ISO/IEC 30161-1

Edition 1.0 2020-11

INTERNATIONAL STANDARD

Internet of things (IoT) – Data exchange platform for IoT services – Part 1: General requirements and architecture

ISO/IEC 30161-1:2020-11(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 It also gives information on projects, replaced and withdrawn publications.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 30161-1

Edition 1.0 2020-11

INTERNATIONAL STANDARD

Internet of things (IoT) – Data exchange platform for IoT services – Part 1: General requirements and architecture

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.020

ISBN 978-2-8322-8997-6

CONTENTS

INTERNET OF THINGS (IoT) – DATA EXCHANGE PLATFORM FOR IOT SERVICES – Part 1: General requirements and 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) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 30161 was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

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

FDIS	Report on voting
JTC1-SC41/178/FDIS	JTC1-SC41/187/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

IoT implements various services in many fields, such as "Remote Management of Large Equipment in a Plant", "Warehouse Goods Monitoring", "IoT Endpoint (Sensors and Actuators) Monitoring Systems", etc. The IoT architecture can be categorized into vertical and horizontal approaches. For small deployments in limited areas, the vertical approach is possible. However, for large scale deployments, the horizontal approach is required, and then introducing the concept of a common platform is helpful for implementing various services. In the horizontal approach, information processing and networking are positioned as the platform. And also, the types of IoT services are increasing in different application fields. To make IoT services more creative and productive, data exchange between various IoT services needs to be supported and a common platform for data exchange is the simplest way. This document has been developed in accordance with a detailed study of a platform that supports various IoT use cases.

INTERNET OF THINGS (IoT) – DATA EXCHANGE PLATFORM FOR IOT SERVICES – Part 1: General requirements and architecture

1 Scope

This document specifies requirements for an Internet of Things (IoT) data exchange platform for various services in the technology areas of:

- the middleware components of communication networks allowing the co-existence of IoT services with legacy services;
- the end-points performance across the communication networks among the IoT and legacy services;
- the IoT specific functions and functionalities allowing the efficient deployment of IoT services;
- the IoT service communication networks' framework and infrastructure; and
- the IoT service implementation guideline for the IoT data exchange platform.

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 30141:2018, *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
IoT data exchange platform
IoT DEP
set of functional blocks that provide an abstraction of IoT data blocks and exchange of IoT data with other entities

Note 1 to entry: For example, in a huge number of sensors across various networks, IoT DEP reduces traffic volumes and exchanges IoT data with other entities. Functional blocks of IoT DEP are implemented at endpoints and nodal points in IoT networks. These functional blocks cooperate as a platform.

3.2
nodal point
point that investigates routing information specified in communication protocols and relays data blocks according to such information

4 Abbreviated terms

CAC	communication access control
CCN	content centric network
DNS	domain name service
ICN	information centric network
IoT	Internet of Things
IoT DEP	IoT data exchange platform
IP	internet protocol
MQTT	Message Queuing Telemetry Transport
OSI	open systems interconnection
QoS	quality of service
TCP	transmission control protocol
UDP	user datagram protocol

5 Overview of IoT services

Considering IoT use cases across sectors, it can be assumed that data blocks from/to sensors and actuators, referred to as "IoT data", are transferred across networks. To reduce traffic volume and comply with various user requirements on QoS, it is reasonable that an IoT DEP should be deployed. The IoT DEP is positioned in the application layer of the OSI reference model. However, IoT data is transferred over abstracted lower layers including the current Internet. An IoT DEP shall be implemented in accordance with the networking view of IoT reference architecture defined in ISO/IEC 30141:2018.

The IoT DEP should not impact communications other than IoT data and permit co-existence of communications of IoT data and other data. Therefore, this document promotes an approach that isolates communications of IoT data from other communications. It excludes specifications of cloud computing and edge computing, which deal with distributed operations for every layer in the reference model.

Overviews and analyses of the IoT use cases have motivated this document and are summarized in Annex C. These use cases are collected in ISO/IEC TR 22417 [1][1].

6 Network configurations for IoT services

6.1 Overview of network configurations for IoT

An overview of network configurations for IoT is shown in Figure 1. Networks provide connection among IoT users, IoT gateway, and IoT devices specified in ISO/IEC 30141:2018. Moreover, IoT devices – for example specified in ISO/IEC 30118-1 to ISO/IEC 30118-6 [2],[3],[4],[5],[6],[7] – are included.

Each network can have several nodal points. In ISO/IEC 30141:2018, sub-systems (Operations & Management sub-system, Application & Service sub-system, and Resource Access & Interchange sub-system) in entity-based reference models take on the role of nodal points. These sub-systems correspond to the Operations & Management Domain, Application & Service Domain, and Resource Access & Interchange Domain in a domain-based reference model.

1 Numbers in square brackets refer to the Bibliography.

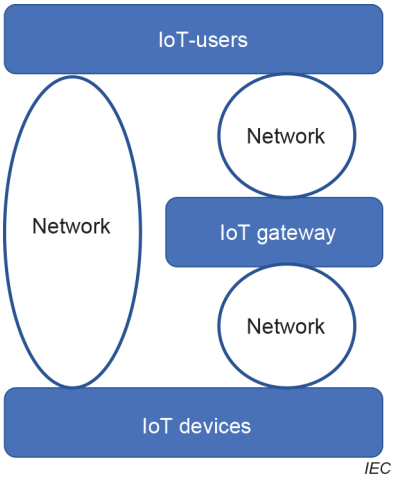

Figure 1 – Overview of network configurations

Detailed network configurations based on Figure 1 are shown in Figure 2. As shown in Figure 2, configurations consist of five service types. Service type 1 provides local services for limited areas. Service types 2 to 5 provide wide area services. In some cases of wide area services, IoT gateway can be deployed for connections between IoT users and IoT devices. However, in other cases, IoT users can be connected to IoT devices without IoT gateway. In network types based on ISO/IEC 30141:2018, a proximity network provides connections for the limited areas. For the wide area services, the user network, service network, and access network are deployed. In these, the user network takes the role of network for IoT specific applications and is operated by IoT user. The service network and access network accommodate generic applications, including IoT-specific applications and legacy applications (e.g. telephony, video distribution, and Internet access). The service network includes switching functions among locations. The access network provides multiplexing functions of traffic flow from every specific area.

