ISO/IEC 30161-2

Edition 1.0 2023-03

INTERNATIONAL STANDARD

Internet of things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points

ISO/IEC 30161-2:2023-03(en)

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

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

ISO/IEC 30161-2

Edition 1.0 2023-03

INTERNATIONAL STANDARD

colour inside

Internet of things (IoT) – Data exchange platform for IoT services – Part 2: Transport interoperability between nodal points

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.020

ISBN 978-2-8322-6537-6

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

CONTENTS

INTERNET OF THINGS (IoT) – DATA EXCHANGE PLATFORM FOR IoT SERVICES –

Part 2: Transport interoperability between nodal points

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.

ISO/IEC 30161-2 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

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

Draft	Report on voting
JTC1-SC41/326/FDIS	JTC1-SC41/336/RVD

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

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

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

A list of all parts in the ISO/IEC 30161 series, published under the general title *Internet of Things (IoT) – Data exchange platform for IoT services*, can be found on the IEC and ISO websites.

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

INTRODUCTION

ISO/IEC 30161-1:2020 specifies the requirements of an Internet of Things (IoT) data exchange platform (IoT DEP), which transfers IoT data to and from various IoT devices with small delay. The IoT DEP provides the following functions: abstraction of communication networks and lightweight transfer of IoT traffic. However, ISO/IEC 30161-1:2020 specifies only the concept and structure of the platform for IoT data exchange between an IoT device and an IoT-user through an IoT DEP. Therefore, it is essential to take into account that IoT devices and IoT-users are connected to each other through multiple nodal points, when a large number of IoT devices and IoT-users is included in the IoT system and is deployed over a wide geographical area.

This document focuses on the transport interoperability among nodal points in an IoT system. The transport interoperability among nodal points enables data exchange among nodal points in an IoT system with small overheads or data acquisition with low latency. Requirements for efficient transfer of IoT data among nodal points are specified. Functional blocks on a nodal point for the transport interoperability between nodal points in the IoT DEP are specified.

The transport interoperability among nodal points is realized by an IoT DEP network consisting of multiple nodal points. The transfer of IoT data among nodal points is not affected by a communication protocol in the transport layer. A nodal point has routing function and forwarding function to realize the transport interoperability.

INTERNET OF THINGS (IoT) – DATA EXCHANGE PLATFORM FOR IoT SERVICES –

Part 2: Transport interoperability between nodal points

1 Scope

This part of ISO/IEC 30161 specifies the following items for the transport interoperability between nodal points in the IoT data exchange platform (IoT DEP):

- requirements;
- functional blocks;
- operation mechanism.

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 30161-1:2020, *Internet of Things (IoT) – Data exchange platform for IoT services – Part 1: General requirements and architecture*

3 Terms and definitions

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

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

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

3.1
IoT data
bit strings exchanged among IoT DEP functions

3.2
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.

[SOURCE: ISO/IEC 30161-1:2020, 3.1]

3.3
IoT DEP network
network which consists of multiple nodal points

3.4
IoT service
service which exchanges data among endpoints in an IoT system

3.5
IoT system
system providing functionalities of IoT

Note 1 to entry: An IoT system can include, but not be limited to, IoT devices, IoT gateways, sensors, and actuators.

[SOURCE: ISO/IEC 20924:2021 [1], 3.2.9]

3.6
nodal point
point that investigates routing information specified in communication protocols and relays data blocks according to such information

[SOURCE: ISO/IEC 30161-1:2020, 3.2]

4 Abbreviated terms

CAC	communication access control
IoT	Internet of Things
IoT DEP	IoT data exchange platform
IP	internet protocol
OSI	open systems interconnection
QoS	quality of service

5 Overview

ISO/IEC 30161-1:2020 specifies an IoT data exchange platform (IoT DEP), which transfers IoT data to and from various IoT devices with small delay. Such various IoT devices are described in ISO/IEC TR 22417 [2][1]. The IoT DEP suppresses processing time delay (i.e. overhead due to DNS, IP routing based on a location) and reduces traffic volume by eliminating complicated protocols used by existing communication infrastructures (e.g. the Internet). ISO/IEC 30161-1:2020 also specifies four cases of IoT DEP implementation (Cases A, B, C, and D). IoT DEP functions for Case A are implemented in an IoT-user, IoT DEP functions for Case C are implemented in an IoT gateway, and IoT DEP functions for Case D are implemented in an IoT device. Case B of an IoT DEP is specified as a component which takes on the role of a nodal point.

