ISO/IEC 21823-1

Edition 1.0 2019-02

INTERNATIONAL STANDARD

colour inside

Internet of things (IoT) – Interoperability for iot systems – Part 1: Framework

ISO/IEC 21823-1:2019-02(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

ISO/IEC 21823-1

Edition 1.0 2019-02

INTERNATIONAL STANDARD

Internet of things (IoT) – Interoperability for iot systems – Part 1: Framework

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.020

ISBN 978-2-8322-6567-3

CONTENTS

INTERNET OF THINGS (IoT) – INTEROPERABILITY FOR IoT SYSTEMS –

Part 1: Framework

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or 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 National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC 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 publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 21823-1 was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 21823 series, under the general title *Information technology – Internet of Things (IoT) – Interoperability for IoT systems*, can be found on the IEC and ISO websites.

The text of this standard is based on the following documents:

FDIS	Report on voting
JTC1-SC41/75/FDIS	JTC1-SC41/87/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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

Internet of Things (IoT) systems involve communications between different entities. This applies to connections between different IoT systems. It also applies to the many connections that exist within IoT systems. The various entities and their connections are described in ISO/IEC 30141.

The ISO/IEC 21823 series addresses issues that relate to interoperability of the communications between IoT systems entities. ISO/IEC 21823-1 describes a general framework for interoperability of IoT systems. This includes a facet model for interoperability which includes five facets of interoperability (i.e. transport, syntactic, semantic, behavioural and policy). This document addresses the framework to achieve interoperability for IoT; the specific facets are addressed in other parts of ISO/IEC 21823.

INTERNET OF THINGS (IoT) – INTEROPERABILITY FOR IoT SYSTEMS –

Part 1: Framework

1 Scope

This document provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems.

This document ensures that all parties involved in building and using IoT systems have a common understanding of interoperability as it applies to IoT systems and the various entities within them.

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 30141, *Internet of Things (IoT) – Reference architecture*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

3.1
interface
named set of operations that characterize the behaviour of an entity

[SOURCE: ISO 19142:2010, 4.10]

3.2
operation
specification of a transformation or query that an object may be called to execute

[SOURCE: ISO 19142:2010, 4.17]

3.3
framework
structure of processes and specifications designed to support the accomplishment of a specific task

[SOURCE: ISO/IEEE 11073-10201:2004, 3.22]

3.4
interoperability
ability for two or more systems or applications to exchange information and to mutually use the information that has been exchanged

[SOURCE: ISO/IEC 17788:2014, 3.1.5]

3.5
transport interoperability
interoperability (3.4) where information exchange uses an established communication infrastructure between the participating systems

Note 1 to entry: System means IoT system.

Note 2 to entry: IoT device, IoT gateway, sensor and actuator are considered as a system.

[SOURCE: ISO/IEC 19941:2017, 3.1.3]

3.6
syntactic interoperability
interoperability (3.4) such that the formats of the exchanged information can be understood by the participating systems

Note 1 to entry: System means IoT system.

Note 2 to entry: IoT device, IoT gateway, sensor and actuator are considered as a system.

[SOURCE: ISO/IEC 19941:2017, 3.1.4

3.7
behavioural interoperability
interoperability (3.4) so that the actual result achieves the expected outcome

Note 1 to entry: System means IoT system.

Note 2 to entry: IoT device, IoT gateway, sensor and actuator are considered as a system.

[SOURCE: ISO/IEC 19941:2017, 3.1.6, modified – In the definition, "result of the exchange" has been replaced with "result".]

3.8
policy interoperability
interoperability (3.4) while complying with the legal, organizational, and policy frameworks applicable to the participating systems

Note 1 to entry: System means IoT system.

Note 2 to entry: IoT device, IoT gateway, sensor and actuator are considered as a system.

[SOURCE: ISO/IEC 19941:2017, 3.1.7]

3.9
semantic interoperability
interoperability (3.4) so that the meaning of the data model within the context of a subject area is understood by the participating systems

Note 1 to entry: System means IoT system.

Note 2 to entry: IoT device, IoT gateway, sensor and actuator are considered as a system.

[SOURCE: ISO/IEC 19941:2017, 3.1.5, modified – The term "semantic data interoperability" has been replaced with "semantic interoperability".]