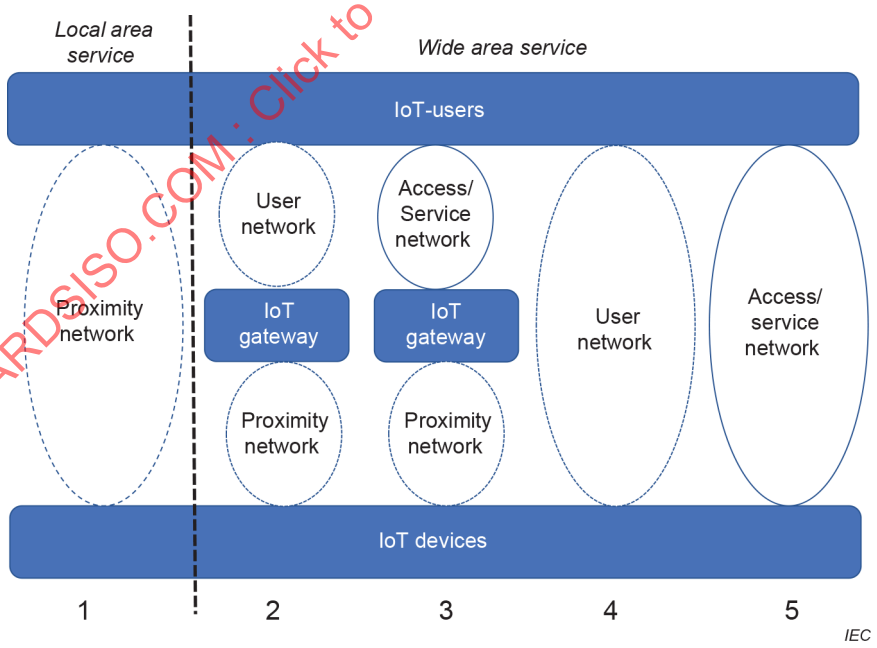

Figure 2 – Service types of the network configurations

6.2 Network models for an IoT DEP

An IoT DEP transfers a huge number of data blocks from/to sensors and actuators effectively. It should be applied to any service including local area services and wide area services for IoT. It should be operated across any network, including proximity networks, access networks, service networks, and user networks specified in ISO/IEC 30141:2018, even if applications other than IoT are deployed in these networks.

Although network configurations are categorized into five types (Figure 2), these five types are aggregated into three types from an IoT DEP point (Figure 3). As shown in Figure 3, configuration type 1, types 2 and 3, and types 4 and 5 are redefined as configuration types X, Y, and Z, respectively.

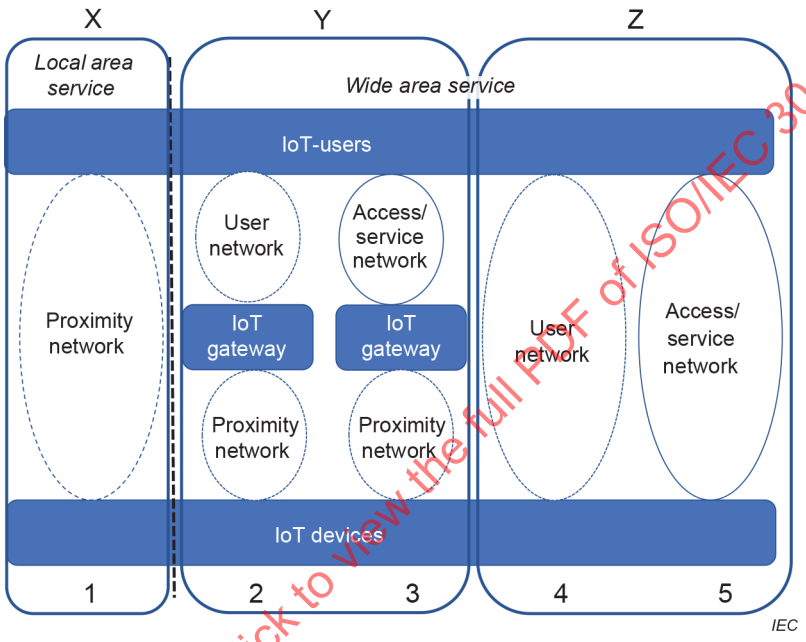

Figure 3 – Redefined configuration types for an IoT DEP

7 Data exchange platform in IoT reference architecture

7.1 General

IoT DEP takes the role of the interworking of information in IoT systems. Cloud computing related technologies, including interfaces of connections to the cloud, are not specified in this document.

An IoT DEP is distributed to entities specified in ISO/IEC 30141:2018. Therefore, it works as a platform by combining distributed parts.

7.2 Position of an IoT DEP in IoT reference architecture

7.2.1 Functions of the IoT DEP

An IoT DEP transfers data to IoT applications effectively as a part of network functions. IoT DEP shall not include data processing and computation in cloud computing.

An IoT DEP shall provide the following functions.

– In order to ensure effective IoT application services, an IoT DEP shall operate independent of communication media and protocols. It shall connect among IoT users and IoT devices via IoT gateway or directly. For example, when a huge volume of data from sensors is transferred across wide area networks using Internet technologies, an IoT DEP provides the communication with small overheads such as small processing delay and/or a small traffic volume by reducing processing on complicated IP related protocols.
– An IoT DEP shall dynamically control the required functions for IoT applications. For example, it controls traffic flows for IoT applications and shall provide a requested QoS.
– An IoT DEP shall manage the validation of communication paths and IoT devices.

