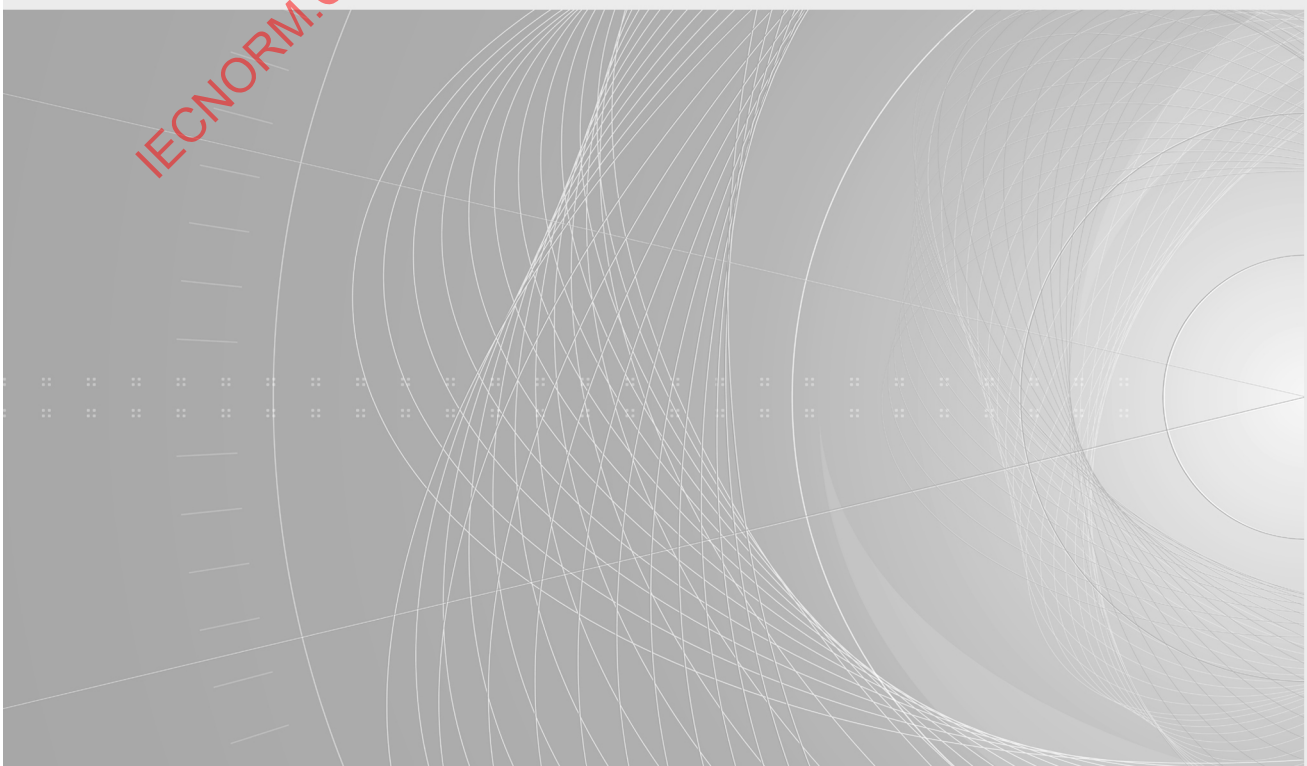
ISO/IEC 21823-2

Edition 1.0 2020-04

INTERNATIONAL STANDARD

colour inside

Internet of things (IoT) – Interoperability for IoT systems – Part 2: Transport interoperability



ISO/IEC 21823-2:2020-04(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 It also gives information on projects, replaced and withdrawn publications.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 21823-2

Edition 1.0 2020-04

INTERNATIONAL STANDARD

Internet of things (IoT) – Interoperability for IoT systems – Part 2: Transport interoperability

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.020; 35.110

ISBN 978-2-8322-8142-0

CONTENTS

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

Part 2: Transport interoperability

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 21823-2 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 *Internet of Things (IoT) – Interoperability for IoT systems*, can be found on the IEC and ISO websites.

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

FDIS	Report on voting
JTC1-SC41/138/FDIS	JTC1-SC41/153/RVD

Full information on the voting for the approval of this International 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 among 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, both between different IoT systems and within a single IoT system. ISO/IEC 21823-1 describes a general framework for interoperability for IoT systems. This includes a facet model for interoperability which includes five facets of interoperability: transport; syntactic; semantic; behavioural; policy. This document (ISO/IEC 21823-2) addresses the transport interoperability for IoT systems. The semantic facet of interoperability will be addressed in a future International Standard (ISO/IEC 21823-3). The potential other parts address the syntactic facet, the behavioural facet and the policy facet of interoperability.

