	– Architect – Project manager – Programme manager – Standards expert – People concerned with the fundamentals of IoT – Domain experts – Business manager – System owner	What is IoT? What are the essential characteristics of IoT systems? What is new (and different) about the concept of IoT? Is a given system or component an IoT system or component? What are the implications of the concept of IoT?
Business viewpoint	– Business manager – System owner – Architect	How to leverage the various capabilities of an IoT system to provide value for a business? How to use IoT for innovative new business models? How do characteristics of an IoT system influence business and system owner?
Usage viewpoint	– System architect – Project manager	How do users (both human and digital) interact with the IoT system? How does the IoT system interact with the physical entity of interest?
Functional viewpoint	– Architect – Project manager – Programme manager – IoT standards expert – Business manager – System owner	What are the types of abstract functions that need to be implemented in an IoT system?
Trustworthiness viewpoint	– System architect – Security engineer – Security manager – Privacy manager – Project manager – Business manager	How to design an IoT system with a level of confidence that meets trustworthiness goals. How to assure the implemented system meets design goals.
Construction viewpoint	– System architect – Project manager – System designer	What types of design are useful when creating an IoT system to meet a given set of requirements? What types of design are useful when creating an IoT component to meet a given set of requirements?

6 IoT RA viewpoints and views

6.1 Overview

The essence of an architecture description lies in the architecture views that it provides. Each view is governed by a corresponding viewpoint. The developers and professional practitioners who are charged with elaboration of the architecture description can adopt the architecture views provided in this document. The different architecture views result from modelling and narrative descriptive activities of the architecting effort.

An architecture viewpoint states relevant information focusing on a particular topic. This information is a collection of concerns, often expressed in use cases, stakeholders provide about the constructed artefacts that they believe are important to the topic. Viewpoints specify the architecture view or views it governs. The architecture viewpoint also identifies modelling or narrative paradigms for generating the architecture view or views.

This document specifies six architecture views and their governing viewpoints:

- an IoT foundational viewpoint in 6.2;
- a business viewpoint in 6.3;
- a usage viewpoint in 6.4;
- a functional viewpoint in 6.5;
- a trustworthiness viewpoint in 6.6;
- a construction viewpoint in 6.7.

Subclause 6.2 presents the foundational IoT viewpoint and the corresponding view which frames the concerns related to the essential characteristics of IoT. The viewpoint addresses concerns related to the fundamental aspects of IoT by specifying the foundational building blocks of IoT enabled systems as architecture views. These views represent the different concepts related to IoT (for example: principles, devices, and connectivity).

Subclause 6.3 presents the business viewpoint and the corresponding view.

Subclause 6.4 presents the usage viewpoint and the corresponding view.

Subclause 6.5 presents the functional viewpoint and the corresponding functional views that describe the IoT reference architecture from the perspective of key functions. The viewpoint addresses concerns related to the fundamental functional aspects of IoT by specifying the foundational building blocks of IoT enabled systems as architecture views. These views represent the functional capabilities of IoT related data, management, communication, interfaces, etc.

Subclause 6.6 presents the trustworthiness viewpoint and provides means for implementing a trust model to consider when creating an IoT product or solution.

Subclause 6.7 presents the construction viewpoint and the corresponding construction views that describe the IoT reference architecture from the perspective of implementation architectures. The viewpoint addresses concerns related to the fundamental implementation aspects of IoT by specifying the different patterns as architecture views. Examples of patterns described in this document include the IoT component capability, the RAMI4.0, the IoT user, the IoT enterprise system, the enterprise networking, and the IoT enterprise usage patterns.

6.2 Foundational IoT viewpoint and views

6.2.1 Foundational IoT viewpoint

The foundational IoT viewpoint is essential to the IoT domain. It frames multiple concerns of several stakeholders, described below. The foundational IoT viewpoint is described in Table 2.

Table 2 – Foundational IoT viewpoint

Viewpoint name		Foundational IoT
Overview		Framing of the concerns related to the essential characteristics of IoT
Known typical stakeholders		– Architect – Project manager – Programme manager – Standards expert – People concerned with the fundamentals of IoT – Domain experts – Business managers – System owners
Concerns		– What is IoT? – What are the essential characteristics of IoT systems? – What is new (and different) about the concept of IoT? – Is a given system or component an IoT system or component? – What are the implications of the concept of IoT?
Viewpoint specification	Model kinds	Interoperability model Component model
	Legends	The foundational IoT view provides text defining the essential characteristics of IoT, text describing the concepts and relationships between an IoT component, IoT system, and IoT environment.
	View methods	NA
	Correspondence methods	NA
	References	NA

6.2.2 Foundational IoT view

6.2.2.1 Description of IoT systems

ISO/IEC 20924 [3] defines IoT as an "infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world".

In practical terms, this IoT definition can be distilled down to two essential characteristics of IoT systems.