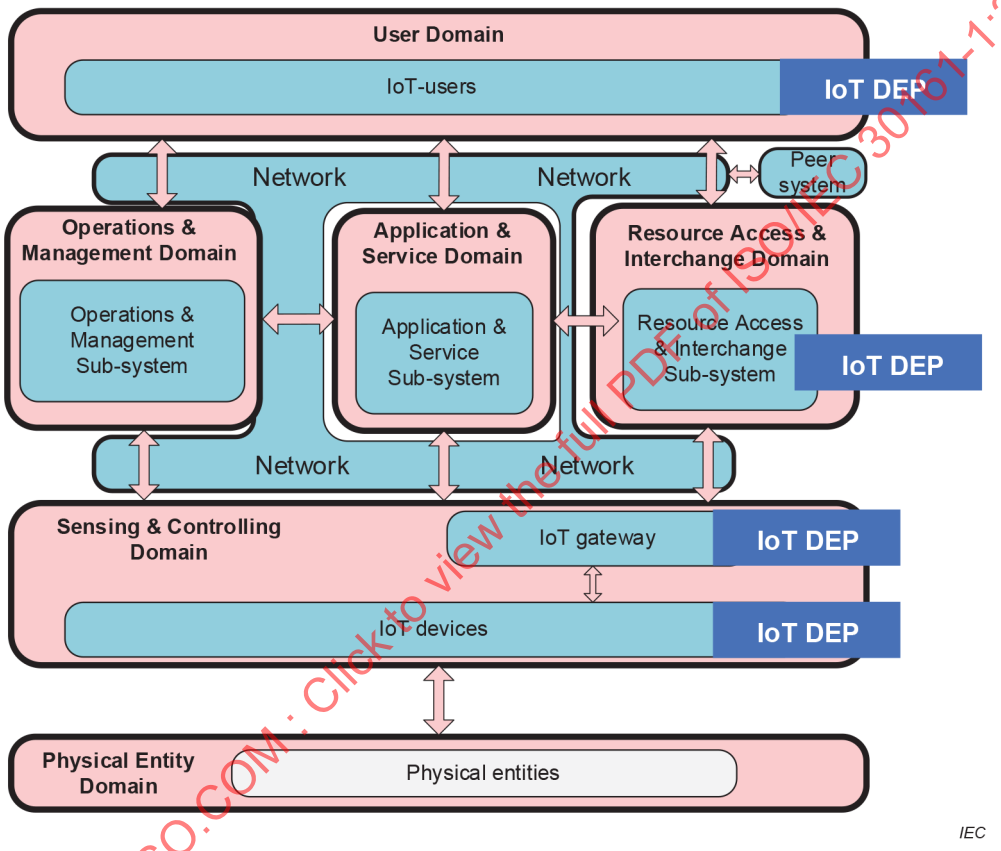

Figure 4 – Locations of IoT DEP functions in the IoT reference models

7.2.2 Positions of the IoT DEP

IoT DEP functions are implemented in IoT user, Resource Access & Interchange sub-system, IoT gateway, and IoT devices that are specified in the entity-based model of ISO/IEC 30141:2018. The relationship between the reference model specified in ISO/IEC 30141:2018 and an IoT DEP is shown in Figure 4. In ISO/IEC 30141:2018, two reference models – entity-based and domain-based – are specified. In Figure 4, locations of the IoT DEP functions are shown, explaining the relationship between both reference models in ISO/IEC 30141:2018.

7.3 Operation of an IoT DEP in an IoT system

Functions of IoT DEP are described in 7.2.1. In Cases C and D, IoT applications provided by an IoT DEP co-exist with legacy applications. Figure 5 shows a logical configuration; however, IoT gateway and Resource Access & Interchange sub-system accommodating IoT DEP functions can be shared with nodal points for legacy applications, from an implementation point of view.

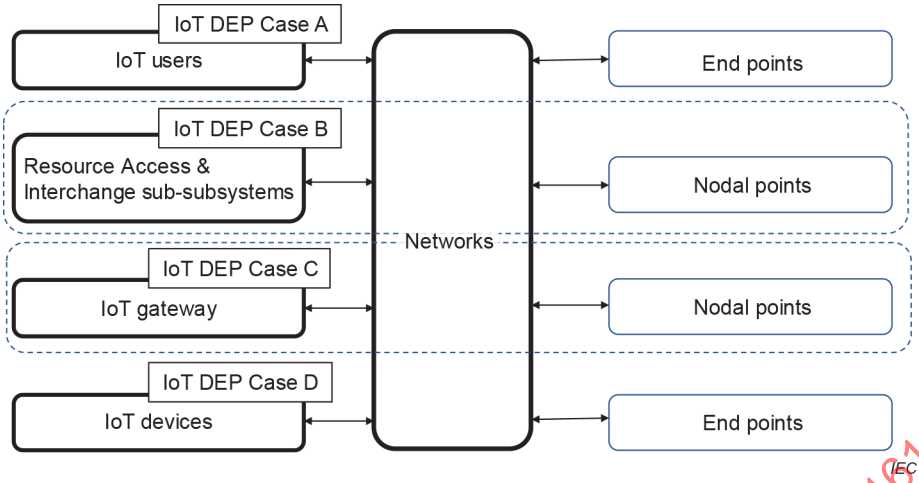

Figure 5 – Cases of an IoT DEP and relationship between IoT and other services

The operations of IoT DEP in each case are described as follows.

– Case A: An IoT DEP shall divide serial data streams from the IoT user to data blocks. Then, it shall transfer these blocks to connected network interfaces, as shown in Figure 6. The connected network interfaces support generic services (e.g. legacy applications on the Internet). An IoT DEP shall isolate communication paths for IoT applications from other paths to provide required QoS in IoT applications. In this operation, some virtualization technologies should be applied.

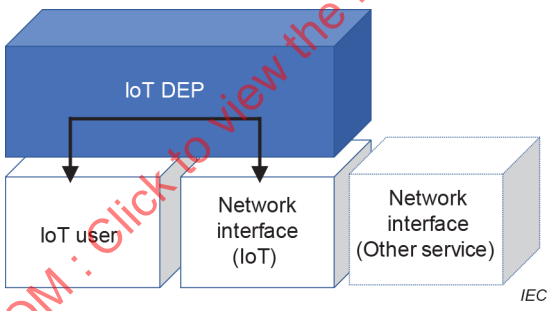

Figure 6 – Operations of the IoT DEP in Case A

– Case B: An IoT DEP takes on the role of a nodal point. In ISO/IEC 30141:2018, network types are categorized into proximity networks, access networks, service networks, and user networks. An IoT DEP shall be applied to all these networks except proximity networks. As shown in Figure 7, IoT applications shall be provided via an IoT DEP between network interfaces. On the other hand, other applications are provided between network interfaces without IoT DEP. In an IoT DEP, paths of IoT applications are controlled to isolate the paths of other applications and to comply with requested QoS requirements in IoT applications.

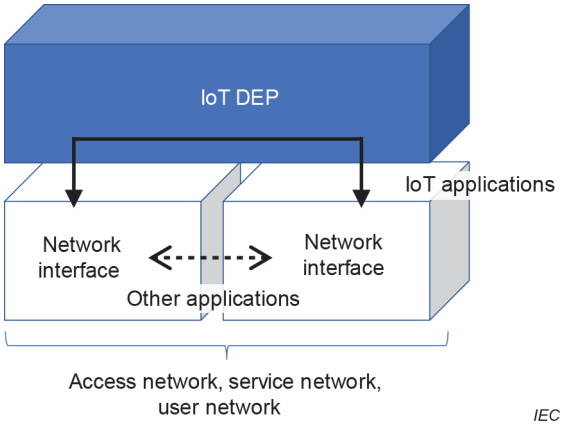

Figure 7 – Operations of an IoT DEP in Case B

– Case C: An IoT DEP is integrated into an IoT gateway. In ISO/IEC 30141:2018, IoT gateway connects between proximity and access networks. An IoT DEP transfers IoT applications between proximity and access networks, as shown in Figure 8. In an IoT DEP, paths of IoT applications are controlled to isolate paths of other applications and to comply with requested QoS requirements in IoT applications, as with Case B.