As described in ISO/IEC 30141, IoT systems have multiple different types of networks connecting the various system entities – network connectivity, addressing the transport facet of the interoperability model, is thus of great importance in the description of interoperability for IoT systems. The different networks need to be combined to provide the necessary network connectivity between entities which are attached to each of the networks – in short, to enable those entities to be interoperable. An example are the centralized applications and services which need to receive data from remote sensors, or issue commands to remote actuators.

Network connectivity is the name given to the methods by which the various networks in an IoT system are connected to one another. This document specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system.

To provide seamless communication and interaction between and within networks, it is important to solve network level interoperability issues in IoT systems. There are four types of networks in IoT systems, including user networks, service network, access network and proximity network, which are defined in ISO/IEC 30141 and used in ISO/IEC 21823-1. The relationship and interface among these networks for supporting networks interoperability need to be specified.

For this purpose, this document focuses on network connectivity, which is the precondition of interoperability in IoT systems.

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

Part 2: Transport interoperability

1 Scope

This part of IEC 21823 specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies:

- transport interoperability interfaces and requirements between IoT systems;
- transport interoperability interfaces and requirements within an IoT system.

2 Normative references

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924 and the following 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
network connectivity
ability to exchange information as bits and bytes, assuming that the information exchange infrastructure is established and the underlying networks and protocols are unambiguously defined

[SOURCE: IIC:PUB:G5:V1.01:PB:20180228. The Industrial Internet of Things Volume G5: Connectivity Framework]

3.2
transport interoperability
interoperability 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]

4 Network connectivity for transport interoperability

ISO/IEC 21823-1 [1] [1] describes the overview and a facet model for IoT interoperability. Interoperability can be defined as a measure of the degree to which various kinds of systems or components interact successfully. ISO/IEC 21823-1 [1] defines interoperability as the "ability for two or more systems or applications to exchange information and to mutually use the information that has been exchanged".

There is both interoperability between two or more IoT systems, and also interoperability between entities which exist in one IoT system. Only with effective interoperability between entities can IoT systems be reliably constructed and used, in support of the many IoT applications which are being built.

A five-facet model of IoT interoperability is introduced in ISO/IEC 21823-1 [1] as shown in Figure 1.

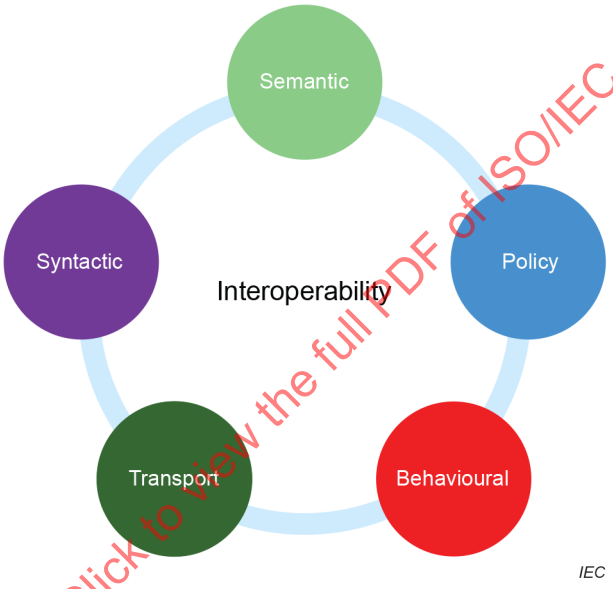


Figure 1 – Facets of IoT interoperability

This document covers network connectivity which deals with the transport facet of this model. Network connectivity describes how the many different IoT networks connect to one another to enable seamless communication, and how different entities, which may be connected to different networks, are able to interoperate. Network connectivity provides common guidelines for the interconnection and interoperation of different networks and pushes IoT large scale application. Network connectivity is a fundamental and key aspect of transport interoperability. Discussion of the other facets of IoT interoperability is handled by other parts of ISO/IEC 21823.

As described in ISO/IEC 30141 [2], there are four types of networks in IoT systems: user network, service network, access network and proximity network. The relationships and interfaces between these networks for supporting interoperability are described in ISO/IEC 30141 [2].

This document defines a framework of transport interoperability in terms of network connection models, interfaces and stack model.

---

1 Numbers in square brackets refer to the Bibliography.

5 Overview

5.1 Network connectivity model and interfaces between IoT systems

Clause 5 focuses on the network interfaces between IoT systems. As shown in ISO/IEC 30141 [2], IoT systems interact with one another through the Resources access and interchange domain functional component, which presents one or more interfaces to support this interaction. This is shown schematically in Figure 2. The related elements are described in ISO/IEC 30141 [2].