4 Abbreviated terms

AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ASD	Application & Service Domain
IoT	Internet of Things
JSON	JavaScript Object Notation
MQTT	Message Queuing Telemetry Transport
OMD	Operation & Management Domain
PII	Personally Identifiable Information
RAID	Resource Access & Interchange Domain
SCD	Sensing & Controlling Domain
UD	User Domain
PED	Physical Entity Domain

5 Overview of Internet of Things interoperability

5.1 Descriptions

Clause 5 provides an overview and facet models for Internet of Things interoperability. The goal is to ensure that parties involved in the IoT, particularly as specified in ISO/IEC 30141, have a common understanding of IoT interoperability for their specific needs. This common understanding helps to achieve interoperability in IoT by establishing common terminology and concepts used to describe it, particularly as they relate to IoT entities.

5.2 Considerations for Internet of Things interoperability

Interoperability can be defined as a measure of the degree to which various kinds of systems or components interact successfully. For the purposes of this document, interoperability is defined in 3.4. In the context of IoT, interoperability is further described as the successful interaction among the IoT entities specified in ISO/IEC 30141.

Interoperability, in the context of IoT, involves a number of different types of interacting entities and their associated interfaces. While interoperability matters in sectors throughout the economy, this document specifically focuses on the context of IoT and especially relating to the framework for interoperability based on the IoT reference architecture defined in ISO/IEC 30141.

There are many considerations when addressing IoT interoperability. These include:

- ability for communication between entities in different domains or between different IoT systems;
- ability for the exchange of data between entities in different domains or between different IoT systems;
- ability of an understanding of the meaning of exchanged data between entities in different domains or different IoT systems;
- ability for an IoT service to work with other IoT services;
- roles and activities of functional components as defined in ISO/IEC 30141 for interoperability.

By taking these considerations into account, this document provides a context of framework for a better understanding of existing and future interoperability standards.

5.3 Internet of Things interoperability facet model

5.3.1 General

Interoperability involves a number of elements, starting at the simple exchange of data bytes, facilitating an understanding of the semantics of the exchanged information, and also an alignment of the business processes, behaviour and policies on either side of the exchange. Semantic, behavioural and policy interoperability can result in a significantly bigger challenge than the bits and bytes. [1][1]

In dealing with the various interactions to which interoperability applies in IoT, it is necessary to explore technological, information and human aspects. Moving forward, interoperability related challenges are likely to intensify and get more difficult to manage as IoT systems grow more complex and interconnected. In IoT systems where anything can be connected, the complexities are further extended from technological aspects to global policies, regulation and international law.

To discuss interoperability within the context of IoT, it is necessary to deal with different perspectives of conceptual interoperability and identify with whom, with what, and circumstances in which interoperability plays a vital role. This document describes these various aspects of interoperability in terms of facets. Interoperability of two entities may be described in terms of different facets, where each facet focuses on one aspect of interoperability. To achieve interoperability, it is important that all facets are understood and mutually agreed upon by interacting entities.

The interoperability facet model described in this document defines five facets within the context of IoT interoperability. These five facets, shown in Figure 1, are transport, syntactic, semantic, behavioural and policy. This model is derived by combining and abstracting the European Interoperability Framework [2] and the Levels of Conceptual Interoperability Model (LCIM) [3].

[1] Numbers in square brackets refer to the Bibliography.