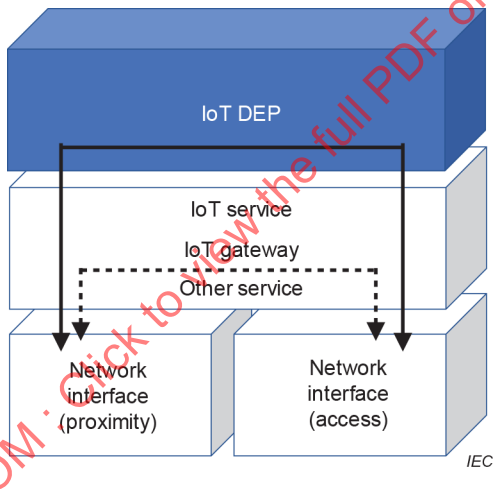

Figure 8 – Operations of an IoT DEP in Case C

– Case D: An IoT DEP is integrated with IoT devices, which accommodate physical entities such as sensors and actuators. It shall assemble data blocks based on signals from physical entities. It shall transfer these data blocks to a proximity network, as shown in Figure 9.

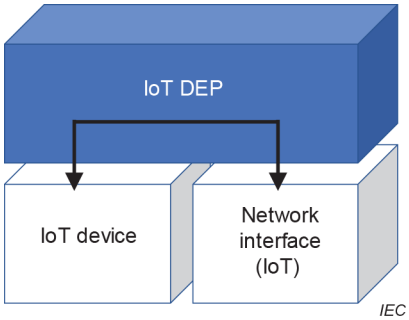

Figure 9 – Operations of an IoT DEP in Case D

8 Requirements for an IoT DEP

8.1 General

The IoT DEP shall comply with the requirements described in Clause 8. In Clause 7, four applied cases of an IoT DEP are specified. Requirements described in Clause 8 are applied to all cases unless otherwise specifically noted. Architecture for implementation in each case on IoT DEP shall be in accordance with Annex A.

8.2 Requirements of functional blocks

8.2.1 Definitions of functional blocks

Figure 10 shows the functional blocks of an IoT DEP. Each block shall be applied according to Table 1.

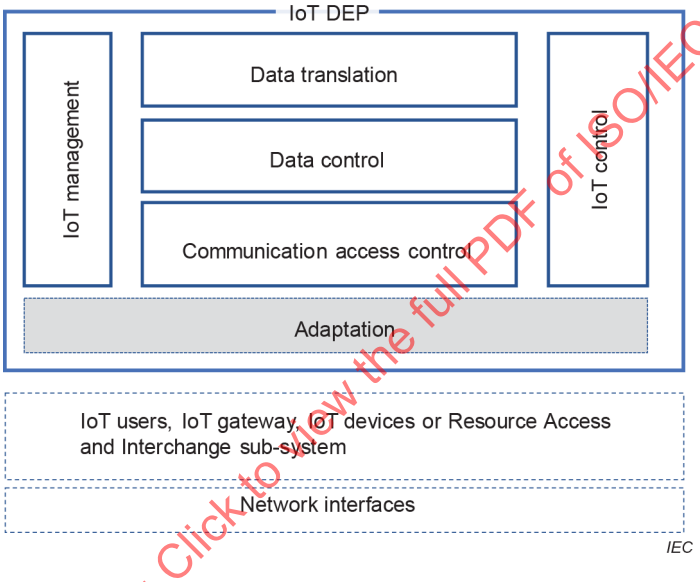

Figure 10 – Functional blocks in an IoT DEP

Table 1 lists all the functional blocks in an IoT DEP. This table clarifies the relationship between functional blocks and applied cases. For example, Case A does not require data control and data translation because an IoT DEP in Case A is located at the edges of the services. Case D does not require data control because an IoT DEP in Case D is located at the connecting point with the devices. However, this case shall include data translation because an IoT DEP assembles signals from the devices to data blocks. In the other cases (i.e. Case B and Case C), all blocks shall be included because an IoT DEP in these cases shall operate as nodal points.

Table 1 – Relationship between functional blocks and cases of an IoT DEP

Blocks	Case A	Case B	Case C	Case D
Communication access control	X	X	X	X
Data control		X	X	
Data translation				X
IoT control	X	X	X	X
IoT management	X	X	X	X
Adaptation	X	X	X	X

8.2.2 Communication access control (CAC)

Communication access control (CAC) shall provide protocol processing for IoT applications, as shown in Figure 11.

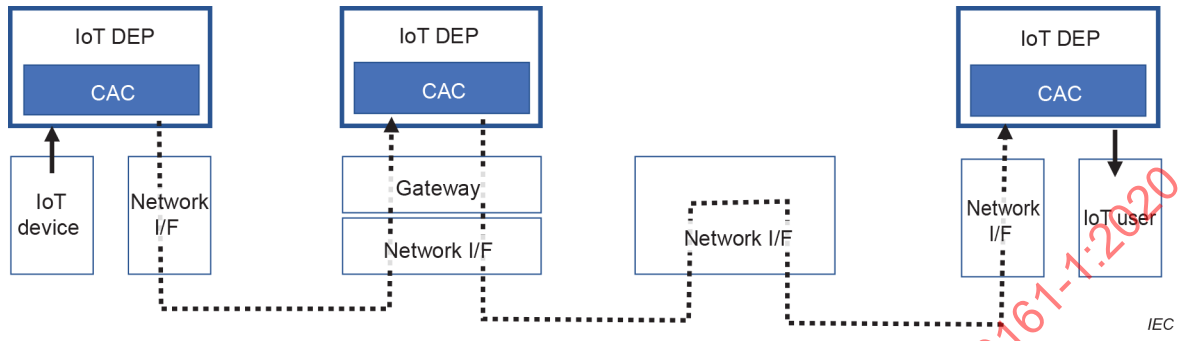

Figure 11 – Functional blocks in an IoT DEP

As shown in Figure 11, at the end points, the CAC in an IoT DEP shall translate between the row data from/to the IoT devices or IoT users and data blocks. At the nodal points, the CAC shall transfer these data blocks to other CACs, independent of the lower-layer protocols and transmission media. The CAC has three requirements as follows.

1) First, a large number of data blocks from/to the sensors and actuators shall be controlled in the CAC block. This communication control will simplify the operations (e.g. realizing small overheads and simple communication sequences). New network technologies can be applied in this control; a promising candidate is the ICN, which is summarized in Annex B. In ICN technologies, simple communication sequences with small overheads are performed because it is not necessary that physical addresses are discovered from transfer information. For example, in the current Internet, IP addresses are discovered by the DNS. However, in ICN technologies, this discovery process is not required. The CAC block shall be applied to all cases: Cases A, B, C and D.
2) Next, an IoT DEP is positioned as an application layer protocol, as shown in Figure 12. Therefore, the CAC shall be adapted between the IoT applications and lower layers, as shown in Figure 13. It shall also abstract the lower-layer protocols. In IoT applications, various networks can be deployed for data transportation. The CAC shall be independent of IoT applications, and shall not investigate or modify content in these data blocks of IoT applications. Although detailed secure mechanisms can be specified, they are beyond the scope of this document.