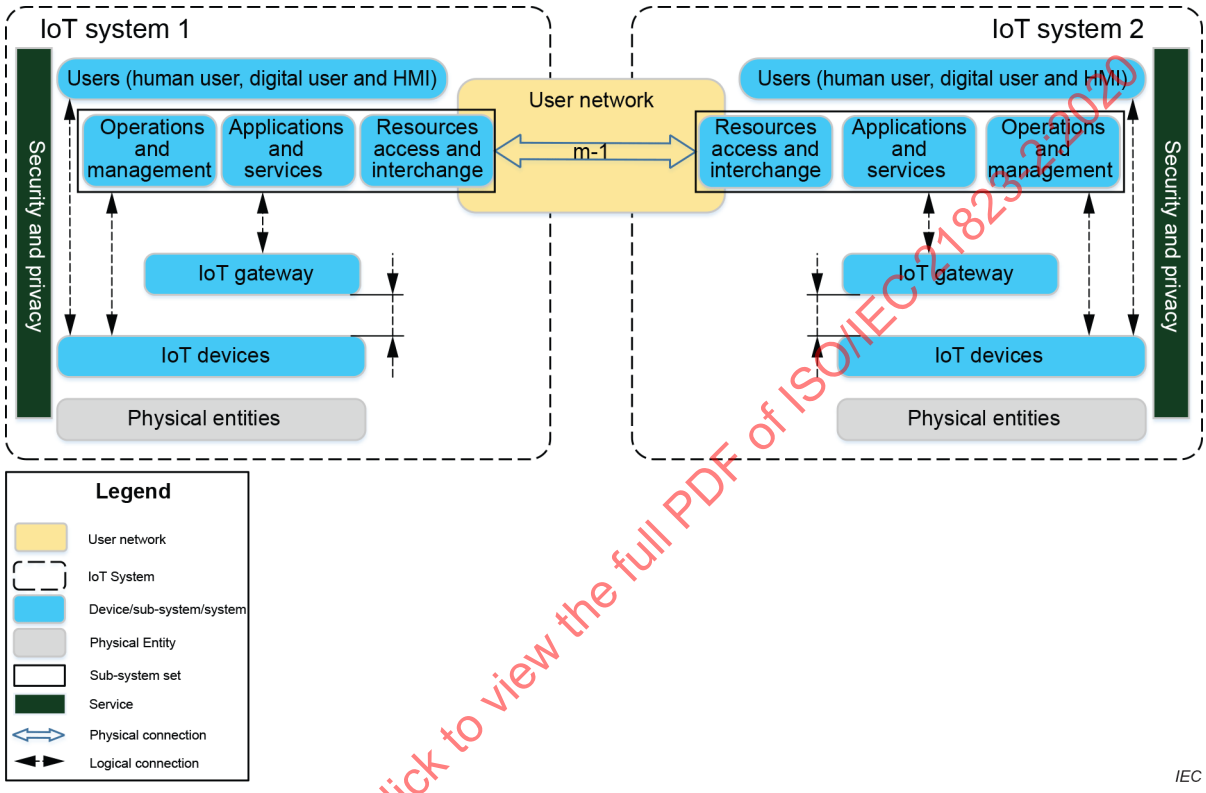


Figure 2 – Network connectivity model between two IoT systems

The connectivity labelled m-1 in Figure 2 represents one or more interfaces for whichever capabilities are offered by each of the IoT systems to the other. Communication takes place via the use network which uses any means or protocol that is feasible for this interaction, and in that way both user devices and digital users can communicate with the rest of the IoT system, as defined in ISO/IEC 30141 [2]. User network only exists between Resources access and interchange domain. When the entities in an IoT system need to collaborate with some entities in another IoT system, the entities communicate with the Resources access and interchange domain, which handles connections to other IoT systems.

For the two IoT systems to interoperate, each of the interfaces in m-1 that are used shall interoperate for transport interoperability. There are many applications that have interoperability requirements. For example, in some industrial applications, two different IoT systems share sensor data. The entities in one IoT system use these data to make decisions. And then they operate on the entities (such as actuators) in another IoT system through the Resources access and interchange domain to achieve interoperation and collaboration between the two IoT systems.