Figure 4 of ISO/IEC 30161-1:2020 shows the locations of IoT DEP functions in the IoT reference models of ISO/IEC 30141 [3], which indicates the relationship of IoT DEP functions among an IoT device, an IoT-user, an IoT gateway, and "Resource access and interchange sub-system" as shown in Figure 1.

When a large number of IoT devices and IoT-users is included in the IoT system and the IoT system is deployed in a wide geographical area as a horizontal approach, IoT devices and IoT-users are connected to each other through multiple nodal points in an IoT DEP network as shown in Figure 2. Note that the IoT gateway corresponds to a nodal point. IoT devices and IoT-users correspond to endpoints connected to any of the nodal points.

1 Numbers in square brackets refer to the Bibliography.

This document specifies requirements, functional blocks and operation mechanism for the efficient transfer of IoT data among nodal points in an IoT system where endpoints connect to multiple nodal points in the IoT DEP network, as shown in Figure 2. The IoT DEP network consists of multiple nodal points. IoT data exchange in an IoT system consisting of a single nodal point is specified in ISO/IEC 30161-1:2020. In this document, IoT data are exchanged among IoT DEPs, as shown in Figure 3. The IoT DEPs are implemented as middleware modules over a transport layer specified in the OSI reference model.

IoT data are transmitted and received as data blocks of IoT data between an endpoint and a nodal point or among nodal points. The bit strings that construct IoT data are composed of plural data blocks. A data block has parameters such as a data block size, a sequence number, a time stamp and a starting time.

The structure of this document is as follows.

Clause 6 includes the IoT DEP network configuration and specifies both system parameters for IoT data exchange between endpoints, and system parameters for IoT data transfer among nodal points. Clause 6 also specifies the functional requirements for the transport interoperability among nodal points. A nodal point has a routing function and a forwarding function to transfer IoT data received from an endpoint.

Clause 7 specifies functional blocks to comply with the requirements specified in Clause 6. Clause 7 also describes the relationship between those functions and the communication access control functional block of IoT DEP Case B and Case C.

Clause 8 describes operation mechanisms of a routing function and a forwarding function.