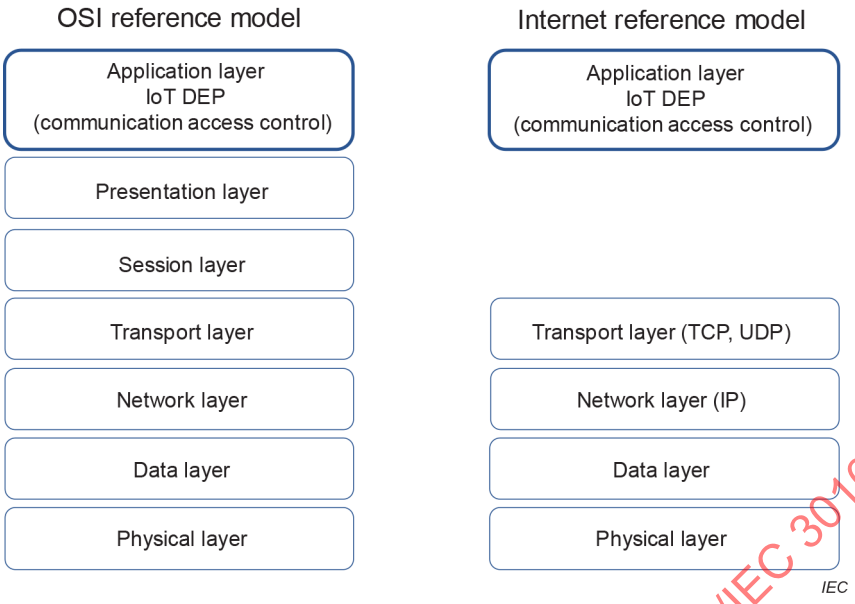

Figure 12 – Layer structures of the communication platforms

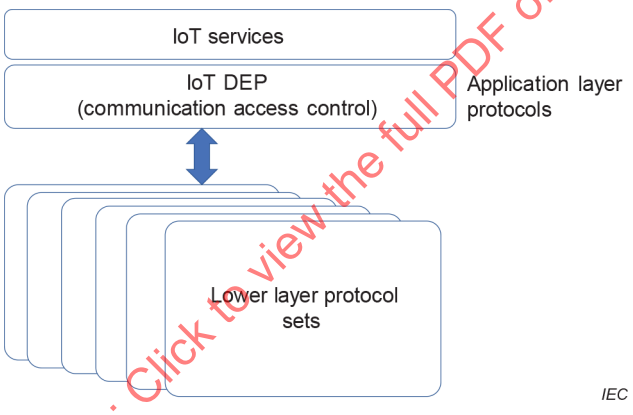

Figure 13 – Independence between CAC and lower layer protocols

3) Lastly, an IoT DEP shall provide a co-existence between IoT applications and other applications, if other applications are deployed. The co-existence architecture is shown in Figure 14.

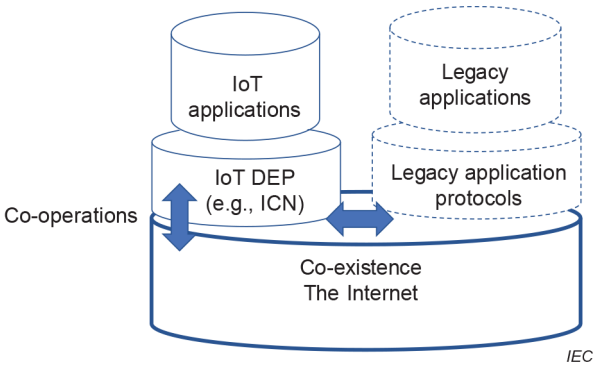

Figure 14 – Co-existence architecture between IoT applications and other applications

IoT applications and legacy applications can be operated in parallel on the Internet as shown in Figure 14. IoT applications and other applications can be operated in parallel. The CAC shall not request modifications of the Internet if this infrastructure is deployed. The CAC shall operate over the interfaces of the transport layers (e.g. TCP or UDP), and isolate IoT applications from other applications using certain technologies such as virtualization technologies.

8.2.3 Data control

Data control caches data in networks to mitigate traffic flows due to the retransfer of the same data. Data control reduces the traffic volume in networks. It shall be installed at nodal points (i.e. Cases B and C).

8.2.4 Data translation

Data translation shall assemble data blocks from the bit streams of IoT devices (e.g. sensors). It shall be installed in Case D.

8.2.5 IoT control

IoT control shall provide operating parameters for the CAC and shall monitor the operating status. It shall manage route transfers of IoT applications in networks. It shall be deployed for all cases.

8.2.6 IoT management

IoT management shall monitor failures of the IoT DEP and communication routes between an IoT DEP and the other IoT DEP.

8.2.7 Adaptation

It is assumed that an IoT DEP is operated over the transport layer in the protocol stack described in 8.3. However, in other cases, the network layer or lower layers are connected to an IoT DEP through this function. This adaptation function depends on the implementations of an IoT DEP.

8.3 Communication protocols

The requirements of an IoT DEP are specified from the communication protocol viewpoint. An IoT DEP shall be positioned as the upper layer of communication protocols (i.e. an application layer protocol, as shown in Figure 15). If it is operated over the transport layer, it shall be connected to the transport layer protocols (i.e. TCP and UDP) through conventional sockets. If it is not operated over the transport layer, the lower layers shall be adapted to an IoT DEP through the adaptation function.

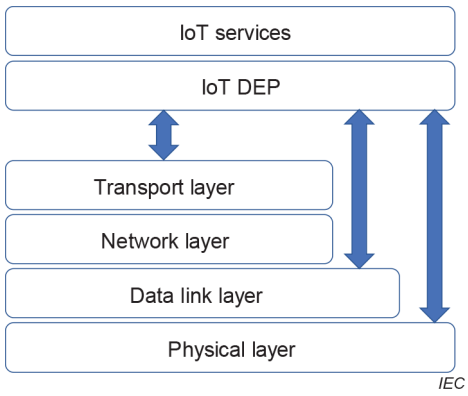

Figure 15 – IoT DEP connections over communication protocols

8.4 Service mapping

An IoT DEP shall provide efficiency in information delivery without investigation and modifications of information-related services. An IoT DEP shall process information from/to the lower layers independent of user services.

An IoT DEP is physically positioned as shown in Figure 16. To deploy services in various use cases, an IoT DEP shall abstract the network configuration, protocols, and services. If an IoT DEP is not deployed, the operations will be complicated, as shown in Figure 17.