5.2 Network connectivity model and interfaces within an IoT system

Within an IoT system, four networks are defined by ISO/IEC 30141 [2]:

- User network: This network connects the User domain with the Application service domain (ASD) and Operations and management domain (OMD). It also connects peer IoT systems and non-IoT systems with the IoT Resources access and interchange domain (RAID). This network connects entities in the User domain with the Resources access and interchange domain.
- Service network: This network connects elements within and between the ASD, the RAID, and the OMD. This network can include both Internet elements and also (private) intranet elements.
- Access network: Access networks are typically wide area networks connecting devices in the Sensing and controlling domain (SCD) to the other domains the ASD and the OMD.
- Proximity network: This network exists within the Sensing and controlling domain. Its main task is to connect the sensors and actuators to gateway.

The primary set of connections that shall be supported by network connectivity within an IoT system are shown in Figure 3 (derived from Figure 17 of ISO/IEC 30141:2018).

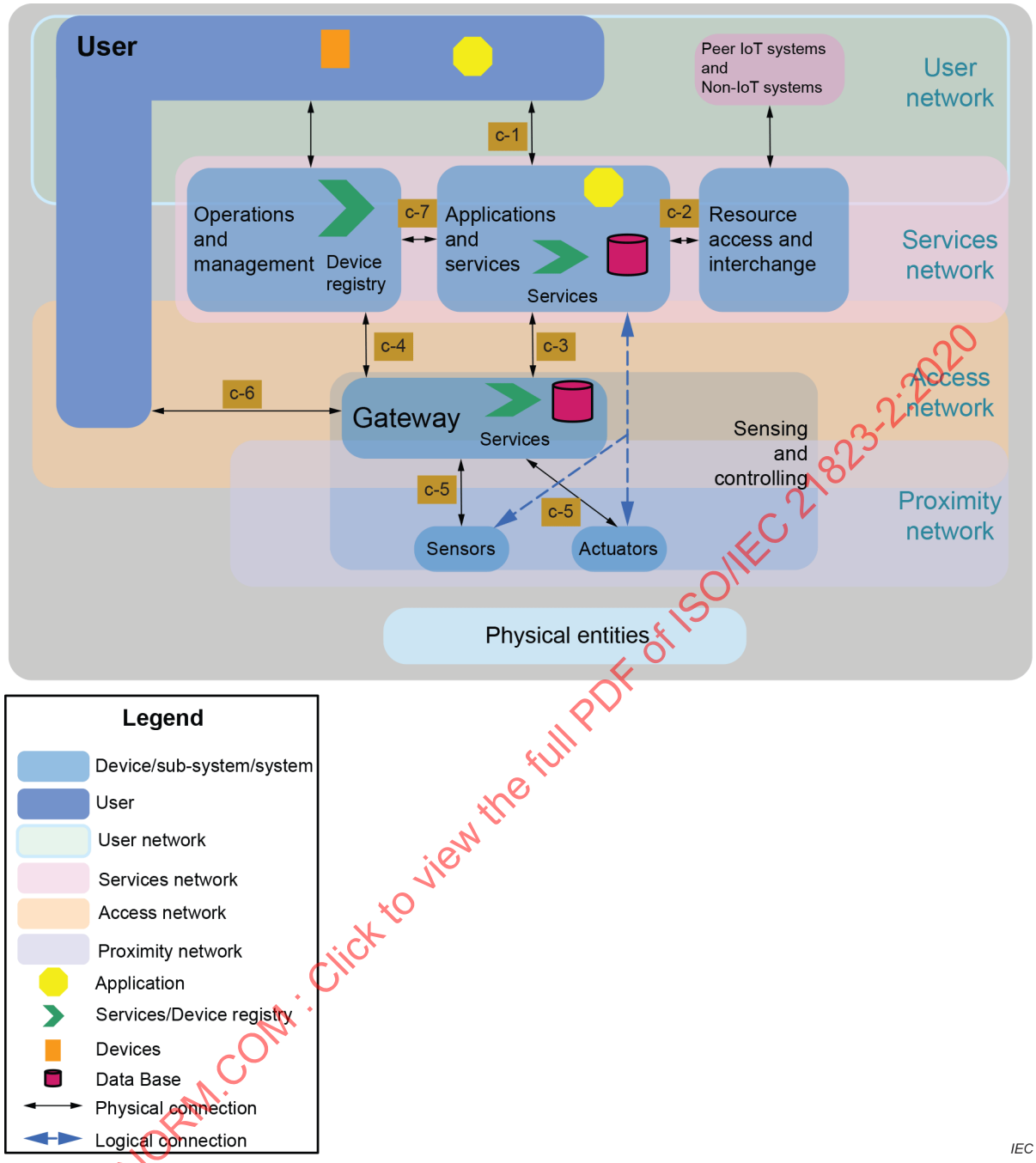


Figure 3 – Network connectivity model within an IoT system

The connections are labelled c-1 through c-7.