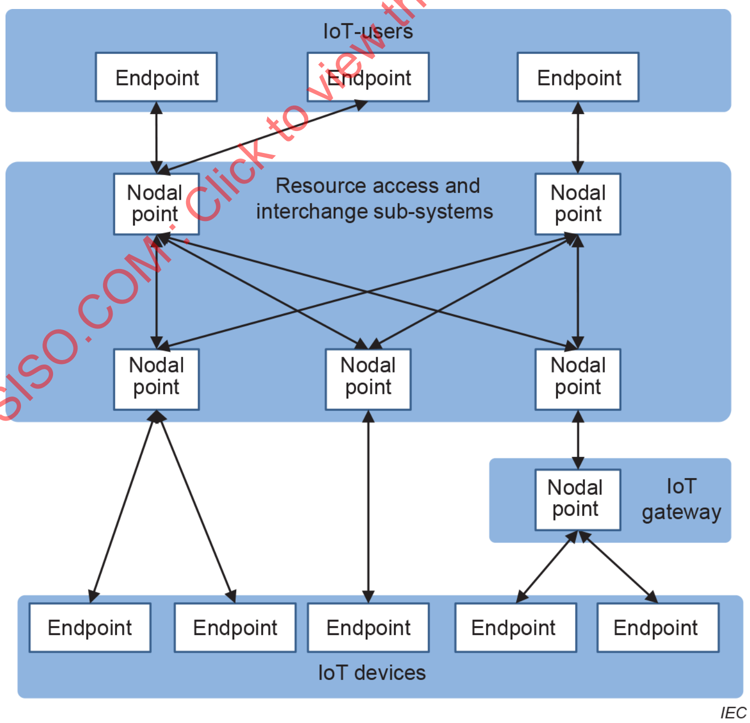

Figure 1 – Relationship with IoT Reference model

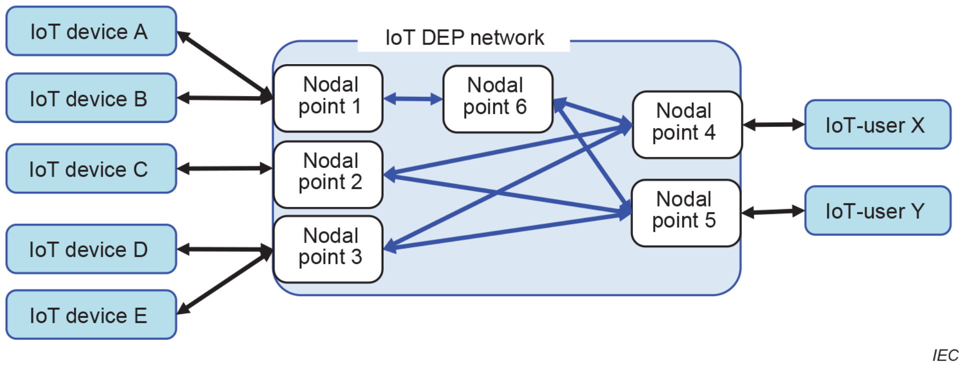

Figure 2 – IoT DEP network by multiple nodal points

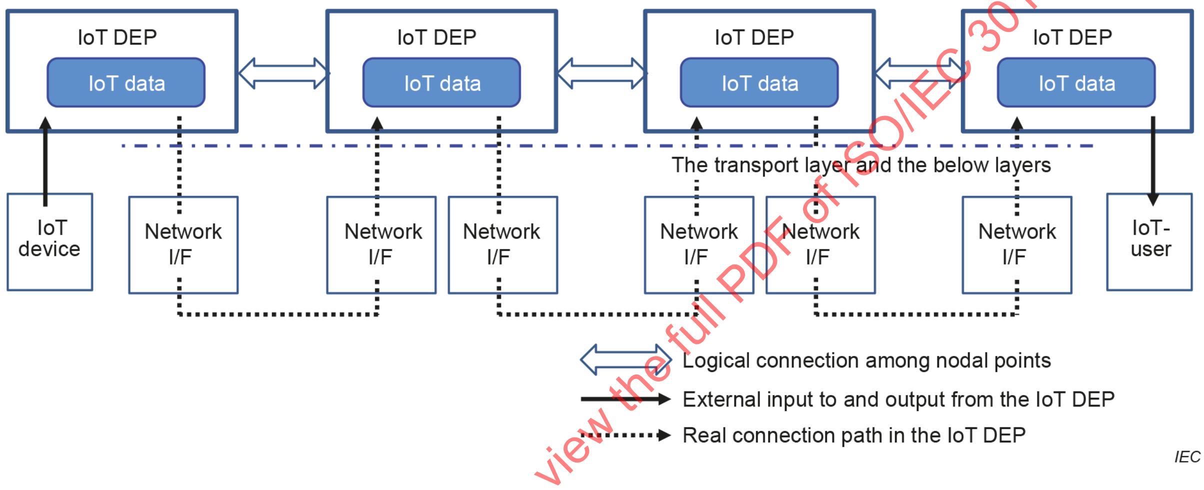

Figure 3 – IoT data exchanged among IoT DEPs

6 Functional requirements

6.1 General

This Clause 6 specifies functional requirements for the transport interoperability among nodal points in an IoT DEP network including multiple nodal points.

6.2 Transport interoperability among nodal points

The requirements and recommendations for the transport interoperability are as follows.

1) A nodal point transfers IoT data received from an endpoint to another nodal point. To transfer IoT data, a nodal point has the following functions.

   – A nodal point shall have a routing function. The routing function resolves an identifier of a next forwarding nodal point as a receiving nodal point of data blocks of IoT data, according to an identifier and attributes of the IoT data, and selects a communication path for the receiving nodal point.

   – A nodal point shall have a forwarding function to transfer IoT data according to the selected communication path.

2) In the case that IoT data need to be temporarily stored in an IoT system to provide an IoT service, an IoT DEP network provides a storage function.
   – A nodal point should have a storage function to store copies of IoT data temporarily. The storage function has the effect of reducing duplicate data transfer in response to requests from multiple IoT-users.
   – At least one nodal point in the IoT DEP network should be a nodal point with a storage function.

In order to configure an IoT DEP network, a nodal point shall provide the following functions in addition to the functions specified in ISO/IEC 30161-1:2020.

a) A nodal point takes the role of a connection point to connect endpoints to an IoT DEP network. Thus, one of the functions of a nodal point is to receive IoT data from endpoints, i.e. IoT devices or IoT-users, and another is to transfer IoT data from other nodal points to endpoints.
b) A nodal point takes the role of a relay point to transfer IoT data from endpoints or another nodal point to other nodal points. Thus, one of the functions of a nodal point is to transfer IoT data to other nodal points.
c) A nodal point takes the role of a temporary storage point to store copies of IoT data. Thus, one of the functions of a nodal point is to store copies of IoT data.