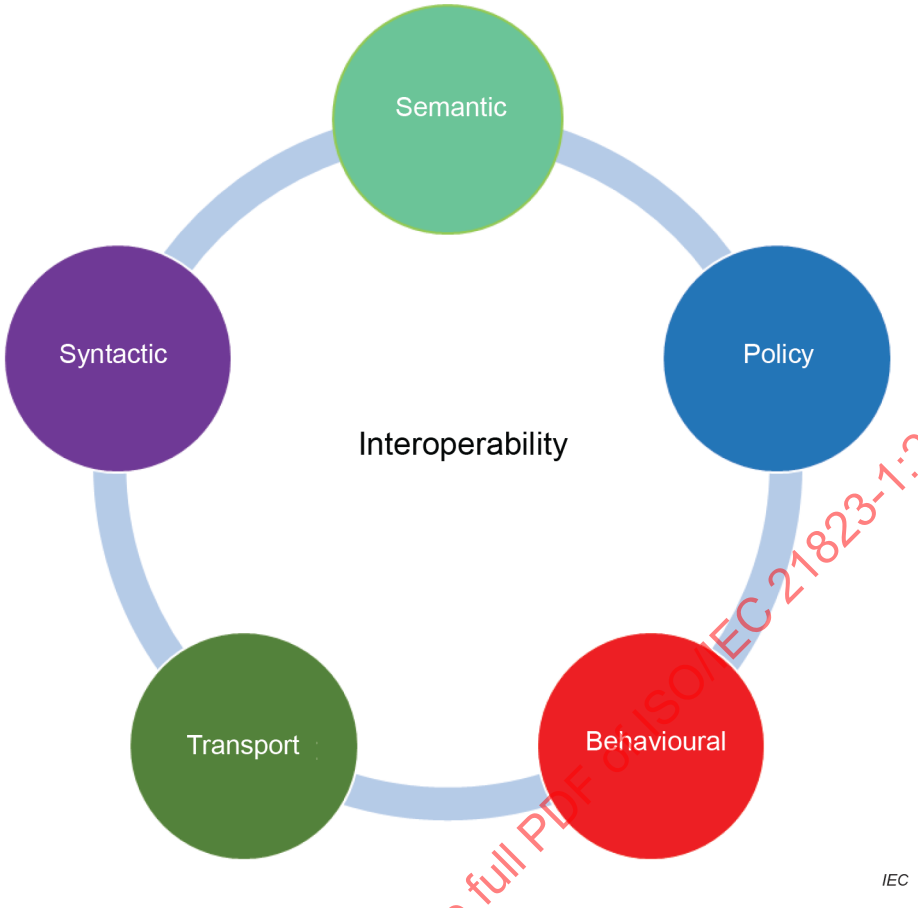

Figure 1 – Facets of IoT interoperability

In Figure 1, the big circle indicates that interoperability has five facets and that they have some effect on each other. This model was originally produced in ISO/IEC 19941 [1] and is adapted to "Internet of Things" to achieve synergy with the system integration viewpoint in ICT.

5.3.2 Transport interoperability

The transport interoperability is the commonality of the communication infrastructure established to exchange data between entities. It includes the physical medium used (e.g. wired, wireless) and the transport mechanism between various entities of an IoT system or between different IoT systems defined as entity-based reference model in ISO/IEC 30141. Examples include IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi®[2]) for the physical layer and protocols such as TCP/IP, HTTP/S, AMQP (as specified in ISO/IEC 19464 [4]) and MQTT (as specified in ISO/IEC 20922 [5]).

5.3.3 Syntactic interoperability

The syntactic interoperability is the ability of two or more systems or devices to exchange information based on their syntaxes such as formats, rules, etc. Example syntaxes for information include OWL (Web Ontology Language), RDFS (Resource Description Framework Schema), UML (Unified Modelling Language), XML (eXtensible Markup Language), JSON (as specified in ISO/IEC 21778 [6]), ASN.1 (as specified in the ISO/IEC 8824 series [7]), etc.

2 Wi-Fi is a registered trademark of Wi-Fi Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

5.3.4 Semantic interoperability

The semantic interoperability is the ability of the entities exchanging information to understand the meaning of the data model within the context of a subject area. Domain concepts in an IoT system are varied and dependent on the nature of the entities concerned.

Semantic interoperability is based on the data models of the information being exchanged at the time of that exchange. The data models depend on the nature of the entities involved and the functional capabilities of the interfaces between them.

5.3.5 Behavioural interoperability

The behavioural interoperability is where the results of the use of the exchanged information match the expected outcome. IoT entities are designed for a particular purpose or intention. However, the actual use of the entity by another entity may have a different intention without violating the other facets of interoperability.

The behavioural interoperability of an IoT entity is defined in the interface description. The interface description includes a declaration of the interface provided by the service, often referred to as an API. The interface declaration describes the interface in terms of a set of operations provided by the interface and the inputs and outputs for each operation. In terms of the interface description, behavioural interoperability requires additional information to be supplied in terms of the expected results of each operation, including elements such as pre-conditions, post-conditions and any sequences of operations that are necessary for successful use of the interface. The behavioural interoperability facet abstracts from implementation details and describes the behaviour of IoT entities in a representation-independent way.

The behavioural interoperability can be particularly important where a particular entity (say an actuator) is replaced with a new version offering the same interface – while the semantic and syntactic elements of the interface can match, the behaviour might be different, producing unexpected results.

5.3.6 Policy interoperability

The policy interoperability is defined as the ability of two or more systems to interoperate within the legal, organizational, and policy frameworks applicable to the participating systems.

This facet concerns governmental laws and regulations, policy terms and conditions applying to the IoT user or IoT system provider, and organizational policies covering the interactions.