- c-1: Connections from user to the Application and Service sub-system via the user network.
- c-2: Connections from the Resource access and interchange domain to entities in both the Applications and services domain and to entities in the Operations and management domain, via the services network.
- c-3: Connections from Applications and services domain to IoT gateways via the access network.
- c-4: Connections from Operations and management to IoT gateways via the access network.
- c-5: Connections between IoT gateways and sensors and actuators via the proximity network.

- c-6: Connections from user directly to entities in the Sensing and controlling domain, such as IoT gateways and/or sensors and actuators, via the access network.
- c-7: Connections from entities in the Operations and management domain to entities in the Applications and services domain.

For supporting network connectivity, connections from c-1 to c-7 rely on the network elements described in 7.2.

Each of the different networks might be using one or more different types of communication technology (e.g. wired, wireless, local area vs. wide area) and a variety of different hardware and communications protocols might be involved. How the various entities communicate with each other, particularly where different networks are involved, is part of the network connectivity stack model. Interconnection can involve a range of devices such as routers, switches, gateways, protocol translators and so on. Addressing target entities across different types of network can sometimes be a challenge and require particular approaches to network connectivity.

5.3 Network connectivity stack model

Subclause 5.3 discusses an IoT connectivity stack model and corresponding architectural role.

The IoT connectivity stack model is shown in Figure 4 and Figure 5. Different protocols can be used in each layer, the pair of corresponding layers in two IoT systems (or two networks within an IoT system) interact with each other through access points for the network connectivity. The network connectivity is a fundamental and key aspect of the transport interoperability.