- a) An IoT system is composed of components connected through a many-to-many digital network. The network capabilities can be based on different options such as using a many-to-many relationship or others and using approaches such as TCP/IP or alternatives.
- b) At least one of those system components interacts with the physical world through either sensing or actuating.

The interaction with the physical world includes:

- Sensing: a sensing capability (provided by a sensor) offers ability to provide observations of an aspect of the physical world as measurement data. Information from sensor observations can be provided to other IoT components through the network interface of the component for processing and storage.

EXAMPLE 1 Temperature sensing (temperature measurement capability), computerized tomography (CT) scans (radiographic imaging), spatial sensing (accelerometers, gyroscopes), optical sensing, and audio sensing.

- Actuating: an actuating capability, provided by an actuator, offers the ability to change the physical world. Such change is based on information that is given as input to the component.

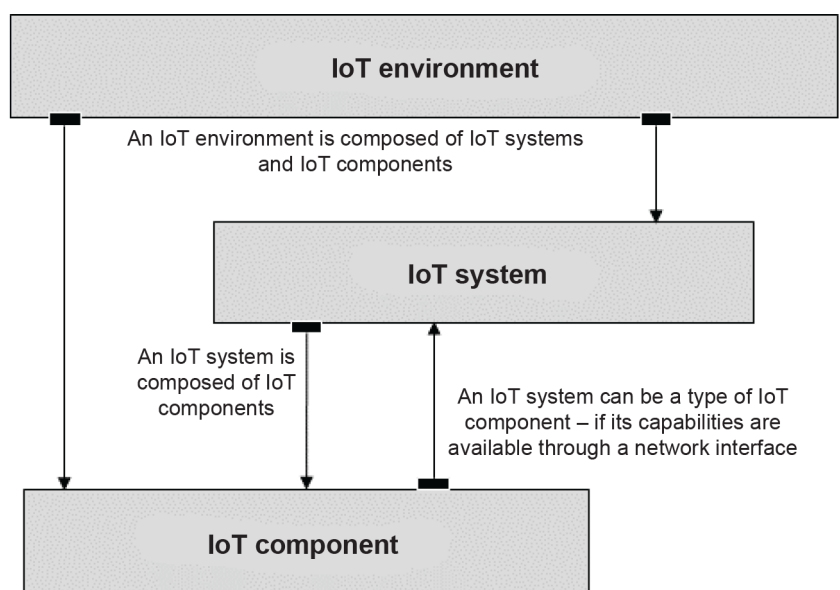
EXAMPLE 2 Heating coils (heating capability), electric shock delivery (cardiac pacing), electronic door locks (lock/unlock capability), unmanned aerial vehicle operation (remote control), servo motors (motion/movement capability), and robotic arms (complex motion/movement capability).

6.2.2.2 IoT system concepts

6.2.2.2.1 General

IoT can be broken down into three important concepts (Figure 2):

- the IoT environment (containing all the components, systems, and related infrastructure);
- the IoT system that provides benefit to the stakeholders;
- the IoT components that interact together to form the IoT system.



IEC

Figure 2 – Relationship between IoT component, IoT system and IoT environment

6.2.2.2.2 IoT components

IoT components are the basic building blocks of IoT systems. IoT components interact with other IoT components to form a system and achieve one or more goals. Each IoT component provides some function that is necessary within the system so it can achieve its goal or goals.

All IoT components have at least one network interface that provides the ability to participate in a many-to-many network. Nevertheless, a given IoT component does not need to communicate with more than one other IoT component in a given system (e.g. assigning and limiting communication between two static IPs). Most IoT components also have an application interface that provides the capacity for application-level interactions between IoT components.

Each IoT component offers one or more IoT capabilities for use by other IoT components. Network interfaces and sensing are two examples of IoT capabilities.

6.2.2.2.3 IoT systems

A system, which is a combination of interacting elements organized to achieve one or more stated purposes, is considered an IoT system when it is composed of networked IoT components. The IoT system also interacts with a physical entity of interest through a sensor or an actuator within the IoT components. IoT systems differ from conventional IT systems in their ability to directly interact with the physical world.

IoT systems range from the very simple, such as an Internet-enabled thermometer, to the extremely complex, such as a city management system, and everything in between. IoT components can be assembled into many different systems. Also, a single IoT component can have the ability to be part of more than one system at a time. An IoT system can also act as an IoT component within another IoT system, if it has a network interface that allows it to be used that way. An IoT system is not necessarily constructed in a particular manner.

The quality of "goodness" is how well requirements of stakeholders are met. Many of the characteristics of an IoT system have lower or higher importance depending on the specific use cases and therefore indirectly stakeholder concerns.