NOTE A connection point which transfers IoT data from the IoT device to the IoT-user directly is not considered as a nodal point.

Figure 4 shows functions and positions on nodal points in an IoT DEP network. Nodal points comply with the requirements specified as a), b) and c).

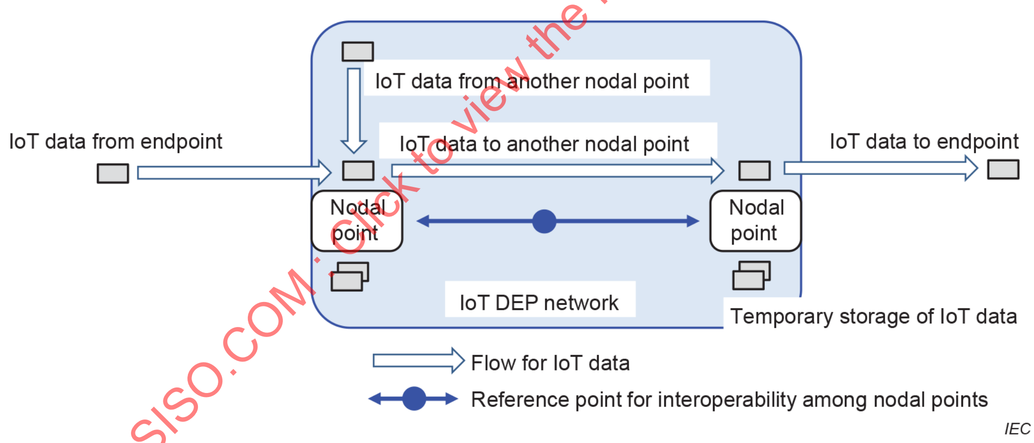

Figure 4 – Functions and positions of nodal points

System parameters for an IoT system are described in 6.3. The relationships between the IoT data exchange between endpoints and the IoT data transfer between nodal points are described in 6.4.

6.3 System parameters for an IoT system

An IoT DEP network has the following characteristics.

a) In order for the IoT DEP network to efficiently realize IoT data exchange between endpoints, it has the following functions:
   1) the function that an endpoint exchanges IoT data with other endpoints using an identifier which is used to identify IoT data;
   2) the function of temporary storage of IoT data.

b) A nodal point manages endpoints which are connected to itself by a function implemented in the IoT management functional block of the IoT DEP. The IoT management functional block is specified in ISO/IEC 30161-1:2020. To manage endpoints which are connected to the nodal point, the nodal point recognizes system parameters described in Table 1.

NOTE The detailed function of the IoT management functional block of the IoT DEP is beyond the scope of this document.

Table 1 lists the system parameters for an IoT system to carry out transfer of IoT data in the IoT DEP network. An IoT system may provide multiple IoT services.

Table 1 – System parameters for IoT system

Category	Parameters	Description and requirements
For IoT data	identifier	An identifier to indicate an IoT service of the IoT data. It is statically determined as a system parameter at the timing of starting the IoT service.
	attributes	Parameters to indicate communication characteristics of IoT data exchange between endpoints. Those parameters include information related to an IoT service. Examples of those parameters include QoS, lifetime of data, and so on. Attributes are statically assigned as system parameters at the timing of starting the IoT service.
For data block	data block size	Data length of a data block in IoT data transferred among nodal points.
	sequence number	Number which uniquely identifies the sequence in the transfer of data blocks in IoT data.
	time stamp	Time that indicates the time of a specific action such as the arrival of a data block in IoT data.
	starting time	Time when a data block in IoT data was generated.
For nodal point	identifier	An identifier to indicate a nodal point. The identifier shall be unique to an IoT DEP network. The identifier is used to transfer IoT data among nodal points.
	storage flag	A flag to indicate that it has enabled the capability to store copies of IoT data temporarily in its storage.
For endpoint	identifier	An identifier to indicate an IoT device or an IoT-user. The identifier shall be unique within an IoT system. The identifier is used to decide the destination for IoT data. A nodal point uses it to recognize endpoints which are connected to itself.

6.4 Data exchange types and data transfer types

The typical operations of the IoT DEP are specified and are summarized in Figure 18 of ISO/IEC 30161-1:2020. Figure 5 shows the IoT data exchange between endpoints and the IoT data transfer between nodal points.

The data exchange type in the short observation period is one of the following three types.

– Type A is a type with a sequence that begins with IoT data by notification from an IoT device to an IoT-user.