5.3.7 Summary of Internet of Things interoperability facet model

See Table 1.

Table 1 – Summary of different facets of IoT interoperability [1]

Facets	Aim	Objects	Requirements	Examples
Transport	Data transfer between systems	Physical connections Signals	Protocols of data transfer	HTTP/S, MQTT
Syntactic	Receive data in an understood format	Data	Standardized data exchange formats	JSON, XML, ASN.1
Semantic	Receive data using an understood data information model	Programmatic interface	Common interpretation of data information model	Directories, data keys, ontologies
Behavioural	Obtain expected outcomes to interface operations	Information	Behavioural model(s) of the invoked IoT entity	UML models, pre- and post-conditions, constraint specifications
Policy	Assurance that interoperating systems follow applicable regulatory and organizational policies	Regulatory and organizational polices and interoperation context	Conditions and control for use and access	Security policies of IoT system stakeholders, restriction on cross-border data transfer, regulations controlling PII

5.4 Issues affecting Internet of Things interoperability

One of the important aspects of IoT interoperability is the mutual understanding of the semantic and behavioural facets which express concepts from a domain of interest.

Challenges related to the semantics of data, the intended use and the organizational realities of people and processes, and the constraints of legal or regulatory frameworks tend to be far more difficult to address. For example, transport interoperability can make it possible to deliver data from one system to another, but political or regulatory restrictions may make the data practically unavailable. A lack of agreement on governance structures may impose legal risks that prevent the sharing of that data [1].

Full interoperability between two interacting systems requires that interoperability exists for all interoperability facets. However, practically speaking, two systems can still interact successfully even if interoperability is not achievable for all facets. For example, for the transport interoperability facet, one system might communicate using a REST HTTP protocol while another system might communicate using the MQTT protocol. Interoperability for the transport facet may still be achievable by using a protocol adapter, such as an Enterprise Service Bus (ESB) [1].

Similarly, if the two systems differ in relation to the syntactic interoperability facet, it may be possible to enable them to interoperate using a syntax translator – an example is a syntax mapping between data encoded in XML and data encoded in JSON [1].

However, systems that differ in data semantics pose significant issues for interoperability. If two systems have different types of data artefacts or the meaning of the data artefacts differs between the systems, it may be the case that data from one system has no meaning or is unusable by the other system. In addition, it might not be possible to create semantic adapters to enable the two systems to connect meaningfully. It might be possible to create metadata or semantic mappings to provide a form (full or partial) of semantic equivalency [1].

The processes or activities of the interacting entities are required to achieve successful behavioural interoperability. The target entity cannot provide the features and functionalities expected by the source entity without them. Lack of behavioural interoperability between two systems can be a very significant barrier to enable full interoperability between them. The

implication is that the actual behaviour of one system does not match the expectations of the other system, even if the functional interface (or API) matches between the systems. It might be possible to create some form of behavioural adapter to deal with the behavioural differences, but this can be a significant challenge for more complex behavioural mismatches.

Policy interoperability can be one of the most challenging and difficult to achieve if there are mismatches between the interacting entities. If there is a legal prohibition on an IoT service connecting to an IoT device because the service runs in a different jurisdiction to the device, for example, then it is not possible for an IoT service to use that device even if all the other facets of interoperability are satisfied. IoT service provider policies concerning data placement (e.g. for sensitive data) can also be a significant barrier to policy interoperability. In some cases, it may be possible to address the policy interoperability issues by reconfiguring the IoT system or modifying the placement of entities in the IoT system.

In order to meet the requirements for interoperability, the requirement is that the processes or activities of entities of IoT systems are matched and fully aligned with the processes or activities of other entities of the same IoT system or of other IoT systems.

6 Consideration of the interoperability requirement for IoT characteristics

6.1 General descriptions

It is necessary to analyse the characteristics of IoT systems which should be considered for the support of interoperability. Clause 6 classifies the characteristics of IoT systems defined in ISO/IEC 30141 in terms of interoperability. In Clause 6, only the characteristics defined in ISO/IEC 30141 that affect interoperability are described. These characteristics are mainly focused on semantic, behavioural, and policy facets.

6.2 IoT system characteristics

6.2.1 Network communication

From a network communication point of view, two IoT entities are interoperable when they use the same communication infrastructure. This includes both the physical medium and the transport protocol used. Network communication is mainly focused on the transport facet.