An IoT system is not required to meet specific security, privacy, reliability, cost, or functional requirements to be considered an IoT system. Even if these criteria are not met it does not stop being an IoT system. However, if the IoT system cannot meet the use case requirements, it might not be a "good" IoT system for a specific use case. In other words, "goodness" is purely in the eyes of the user.

6.2.2.2.4 IoT environments

A digital IoT environment includes:

- the set of IoT components available to be composed into IoT systems;
- the networks connecting the components;
- any associated services that provide the mechanisms for discovery, composition, and orchestration.

Although an IoT environment contains the IoT components that can be used to create IoT systems, it does not necessarily contain any functioning IoT systems. This can be the case if no IoT components have been instructed to interact as a system. The opposite is also true. An IoT environment can be used to create non-IoT systems (conventional IT systems) by excluding IoT components that have sensing or actuating capabilities. In its current state, the Internet can be considered an IoT environment.

For system owners and business managers, it is often relevant to consider the IoT environment as a part of the overall IT environment of an organization.

IoT systems can be components of other IoT systems. IoT systems can also be components of other IT systems. IT systems can be (and often are) components of IoT systems.

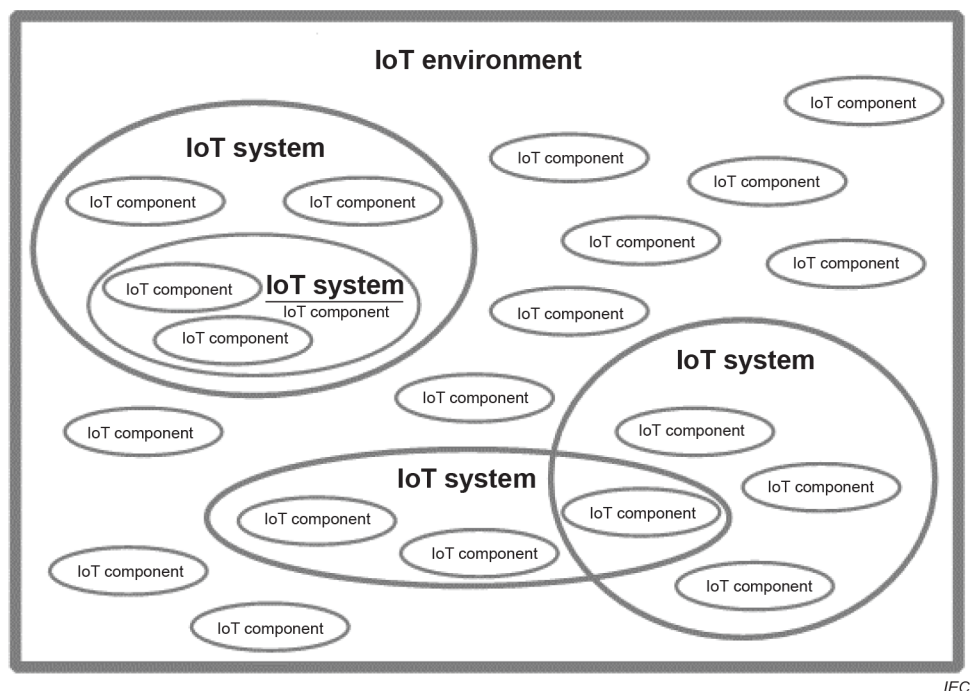


Figure 3 – Example of IoT environment

Figure 3 shows an example of IoT environment with systems, components, and system of systems.

IoT components that are not part of a specified IoT system are nonetheless interconnected in the IoT environment and can become part of an IoT system.

6.2.2.3 Emergent characteristics

6.2.2.3.1 General

The characteristics inherent to IoT are described in 6.2.2.3.2 to 6.2.2.3.10.

NOTE Other characteristics that can be useful to build IoT systems in particular contexts are listed in Annex C.

6.2.2.3.2 Composability

Composability is the ability to combine discrete IoT components into an IoT system to achieve a set of goals and objectives. Composability and interoperability might be important to avoid lock in effects to one or a few IoT suppliers. Especially in the fast-growing IoT area, this might be even more important to meet expected delivery agreements with customers. When the customer demands exceed production capacities, an organization might need to have back up plans for how to upgrade or replace failing equipment.

6.2.2.3.3 Functional and management capability separation

Separation of functional and management capabilities means that the functional interfaces and capabilities of an IoT component, such as an IoT device, are cleanly separated from the management interfaces and capabilities of that component.

It is often wanted to qualify in an early stage the different kinds of users that need to interact with different parts of the IoT system and how. Such qualification makes the separation need more precise and specific. Since the IoT system often consists of components that are widely dispersed geographically, this might be of extra concern regarding remote access. Furthermore, IoT equipment is often equipped with physical interfaces (possibility to interact with the device itself, hands on). Such interfaces might provide challenges if and when such equipment is exposed to the public or nonauthorized users. Furthermore, such devices might be installed in places or areas without possibility to monitor the devices and by whom they are accessed.