– Type B is a type with a sequence that begins with IoT data corresponding to request from an IoT-user, and IoT data corresponding to response to the IoT-user from the IoT device or the nodal point that stores copies of IoT data.

– Type C is a type with a sequence that begins with IoT data by command from the IoT-user to the IoT device.

For example, in the case that sensors send the sensed data as IoT data periodically, it corresponds to Type A. In the case that sensors send the IoT data by the request command from an IoT-user, it corresponds to Type B. In the case that actuators perform their function according to IoT data by the action command from an IoT-user, it corresponds to Type C. An IoT system achieves its functionality by the combination of these three types of IoT data exchange. As mentioned later, there are some cases interposed by temporary storage as a variation in Type B.

The IoT data transfer types are classified into the following two types: Type 1: request-based transfer and Type 2: data-based transfer.

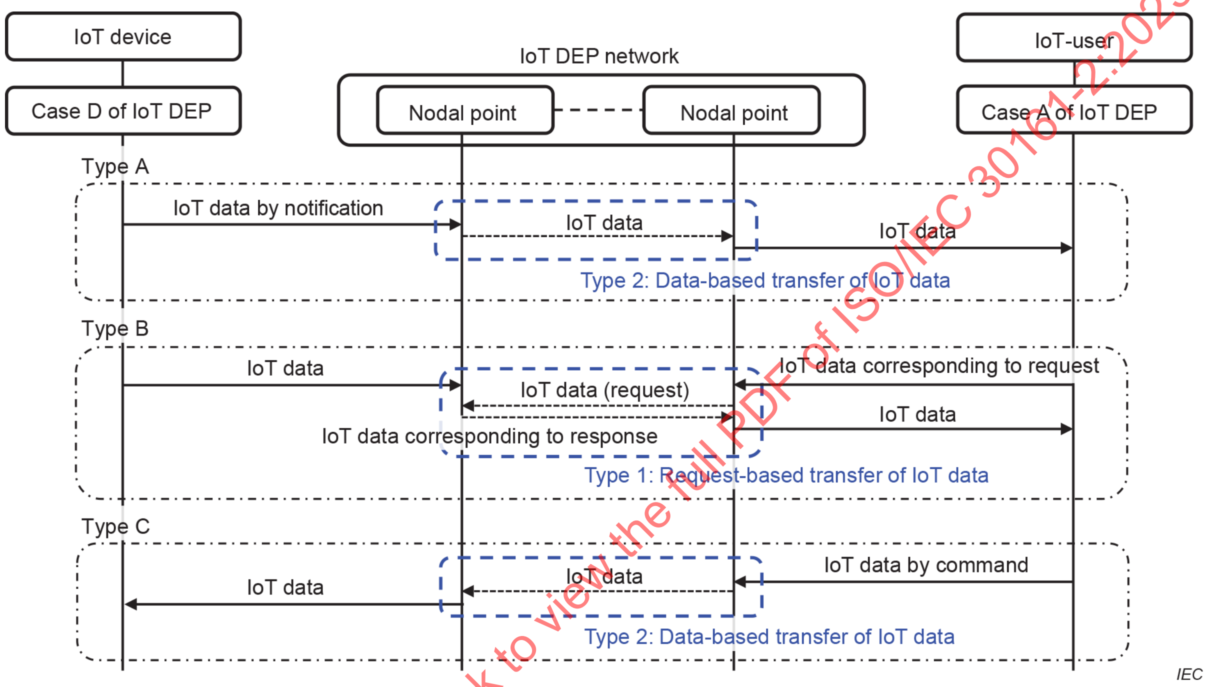

Figure 5 – Data exchange types and data transfer types

7 Functional sub-blocks

7.1 General

Clause 7 specifies functional blocks that satisfy the requirements in an IoT DEP network specified in Clause 6. Specifically, functional sub-blocks in the communication access control (CAC) functional block of Case B and Case C of the IoT DEP are specified. The CAC functional block of the IoT DEP is specified in ISO/IEC 30161-1:2020.

7.2 Definitions of functional sub-blocks

Functions that provide protocol process to realize the transport interoperability among nodal points are implemented as sub-functions of the CAC functions implemented in Case B and Case C of the IoT DEP.