Where the physical medium does not match for the two entities, network intermediary devices can be used to enable communication, such as routers and gateways. Where the protocol does not match between the two entities, a protocol translator can be used to enable communication between the two entities.

6.2.2 Self-description

To enable communication with an IoT entity from other IoT entities, self-description of a number of elements is necessary. Self-description is mainly focused on the syntactic facet.

The elements include:

- interface definition(s);
- network description (type of network, endpoint identifiers);
- security capabilities and parameters;
- entity metadata including entity type, capabilities description, constraints.

6.2.3 Other IoT system characteristics not considered in interoperability

This document does not consider the following IoT system characteristics for interoperability:

- network management and operation.

These characteristics are mainly focused on semantic, behavioural, and policy facets.

6.3 IoT component characteristics

6.3.1 Discoverability

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. Therefore, discovery should be considered to discover information provided by self-description stated in 6.2.2.

6.3.2 Network connectivity

In order to support network communication interoperability stated in 6.2.1, network connectivity should be described as self-description such as the communication protocol stated in 6.2.2.

6.3.3 Unique identification

Unique identification is very important to make one IoT system interoperable with other IoT systems. For unique identification, several types of unique identifier will be used.

6.3.4 Other IoT component characteristics not considered in interoperability

This document does not consider the following IoT component characteristics for interoperability:

- composability;
- modularity;
- shareability.

6.4 Legacy support

A support for service, protocol, device, system, component, technology, or standard that is outdated but which is still in current use may be needed for interoperability with backward compatibility.

6.5 Security

6.5.1 Confidentiality

Confidentiality should be guaranteed between two interoperating IoT systems.

6.5.2 Integrity

Data integrity should be guaranteed between two interoperating IoT systems.

6.5.3 Protection of personally identifiable information

Protection of Personally Identifiable Information should be guaranteed over two interoperating IoT systems. Confidentiality may impact the behavioural and policy facets.

6.6 Heterogeneity

Heterogeneity of IoT systems indicates that they may have different interfaces with each other. Heterogeneous IoT systems should be interoperable by means of appropriate mechanisms.

6.7 Compliance

In order to support policy interoperability between IoT entities, those IoT entities should conform to the applicable regulations.

6.8 Other IoT characteristics not considered in interoperability

This document does not consider the following IoT characteristics for interoperability:

- usability – including manageability, well-defined components and flexibility;
- reliability, resilience, and availability;
- data characteristics – volume, velocity, veracity, variability and variety;
- scalability;
- trust and trustworthiness.

7 Framework for interoperable IoT systems based on IoT reference architecture

7.1 Context for interoperability within and between IoT systems

The framework for interoperable IoT systems has a context which is established by ISO/IEC 30141. Figure 2 shows the interactions which take place in IoT systems and the entities which are involved. Figure 2 is a simplified version of Figure 14 in ISO/IEC 30141:2018, which concentrates on the interactions that take place.

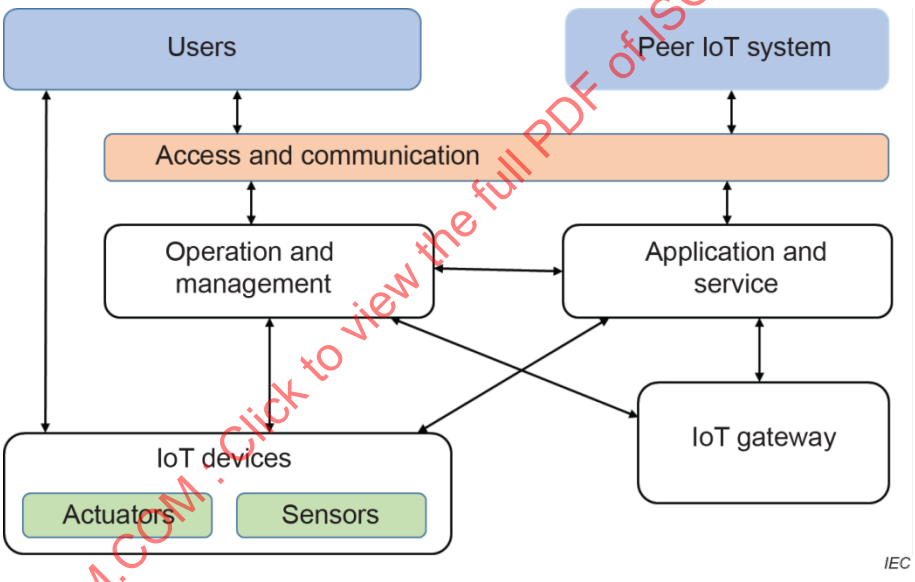

Figure 2 – Entities and interactions in IoT systems

There are two broad types of interactions depicted in Figure 2:

1) interactions between two IoT systems, indicated by the arrow linking Peer IoT system and Access and communication
2) Communication between entities within a single IoT system, indicated by all the other arrows.