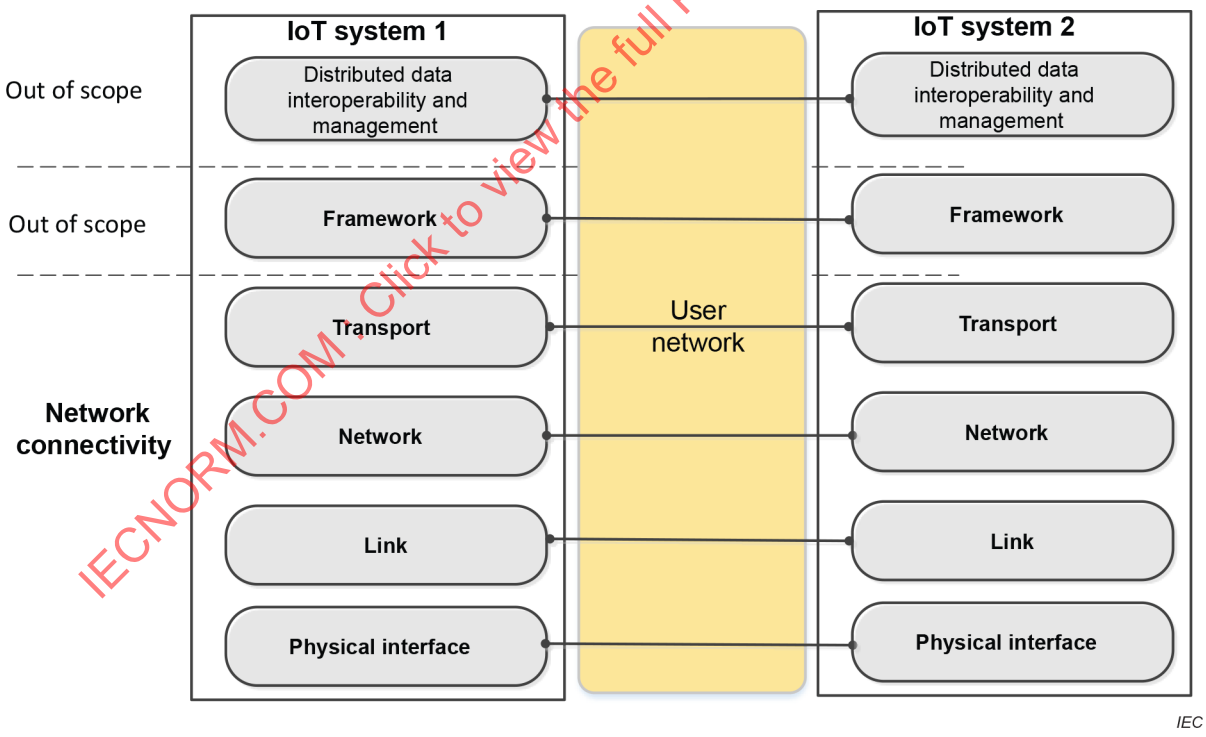


Figure 4 – Network connectivity stack model between IoT systems

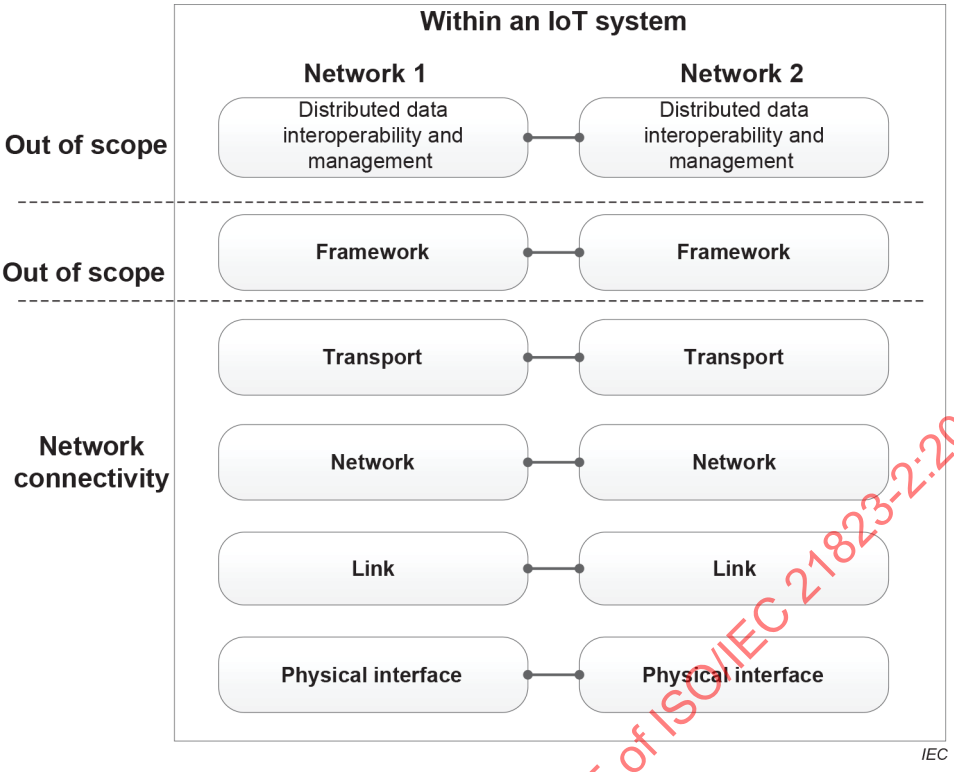


Figure 5 – Network connectivity stack model within an IoT system

Referring to seven-layer Open Systems Interconnect (OSI) Model and "The Industrial Internet of Things Volume G5: Connectivity Framework" [3], the layers are defined as follows.

The seven-layer Open Systems Interconnect (OSI) model and the four-layer Internet model do not capture all IoT connectivity requirements. IoT systems require a new connectivity functional layer model to address IoT entities. Subclause 5.3 proposes an IoT connectivity stack model using the OSI model, the Internet model and IIC Industrial Internet Connectivity Stack Model as reference.

In this IoT connectivity stack model, the physical layer is the lowest one, which refers to the exchange of physical signals on the physical media (wired or wireless) connecting the participants. Link layer refers to the exchange of frames using signalling protocols on the shared physical link between adjacent participants. Network layer refers to the exchange of packets, possibly routing them over multiple links to communicate between participants. Transport layer refers to the exchange of messages between participant applications. Framework layer refers to the exchange of structured data (state, events, streams) with configurable quality-of-service between participant applications. Above it, but outside the scope of connectivity, is the data semantic interoperability. Each layer builds on the capabilities provided by the layer below. It covers from the information (data in context), data (state, event, streams), message, packets, frames and bits. The document discusses Transport, Network, Link and Physical interface layers. Framework layer contains the Syntactic facet of the ISO/IEC 21823-1 [1] model. The four layers are valid for the "Transport" facet of the ISO/IEC 21823-1 [1] model. Those two parts of syntactic and semantic are out of scope of this document. ISO/IEC 21823-2 addresses physical interface layer, link layer, network layer and transport layer, which are important components of network connectivity. For IoT systems, connectivity comprises three functional layers.

- The connectivity network layer evolves the IP and non-IP connections and help for large scale application of IoT.
- The connectivity transport layer provides the means of carrying data between endpoints. It provides end-to-end interoperability between endpoints participating in a data exchange.

- The connectivity stack model layer facilitates how data is unambiguously structured and parsed by the endpoints.