Figure 6 shows in more detail the functional blocks of Figure 10 of ISO/IEC 30161-1:2020. It shows three functional sub-blocks newly defined in the CAC. The data transportation functional sub-block is a functional sub-block that provides protocol process for data exchange between endpoints that is specified in 8.2.2 of ISO/IEC 30161-1:2020. The interworking functional sub-block, the interoperability management functional sub-block, and the interoperability control functional sub-block are related to realize the transport interoperability. Received IoT data are notified from the adaptation block to the CAC block. In the CAC block, IoT data are notified to the interworking functional sub-block, and copies of IoT data are notified to the interoperability control functional sub-block.

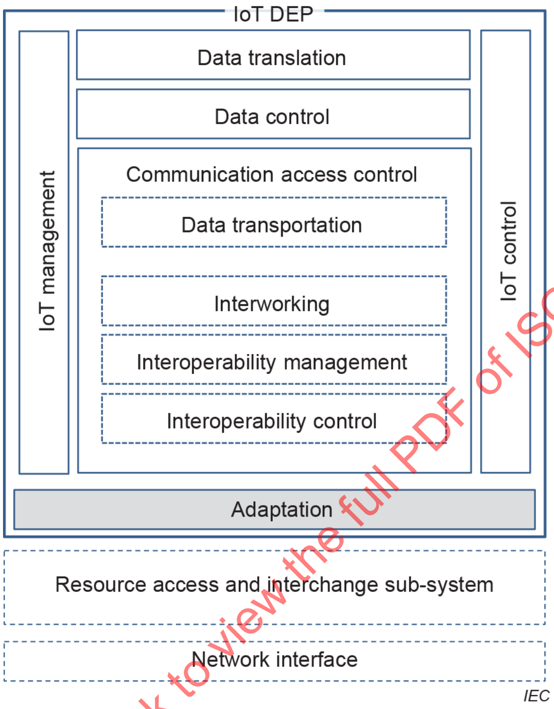

Figure 6 – Detailed functional blocks with functional sub-blocks in IoT DEP

7.3 Interworking functional sub-block

7.3.1 General

The Interworking function provides protocol process for transferring IoT data among nodal points in the IoT DEP network. This sub-block shall include a routing function and a forwarding function. As an example, the following shows the capabilities of the routing function and the forwarding function.

7.3.2 Routing function

The routing function has the following capabilities:

a) to extract the identifier and attributes of IoT data received from an endpoint or another nodal point;

b) to resolve an identifier of a next forwarding nodal point toward a receiving nodal point of the IoT data according to the parsed identifier and attributes of the IoT data;

   The resolution process of the identifier of the next forwarding nodal point is taken on one or more of the following methods:

   1) static assignment of identifiers of nodal points determined from pre-defined table by each identifier of IoT data;

   2) dynamic assignment by a discovery protocol for identifiers of nodal points resolved by an identifier of IoT data.

c) to discover possible plural communication paths to the resolved next forwarding nodal point;

d) to select one or more communication paths among the discovered communication paths according to attributes of IoT data.

The process to discover communication paths to a nodal point is selected from one or more of the following methods:

1) static configuration of communication paths to a nodal point;

2) periodic discovery of communication paths to a nodal point;

3) on-demand discovery of communication paths to a nodal point. The demand is generated by the trigger of receiving IoT data from an endpoint or receiving a request for IoT data from other nodal points;

4) broadcasting the received IoT data to other nodal points.

   This method can be used with a mechanism to avoid loop transfer.

NOTE The detailed operation of the discovery protocol for an identifier of a nodal point is beyond the scope of this document.

7.3.3 Forwarding function

The forwarding function has the following capabilities:

a) to transfer IoT data to another nodal point using the selected communication paths;

   The transfer process of IoT data is selected from one or more of the following cases according to the attributes of IoT data.

   1) At most once delivery: a data block in IoT data is transferred to another nodal point according to the capabilities of the transport layer. No response is sent by the receiver, and no retry is performed by the sender. A data block in IoT data arrives at the receiver either once or not at all.

   2) At least once delivery: this transfer method ensures that a data block in IoT data arrives at the receiver at least once by means of acknowledgment from the receiver.

   3) Exactly once delivery: this transfer method is useful when neither loss nor duplication of a data block in IoT data is acceptable. The receiver acknowledges the receipt with a two-step acknowledgement process.

   4) Other specific methods: a data block in IoT data is transferred to other nodal points by way of a system-specific transfer method.

   The transfer process uses the sequence number or time stamp of a data block in IoT data block. The sequence number is utilized for reordering the received data blocks in IoT data on a receiving nodal point. Time stamp is utilized for discard of the received data blocks from the IoT DEP network when the lifetime of the received data block in IoT data expires. The transfer process of IoT data operates independently of a communication protocol in the transport layer.

b) to decide the timing at which a nodal point transfers the IoT data to another nodal point.