The major interactions taking place between entities within an IoT system are:

- applications and services with IoT devices;
- applications and services with IoT gateways;
- IoT gateways with IoT devices;
- applications with services;
- services with services;

- management systems with IoT devices;
- management systems with IoT gateways;
- management systems with applications and services;
- management systems with user devices.

The framework for interoperable IoT systems is applicable to the major interactions identified in 7.2.

7.2 General description

Subclause 7.2 explains the framework for IoT interoperability in terms of the interactions within and between IoT systems described in 7.1.

The interoperability facet model described in 5.3 indicates that for interoperability to take place between two systems each of the interoperability facets shall be handled appropriately.

If one IoT entity can connect to and use another IoT entity, then the IoT entities are interoperable. To connect to and use another IoT entity, it is necessary for the using IoT entity to know about the target IoT entity. Knowledge about a target IoT entity can be gained by a number of means:

- through the use of a discovery protocol;
- through the use of a registry service;
- through manual configuration of the using IoT entity using static information known about the target IoT entity.

The necessary knowledge about the target IoT entity includes information about the endpoint exposed by the target and the interface offered by that endpoint:

- transport information including the physical layer and the protocol(s);
- syntactic structure of exchanged data;
- semantic meaning of exchanged data;
- behavioural aspects of the IoT entity for each of the interface operations;
- policy elements that apply to the use of the IoT entity.

Together, this information about interacting with an IoT entity is termed IoT entity metadata. Therefore, models are needed to describe the IoT entity metadata concerning the endpoints and interfaces of IoT entities.

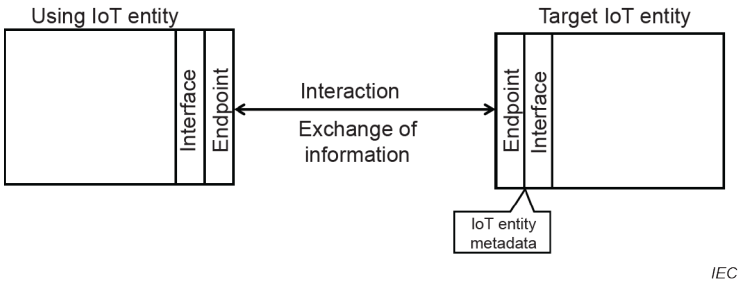

Figure 3 – Concepts for interoperability of IoT entities

Figure 3 shows the concepts for interoperability of IoT entities. In Figure 3, interaction takes place between two IoT entities and information is exchanged. The target IoT entity offers an endpoint with an associated interface that is invoked by the using IoT entity. It is necessary that the processes or activities of the interacting entities achieve successful behavioural interoperability. Otherwise, the target entity cannot provide the features and functionalities that are expected by the source entity.

One important aspect of any IoT entity is that it may have multiple separate interfaces, often exposed on different endpoints. It is common for an IoT entity to have a functional interface which offers the main capabilities of the IoT entity and a separate management interface which enables the IoT entity to be managed and controlled. Interoperability for the functional interface is likely to be separate from interoperability for the management interface, each likely to have different using IoT entities.

The framework for IoT interoperability includes IoT entity models and includes interaction models between IoT entities, plus models for the IoT entity metadata used to describe them.

7.3 Interoperability of IoT entities

In many cases, interacting IoT entities are interoperable. This can be the case because the using IoT entity is designed and built with the use of the particular target IoT entity as a primary requirement. An alternative case is where the using IoT entity and the target IoT entity are both designed to use a specific standardized interface for a specific capability.

In these cases of interoperable IoT entities, it is likely that the transport, syntactic, semantic data and behavioural facets all match between the using IoT entity and the target IoT entity.

The real value of the interoperability model for IoT systems applies to cases where there is a mismatch between the using IoT entity and the target IoT entity. The interoperability model can offer approaches that can be taken to overcome interoperability mismatches between the two IoT entities. Annex A will be helpful to understand the interaction among the entities.