ISO/IEC 21823-2

Edition 1.0 2020-04

INTERNATIONAL STANDARD

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

colour inside

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

ISO/IEC 21823-2

Edition 1.0 2020-04

INTERNATIONAL STANDARD

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

colour inside

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.

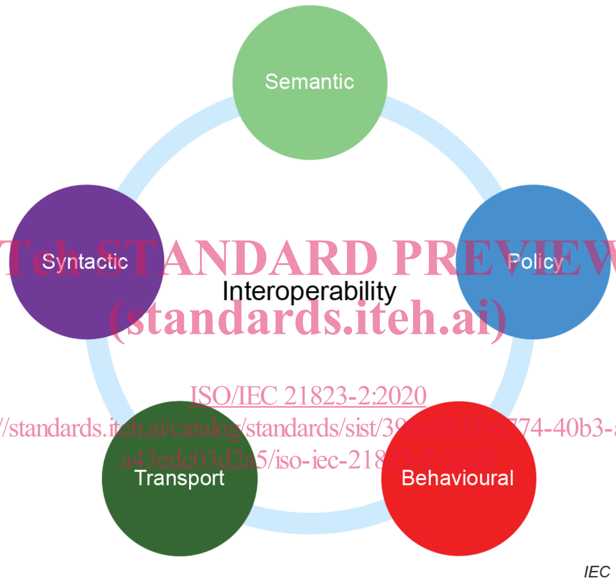

Figure 1 – Facets of IoT interoperability

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].

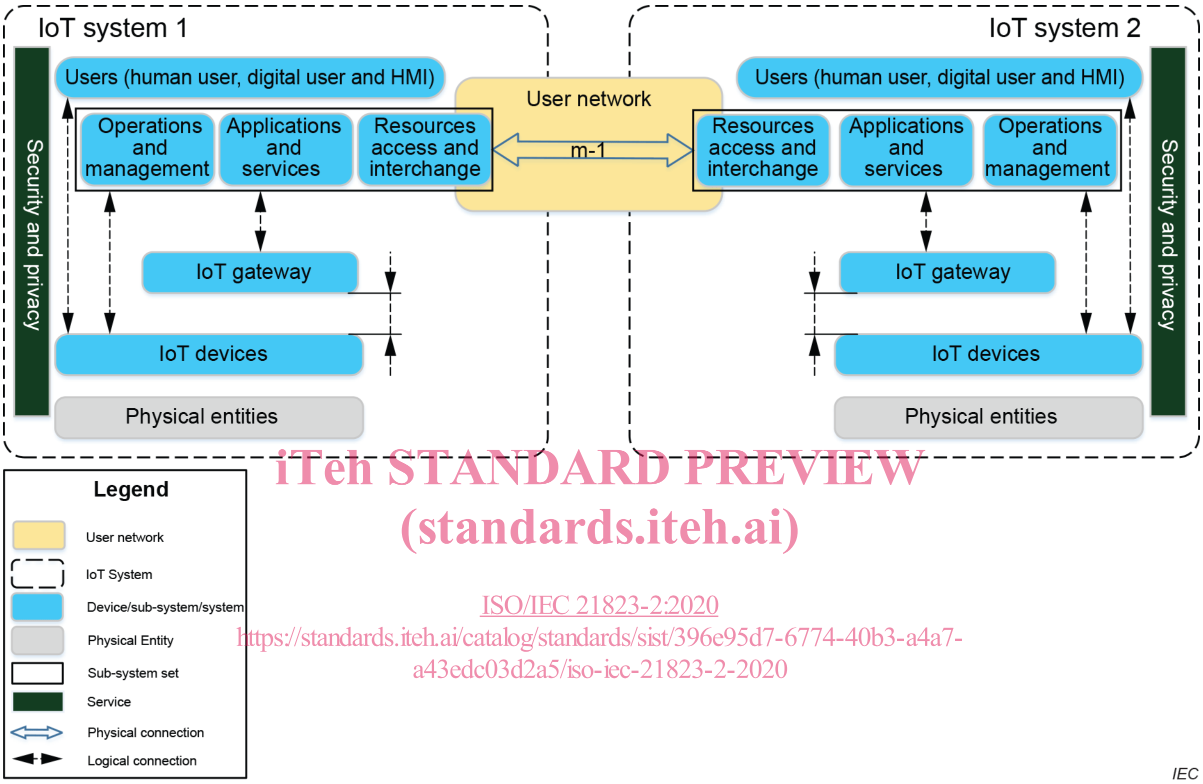

Figure 2 – Network connectivity model between two IoT systems

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).