6.2.2.3.4 Heterogeneity

IoT is typically cross-system, cross-product, and cross-domain. This often requires interoperability between heterogeneous components and systems. The degree to which heterogeneity is considered is often a matter of the protocols and communication needed for a product at different stages of the lifetime of the IoT system. The degree of heterogeneity for components and physical entities often drives cost and it is important that it is balanced compared with the business needs.

6.2.2.3.5 Highly distributed systems

IoT environments are often built by highly distributed systems which, while being functionally integrated, consist of sub-systems that can be physically separated and remotely located from one another. As an example, IoT systems can span whole buildings, whole cities and even the globe. Data can be stored at the edge of the network, centrally, or both. Distribution can also apply to processing – some processing taking place centrally or in the edge of the network, in IoT gateways or within more capable types of sensors and actuators.

It is important to consider the degree of distribution for the IoT system since most IoT systems are highly distributed by nature. Measurements often need to be taken to ensure the distributed components of such an IoT system can be handled remotely. This is needed for the component to be maintained, debugged, and upgraded and so on. Also, a high distribution might put constraint on trustworthiness characteristics of the system.

6.2.2.3.6 Modularity

Modularity is about how components can be removed cleanly from a system and replaced with another module of similar size and with similar physical and logical interfaces.

The modularity for an IoT system does not differ from the wanted modularity of any IT system. Nevertheless, it might be worth considering that IoT is a fast-growing technology. This makes it even more important to be able to upgrade separate parts of the IoT system continually; thus, placing even higher demands on the wanted degree of modularity. Modularity is also closely related to the composability characteristics of the system.

6.2.2.3.7 Network communication

IoT systems make use of a broad variety of network types. These can be limited range, low power networks collectively termed proximity networks that form the local connections for IoT devices. They can also be wide area networks that connect the proximity networks to the Internet. Gateways can be employed to connect networks of different types, typically between the proximity networks and the wide area.

The choice of communication protocols and network technology might be crucial to the business case and the life span of the IoT system. The choice of network technology also relates to the wanted scalability capability and data capabilities of the IoT system. Most communication protocols and network technologies often have both strengths and limitations. For crucial IoT applications the data characteristics of the chosen network technology are important.

Especially before investing in large scale implementation of sensors, it might be important to consider if the chosen network connectivity will be appropriate for the lifetime of the sensors.

It can also be beneficial to aggregate or in other ways reduce the amount of data transferred through the network.

6.2.2.3.8 Scalability

Since the number of connected entities in an IoT system often grows very quickly, it is of utmost importance that an IoT system is built to scale and to be able to handle a very large number of IoT devices as well as massive amounts of incoming data.

Furthermore, it is important for the user interface of an IoT system to consider how to display and sort information about millions of IoT devices, their data, and their metadata. The same goes for displaying a large number of rules and similar additional information.

Business managers might also want to take into consideration that deploying millions of IoT devices often will be at a large cost. Thus, the time it takes to deploy each IoT device and the possibility to mass deploy many IoT devices at the same time will have a large impact on the overall cost over time for the IoT investment as such.

When there is a risk of high load in incoming data it can be desirable to provide a means to prioritize incoming critical application sensor data.

New IoT actors sometimes can be at a developing stage where they primarily are working with demonstration and test data. It can be wise to carry out load tests with new IoT systems where the entire system is forced to handle a very large number of sensors simultaneously, be it real sensors or simulated.

6.2.2.3.9 Shareability

Many IoT components are underutilized since a single system often uses only a fraction of the capabilities of a component. If functionality or outputs of components can be shared among multiple systems, resources can be used more efficiently.

Determining shareability possibilities is often a good way to boost business opportunities for IoT components. At the same time business managers and system owners must ensure that a specific IoT component also meets the regulatory requirements. Especially for such other usage that differs from the primary intended functionality of that component.

6.2.2.3.10 Accuracy

Accuracy is a characteristic of various elements in an IoT system: Sensors make measurements on properties of the physical world. Accuracy of these sensors is the closeness of agreement between the measured values and the actual values of those properties. The usage of the data produced by the measurement is often highly dependent on the level of accuracy of the sensors as well as those computational algorithms used to manage the data. Actuators operating on the physical world translate digital commands into actions. The accuracy of such actions is also dependent on the accuracy of the provided data and the actuator itself.

It is often important to carefully decide what accuracy is needed for a specific business purpose. Often higher accuracy comes with a higher cost. IoT systems often consist of many components. Because of this, the impact on costs of choosing a component with higher accuracy than needed can result in unnecessary higher overall costs for the IoT system.

One thing to consider regarding accuracy is to what extent the surrounding environment might influence the accuracy. For example, a sensor measuring distance might be influenced by the air temperature or the temperature of the sensors, losing accuracy in high temperatures.