   The decision process of transfer timing is selected from one of the following items according to the attributes of IoT data:

   1) the timing when a nodal point receives IoT data from endpoints;

   2) the timing when a nodal point receives a request from another nodal point to send IoT data in its temporary storage;

   3) the timing of starting the IoT service.

7.4 Interoperability management functional sub-block

The Interoperability management function provides a monitoring process for the communicable status of nodal points. This sub-block shall have the capability to detect the blockage of the communication capability of other nodal points.

7.5 Interoperability control functional sub-block

The Interoperability control function provides a storage process to store copies of IoT data temporarily. To realize the process, this sub-block shall have the capabilities to store copies of IoT data temporarily according to IoT services.

The control mechanism to control the storage process for each data block in IoT data is selected from one or more of the following mechanisms according to the attributes of IoT data and a predetermined policy by the IoT service:

1) to replace an old data block in IoT data with a newly received data block in IoT data at excess of the storage capacity;
2) to invalidate data blocks in IoT data that are stored for more than the latency-tolerant period in the case of IoT data which are exchanged on latency-critical IoT services;
3) to overwrite a copy of the stored IoT data with the latest data block in IoT data in the case that an endpoint sends data blocks in IoT data periodically;
4) other specific mechanism.

NOTE The latency-tolerant period is derived based on time constraints in the case of IoT data which are exchanged on latency-critical IoT services.

8 Operation mechanism

8.1 General

As shown in Figure 5, there are two IoT data transfer types among nodal points: request-based transfer and data-based transfer. From the viewpoint of discovering communication paths in the IoT DEP network, there are two methods: static configuration and dynamic discovery, as mentioned below.

This Clause 8 describes operation mechanisms of a routing function and a forwarding function. The operation mechanisms consist of transferring IoT data among nodal points depending on the IoT data transfer types and discovering communication paths in the IoT DEP network. A nodal point determines the IoT data transfer type according to the attributes of IoT data. By coordinating nodal points in the IoT DEP network with each other, the IoT DEP provides data exchange among nodal points with small overheads or with low latency.

Examples of services with low latency are shown in Annex A.

Temporary storage of IoT data at a nodal point affects IoT data exchange delay between endpoints. Therefore, for provision of latency-critical IoT services, it is necessary to consider the temporary storage operation at a nodal point. Temporary storage operation at a nodal point is described in Annex B according to the requirements of IoT service, for example, latency-critical IoT services. Rec. ITU-T Y.3033 [4] and Rec. ITU-T Y.3071 [5] are examples of usage for temporary storage.

Table 2 shows the classification of operations of transferring IoT data among nodal pints in this Clause 8.

Table 2 – Classification of operations of transferring IoT data among nodal points

IoT data transfer Types among nodal points	Methods of discovering communication paths in the IoT DEP network	
	Static configuration	Dynamic discovery
Request-based transfer	Case 1	Case 2
Data-based transfer	Case 3	Case 4

8.2 Request-based transfer by static assignment

In Case 1, the requested nodal point transfers IoT data from its temporary storage to a requesting nodal point according to one or more configured communication paths when a nodal point receives a request for IoT data from another nodal point.

In this operation, the storage function at the requested nodal point has the effect of reducing duplicate data transfer in response to requests from multiple IoT-users.

8.3 Request-based transfer by dynamic discovery

In Case 2, the requested nodal point transfers IoT data from its temporary storage to a requesting nodal point when a nodal point receives a request for IoT data from another nodal point.

A nodal point discovers communication paths to a requesting nodal point according to attributes of IoT data by the dynamic discovery process. There are two methods of dynamic discovery process: periodic discovery and on-demand discovery.

In the case of the periodic discovery method, although the IoT data in an IoT DEP network increases by periodic discovery, the time to discover the requesting nodal point is shortened.

On the contrary, in the case of the on-demand discovery method, the IoT data to discover the communication path to a nodal point is reduced.

8.4 Data-based transfer by static assignment

In Case 3, a nodal point transfers IoT data to another nodal point, which connects itself to a destination endpoint of IoT data, when the nodal point receives IoT data from endpoints. The nodal point uses configured communication paths to transfer IoT data.

In Case 3, the latency is reduced because IoT data are transferred to nodal points to which the endpoint connects, as soon as a nodal point receives IoT data from an endpoint which generates IoT data.

Broadcasting IoT data from an endpoint to other nodal points without a discovery process is included in Case 3.