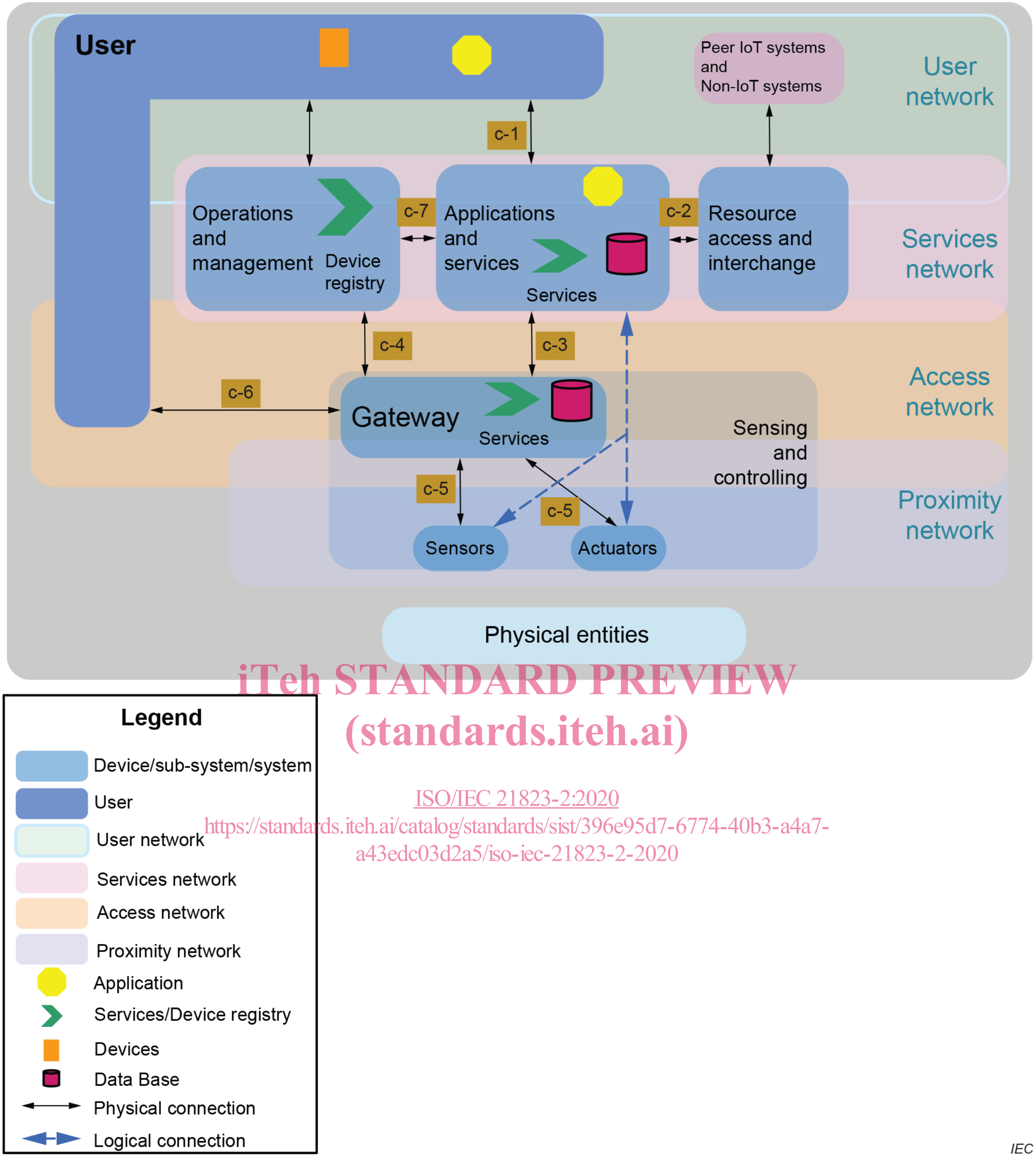

Figure 3 – Network connectivity model within an IoT system

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.