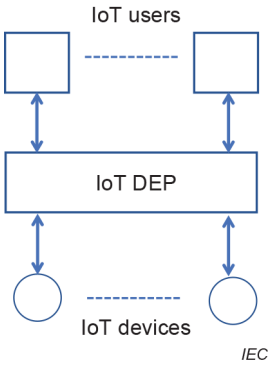

Figure 16 – Connections between IoT users and IoT services with an IoT DEP

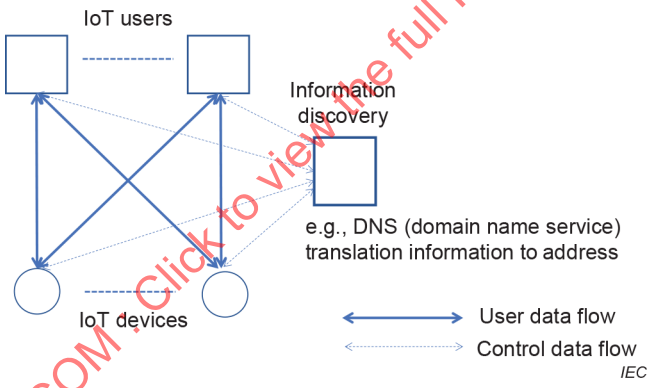

Figure 17 – Connections between IoT users and IoT services without an IoT DEP

9 Operations of an IoT DEP

The generic operations of an IoT DEP are described in 1) to 4) and summarized in Figure 18.

1) Pre-set transfer routes

   When users subscribe to an IoT application, the transfer routes among an IoT DEP are established by IoT management.

2) Data collection request

   When IoT users collect data from IoT devices, a request message is transferred to the IoT DEP in networks using preset routes. In this operation, the DNS is not required, although it is mandatory for the Internet. In cases of multiple pre-set routes, an IoT DEP resolves the route selection. The IP and its related protocols are isolated from this operation.

3) Data transfer

When an IoT device transfers data, it transfers data to the IoT DEP in the networks discussed in 2). The IoT DEP can cache data. Subsequently, when an IoT user requests a data transfer, an IoT DEP transfers data in a cache instead of an IoT device. ICN technologies are applied to data transfer mechanisms. These technologies are described in Annex B.

4) Data access schemes

In operations 2) and 3), two detailed schemes are applied.

Synchronized scheme: Interest/data sequences in the CCN, which is a type of ICN, are applied. Interest message is applied to request data collection. Data message is applied to transfer data corresponding to interest message. Interest/data sequences are paired.

Asynchronized scheme: Publication/subscription sequences in MQTT, which is a type of ICN and also a family of the ICN. Subscription message is applied to obtain data. Publication message is applied to data transfer. These messages are invoked independently. An IoT DEP shall manage the relationship between these messages according to IoT applications.

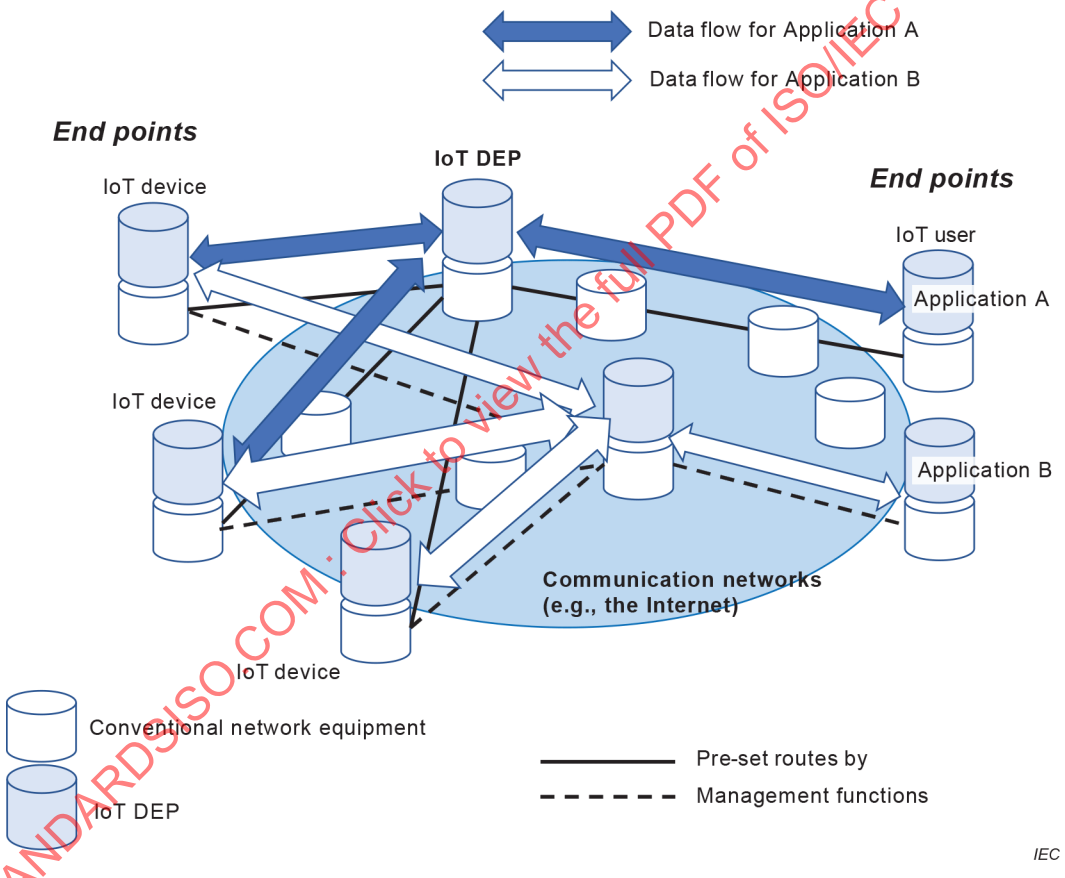

Figure 18 – Operation of information control using an IoT DEP

Annex A
(normative)

Implementation guideline for an IoT DEP

A.1 General

Annex A provides the guidelines for interoperability in an IoT DEP defined as Cases A, B, C, and D. Entities including an IoT DEP for communication are typically configured as shown in Figure A.1. An IoT DEP is implemented over the transport layer without adaptation. If the adaptation function in an IoT DEP is activated, the lower-layer functions can be included in IoT DEP, as shown in Figure A.2.

Annex A provides the following configurations on implementation:

– abstraction of lower layer in IoT DEP;
– internal connections in a component of IoT DEP.