8.5 Data-based transfer by dynamic discovery

In Case 4, a nodal point transfers IoT data to another nodal point, which connects itself to a destination endpoint of IoT data, when the nodal point receives IoT data from endpoints.

A nodal point discovers a communication path to a nodal point, which connects itself to a destination endpoint of IoT data, according to attributes of IoT data by the dynamic discovery process. There are two methods of dynamic discovery process: periodic discovery and on-demand discovery.

Annex A
(informative)

Latency-critical IoT services

According to the advances in communication technologies, in addition to classic IoT services, low latency and high reliability are extremely important communication requirements for many IoT use cases. In this Annex A, latency-critical IoT services are introduced, and the communication requirements are shown in Table 1 of P. Schulz et al. [6]. The reliability requirements for factory automation applications are typically 10^{-9} packet loss rate (PLR), while the latency requirements vary from 0,25 ms to 10 ms.

Annex B
(informative)

Storage strategy for latency-critical IoT services at a nodal point

B.1 General

A nodal point provides temporary storage capacity. However, temporary storage of IoT data at a nodal point affects latency for IoT data exchange between endpoints. This Annex B describes operation of temporary storage at a nodal point according to the requirements of IoT service, especially an operation by latency-tolerant period on latency-critical IoT services.

B.2 Operation for latency critical IoT services

In latency-critical IoT services which have time constraints until IoT data generated by an endpoint are transferred to other endpoints, the endpoint that requires IoT data must receive IoT data within the constrained time, called a latency-tolerant period. Therefore, the nodal point, which receives data blocks in IoT data in the latency-critical IoT service from the endpoint, should transfer the received data blocks in IoT data to other nodal points within the constrained time. The nodal points, which the corresponding IoT data are transferred to, are registered in advance by the endpoints that require the corresponding data in IoT data. In this case, the time stored in the temporary storage of data blocks in IoT data at nodal point should be within the latency-tolerant period allowed by the latency-critical IoT service, and a data block in IoT data should be discarded from the temporary storage when the time stored in the temporary storage of the corresponding data block in IoT data exceeds the latency-tolerant period. If the latency-tolerant period is set to 0, it corresponds to the operation of discarding without storage.

Figure B.1 describes an assignment process of latency-tolerant period to each nodal point according to declaration of a time constraint from an IoT DEP user. An IoT DEP operator derives a latency-tolerant period at each nodal point from declaration of a time constraint by the IoT DEP user, and assigns the derived latency-tolerant period to each nodal point.

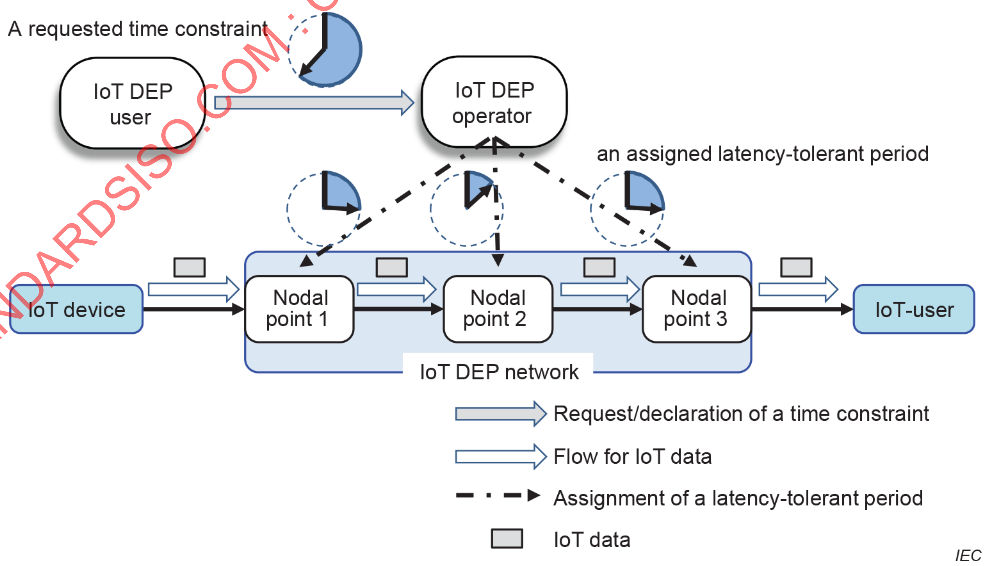

Figure B.1 – Assignment process of latency-tolerant periods