6 Requirements for network connectivity between IoT systems

6.1 Overview

Clause 6 describes interfaces c-1 and the network connectivity requirements for the operability between different IoT systems. The c-1 is an interface between two IoT systems. The connectivity between different IoT systems is described in Figure 6.

Clause 6 also gives the definition of specific interfaces between IoT systems, including the network time synchronization interface, network protocol translation interface, network resource interface, etc.

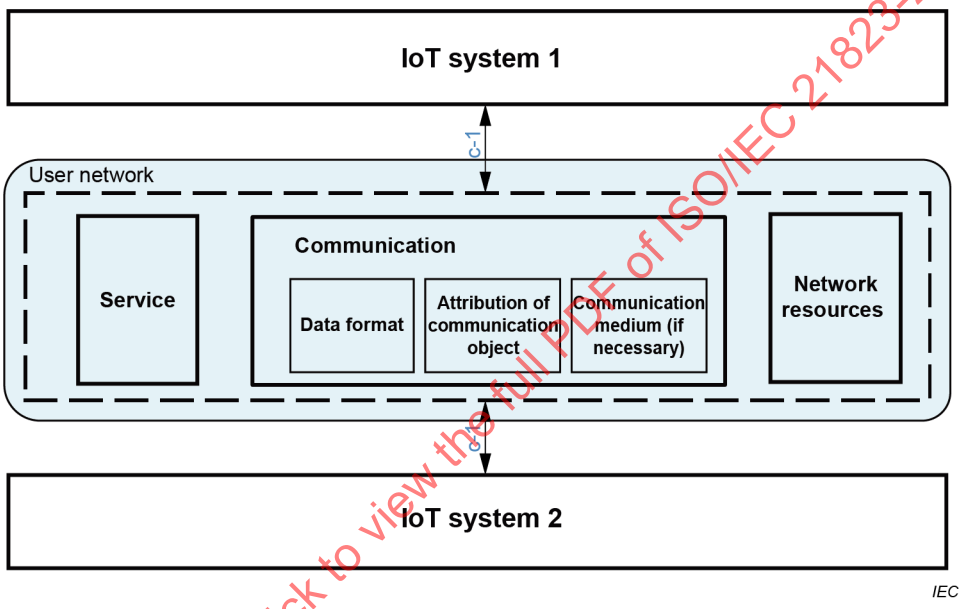


Figure 6 – The connectivity between different IoT systems

In order to achieve the transport interoperability between different IoT systems, related interoperability requirements need to be considered from three aspects: service, communication and network resources. Here, three interoperability requirements are discussed.

- Service-related interoperability: for interoperability, the interface offered by IoT system 2 to IoT system 1 shall match that expected by IoT system 1, in terms of syntax, semantics and behaviour.
- Communication-related interoperability: the communication protocols specify interactions between the communicating entities. The networks need to have the rules for interoperability.
- Network resource-related interoperability: the network needs to provide the resources of the network attributes that need to be unified, such as QoS, communication channels, etc.

The service-related interface is actually related to semantic and syntactic layers in the network connectivity stack model. The communication-related interface is related to layers of the transport, network, link, and physical interface. And the network resource-related interface is related to the physical interface layer.

6.2 Network interfaces between different IoT systems

6.2.1 Network service interface

The network service interface between different IoT systems provides the ability to support the service over connectivity IoT systems. The services may include publish-subscribe, request-reply, discovery, exception handling.

A request-reply service interface shall support the request-reply data exchange pattern in which a requestor initiates a service request with regard to a special endpoint that will operate in a replier role.

A publish-subscribe service interface provides the ability to support a pattern of data-exchange that related to a pair of endpoints. One publishes data on a well-known topic without regard to subscribers, while another subscribes to data without regard to publishers.

An exception handling service interface provides a way to handle exceptions from all consequences that may arise as a result of disconnected or intermittent connection, network configuration changes, data quality of service not being met, remote endpoint or component failure, etc.

A discovery service interface shall support a discovery mechanism so as to facilitate the implementation of a more intelligent decision. The targets to be discovered may include services and their associated quality of service, data types, and entities participating in a service process for network connection.

6.2.2 Network protocol translation interface

A network protocol translation interface between different IoT systems provides a unified way to translate the different network protocols. A network protocol translation interface provides a data format system for representing data objects as structures for formatting data to be communicated with other networks over IoT systems. It shall have the ability to manage the evolution of data types and defines the serialized data format in communication and storage.

Meanwhile, the network protocol translation interface provides a means to manage the lifecycle of a communication object. The four critical operations are create, read, update and delete. An attribution of communication object should provide a state management function to manage the historical state of the communication objects. The IoT system can obtain the state for different time periods.