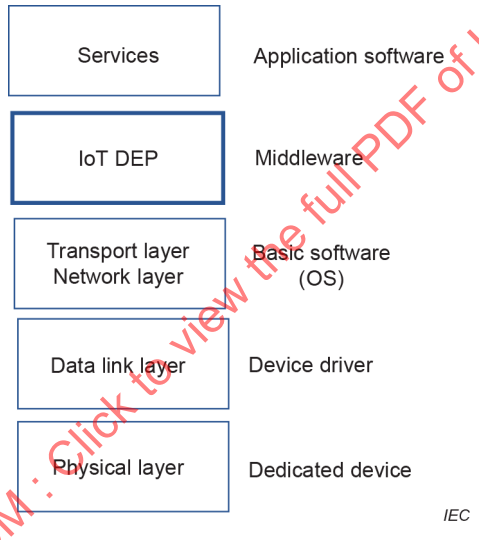

Figure A.1 – Configuration of entity including an IoT DEP without adaptation

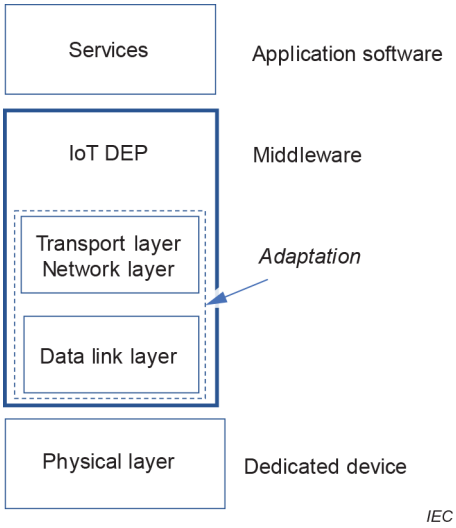

Figure A.2 – Configuration of entity including an IoT DEP with adaptation

A.2 Abstraction of lower layer in IoT DEP

When an IoT DEP is operated over the transport layer, an IoT DEP shall be connected to this layer through the socket interface specified in the TCP or UDP. This socket interface is identified by port numbers, such as newly assigned well-known ports or negotiated ports.

When the communication access control in an IoT DEP supports multiple access protocols of various ICN technologies described in Annex B, multiple ports should be assigned for the interfaces between the IoT DEP and transport layer to identify each access protocol, as shown in Figure A.3.

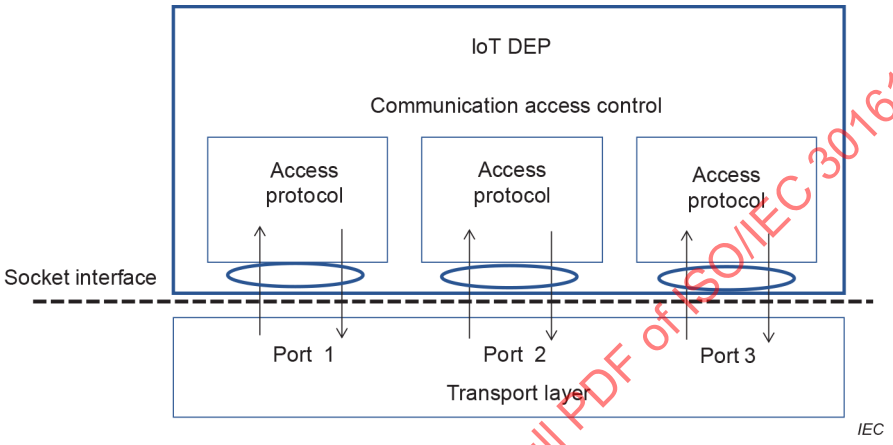

Figure A.3 – Implementation on support of multiple access protocols in an IoT DEP

When the communication capability in an IoT DEP requests different capabilities, such as transfer route, etc. to transfer information in lower layers, multiple ports should be assigned for the interfaces between an IoT DEP and transport layer to identify the transfer capabilities, as shown in Figure A.4. Port selection is invoked in the communication access control of an IoT DEP.

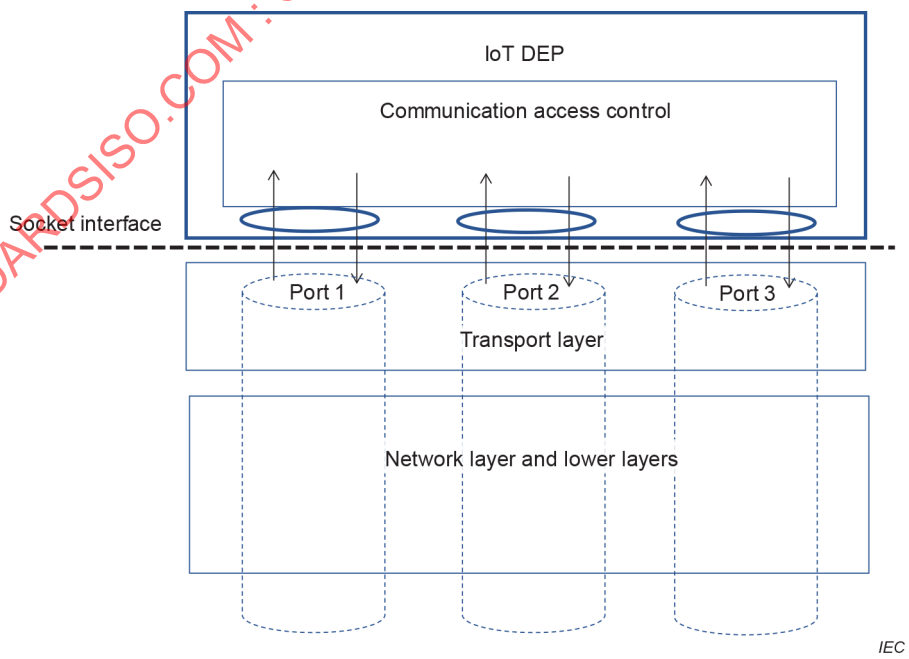

Figure A.4 – Implementation on support of multiple socket interfaces in an IoT DEP

When an IoT DEP is operated on the data link layer or physical layer, an IoT DEP should be connected to this layer through the adaptation function. The adaptation function converges various interfaces in the data link layer or physical layer to the socket interface, as shown in Figure A.5.

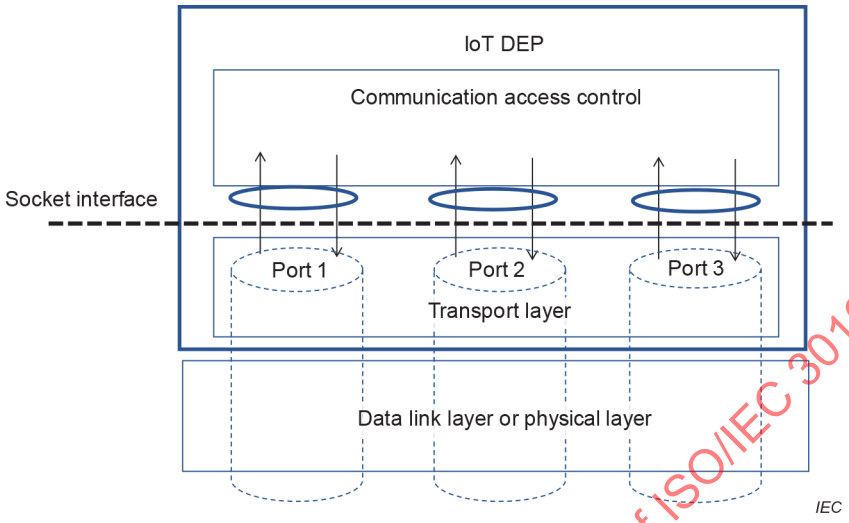

Figure A.5 – Implementation on support of multiple socket interfaces in an IoT DEP with adaptation function

A.3 Abstraction of lower layer in IoT DEP

Each function block in an IoT DEP is implemented as follows.