6.2.3 Network resource interface

A network resource interface provides a way of accessing the resources of the network attributes that need to be unified. A resource object is an entity or abstractor with special meanings, such as QoS, communication channels, etc.

6.3 Requirements of network connectivity

6.3.1 General

The requirements are not only the functional requirements, but also the non-functional requirements of service, protocol, network resource, time-dependence QoS, bandwidth, signalling, status monitor and security.

6.3.2 Service-related requirement

The network service interface between different IoT systems is the most significant role for ensuring the service of one IoT system meets its service level commitments to any other specific IoT systems. The service interface shall encapsulate all available services provided by the IoT system.

The implementing of service interfaces may increase time delay and reduce bandwidth; thus a trade-off shall be considered.

The service interface is usually capable of being addressed by the specific device over other IoT systems. The design of service interface shall decouple the interface implementation from the business logic.

6.3.3 Communication-related requirement

The network protocol interface between different IoT systems shall encapsulate all aspects of the network protocol used for communication over the IoT systems. The network communication implementation has its own contract with the network protocol interface, and shall have no dependencies on the specifics of the network protocol.

The network protocol interfaces may be configured and optimized for different IoT system configurations according to the bandwidth, round-trip time and maximum message size.

6.3.4 Network resource-related requirement

IoT systems involve management of large volumes of network resource. For a special operation at a given time, the interest network resource set is usually a specific subset of the network resources, and the interest set changes with time. For IoT systems, it is highly desirable to specify a content-based network resource subset of interest, so as to automatically optimize the resource management.

The demands for network resource are quite different for two connectivity components within an IoT system. Also, for a specific component, its desired resource items and resource rate may change over time. For IoT systems, it is highly desirable to specify a time-based network resource subset of interest by analysing the desired resource-rate needs across components.

6.3.5 QoS requirement

IoT systems have varying requirement for the data QoS.

From the aspect of data delivery, the QoS requirement includes best-efforts delivery in which the data are delivered only once, and reliable delivery in which the data are delivered many times until a reply is received.

In addition, the requirement includes the following.

- Timeliness: a description of the ability of the connectivity network to ensure device-to-device timing constraints.
- Ordering: a description of the ability of the connectivity network to present the data in the specific order.
- Durability: a description of the ability of the connectivity network to make data available in the lifecycle.
- Lifespan: a description of the ability of the connectivity network to make some useless data expire.
- Fault tolerance: the ability to guard against the fault or adaptability of the system to function properly in the midst of several errors/anomalies in the devices and the IoT network.

6.3.6 Bandwidth requirement

Bandwidth is used to represent the ability of data distribution over a network per unit time. In different cases, the bandwidth requirements can vary widely; for example, in the case of large load conditions, the requirements for bandwidth are more demanding compared to normal state. A connectivity network shall be able to ensure the time-related performance such as latency and jitter while increasing bandwidth requirements. Thus, in IoT systems, the trade-off between time-related performance and bandwidth requirement shall be carefully evaluated.

6.3.7 Signalling requirement

A communication path over different IoT systems may span across different physical signals. The connectivity network shall be able to meet the signalling requirements for spanning the different networks. For IoT systems, it is desirable to support a variety of signals.

6.3.8 Status monitor requirement

Status monitor shall be considered for IoT systems in order to support the operational needs of systems. Further management and dynamic replacement of the connectivity elements may be achieved by monitoring the prosperities of the connectivity function, like health, performance and service-level characteristics.

6.3.9 Security requirement

Adequate protective measures shall be considered for each of the network connectivities between different IoT systems. Different network connectivities may have different choices of security requirements. The security requirement for each network connectivity shall be considered according to its own application requirement.

The security policies govern all kinds of protective measures as a part of a broader protection strategy. The security mechanisms shall provide a means to guarantee data exchange permissions authorization management, data integrity and trustworthiness, sensitive data flows encryption, secure logging and auditing capabilities, etc.

6.3.10 Time-dependent requirement

In order to ensure the effectiveness of data in separate networks over different IoT systems, the devices in one network or over different IoT systems shall maintain the consistency of time. This requires all devices to be able to implement time synchronization through the interface.

In some cases, the real time is required over different IoT systems, which is more concerned with deterministic response than fast response.

7 Requirements for network connectivity within an IoT system

7.1 Overview

Clause 7 defines the interfaces and requirements of each network within an IoT system and achieves the connectivity of the networks within the IoT system. IoT entities communicate with each other and the networks connect them.

Clause 7 will also give the definition of specific inner-networking interface, including the network time synchronization interface, network protocol translation interface, and network resource interface.

The functional networks in IoT system have been specified, including the user network, service network, and proximity network.