All the functions are implemented as middleware modules on basic software. However, the communication access control and data control blocks require assistance by hardware, because protocol processing including finite-state machines and timer, and data cache can be handled by hardware, for example, ASIC (application specific integrated circuit) or specific accelerators.

Annex B
(informative)

Typical communication protocols for ICN

Information centric network (ICN) technologies are described as an example of the data exchange platform.

ICN technologies can be categorized into four types as described in Figure B.1:

– data-oriented network architecture (DONA);
– content centric network (CCN);
– publish–subscribe Internet routing paradigm (PSIRP);
– network of information (NetInf).

Although the detailed mechanisms of these types are different, the basic concepts are the same: mitigation of overhead in Internet such as location base routing and data discovery, and reduction in traffic volume using networked cache.

PSIPR is an asynchronous architecture using publication and subscription. MQTT can be categorized into this part. Other types include synchronous architecture using data request on demand and response, which are paired. The features of these types are summarized in Figure B.1.

	DONA	CCN	PSIRP	NetInf
Namespace	Flat with structure	Hierarchical	Flat with structure	Flat with structure
Name-data integrity	Signature, PKI independent	Signature, external trust source	Signature, PKI independent	Signature or content hash, PKI indep.
Human-readable names	No	Possible	No	No
Information abstraction model	No	No	No	Yes
NDO granularity	Objects	Packets	Objects	Objects
Routing aggregation	Publisher/explicit	Publisher	Scope / explicit	Publisher
Routing of NDO request	Name-based (via RHs)	Name-based	NRS (rendezvous)	Hybrid NRS and name-based
Routing of NDO	Reverse request path or direct IP connection	Reverse request path using router state	Source routing using Bloom filter	Reverse request path or direct IP connection
API	Synchronous get	Synchronous get	Publish/subscribe	Synchronous get
Transport	IP	Many including IP	IP/PSIRP	Many including IP

Figure B.1 – Types of ICN technologies

See B. Ahlgren et al. [8]

Annex C
(informative)

Applied use cases based on an IoT data exchange platform

C.1 General

In the use cases summarized in Annex B, the most effective cases of the deployment of IoT DEP are indicated as follows.

C.2 Farm product tracking use case: Actors and information exchange

This use case is indicated in 7.5 of ISO/IEC TR 22417:2017 [1]. Figure C.1 shows the IoT system for distributing farm products to consumers safely.

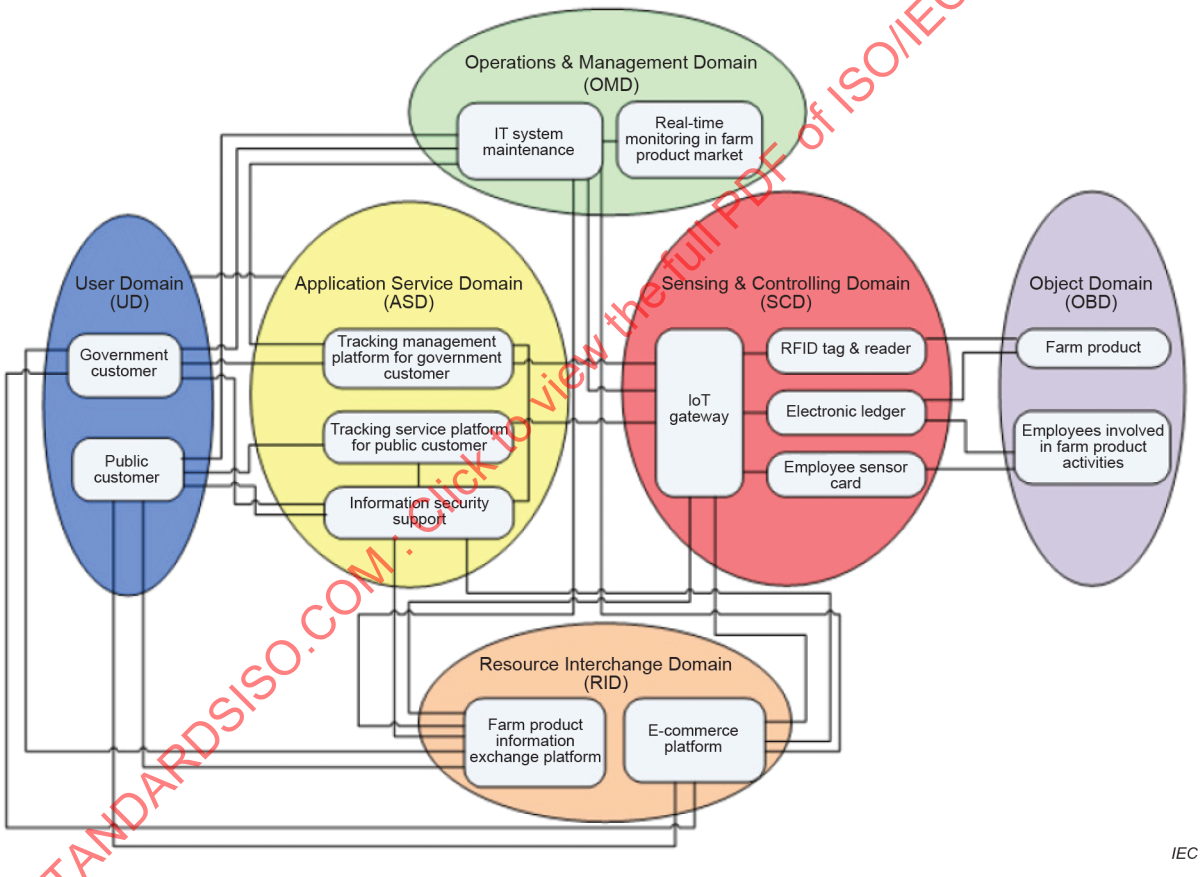

Figure C.1 – Diagram of farm product tracking system

In this case, various sensing data (e.g. RFID data with farm products, ID card data for farmers) are collected for every stage in a supply chain (e.g. producing, processing, transporting, and selling). Subsequently, centralized administrative control over the data is performed.

In this system, data are collected from different supply chains; therefore, traffic volume is increased. Various QoS are required for each type of IoT data. If these problems are solved, the development cost of this system is increased.

To address these problems, an IoT DEP is deployed to abstract networks for data collection. An IoT DEP is installed to a Sensing & Controlling Domain, as in Figure C.1.