Technical Specification

ISO/TS 7344

Short-range wireless sensor to device communication

Communication courte portée pour transfert de données entre capteurs et relais embarqués

First edition
2024-03

Reference number
ISO/TS 7344:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 104, *Freight containers*, Subcommittee SC 4, *Identification and communication*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The use of wireless communication has expanded globally thanks to new wireless standards and very low-cost transceiver chips and modules. However, there is a need to specify the use of open protocols and intended behaviour in diverse use cases, to allow compatibility of hardware from different origins. Wireless communication capability has become an easy and relatively low-cost addition to almost any Internet of Things (IoT) device in transport and logistics, where a wireless feature can enhance performance, convenience, and/or marketability. In the machine-to-machine communication space, remote keyless entry (RKE) and remote pairing are the most widespread. A wireless temperature sensor within a cargo container, for instance, can transmit temperature updates to the IoT device, which serves as a gateway to the Internet, thus providing "near real-time" temperature monitoring for sensitive cargo. When choosing a communication technology between the measuring sensor and the IoT device in one environment, e.g. a freight container, the operational context plays a crucial role, i.e. container design, distance from sensor to IoT device, location of both on/in a container and communication protocols that support these hardware items.

NOTE So-called "real-time" is mainly used as a commercial term. Due to the limitation of the technology to transmit data non-stop, in order to manage the battery lifetime expectation, connectivity with cloud computing is done in defined periodical intervals, e.g. every 5 min, 15 min, 1 h or similar. Therefore, from a technical point of view, this reference is related to "near real-time".

ISO/TS 18625 provides guidance for a system and its enabling devices, used to track, monitor and/or report the status of the container. Based on existing technology, ISO/TS 18625 defines three levels (Tier 0, Tier 1 and Tier 2) of capabilities for a container tracking device (CTD) to be matched with the needs of the users (e.g. a shipper, a consolidator, a logistic service provider and more).

This document refers to CTD as described in Tier 2 of ISO/TS 18625 (reporting without a reader using technologies such as satellite or cell phone) and CTD's "local" communication within one environment to dependent wireless sensors. Being in one environment, the expected wireless communication between sensors and a CTD can be short-range, however it needs to withstand conditions prescribed by the purpose of such technical application. Therefore, a choice of the applicable technologies is directly related to the types of sensors and measurements they make, container configuration, location of the receiving device, size of the message and minimal sending interval.

Short-range wireless technology refers to the technology that can communicate wirelessly within a smaller diameter region. Short-range wireless communication technology has a considerable application prospect in the field of container equipment and management. Short-range wireless communication technologies are NFC, wireless network protocols based on the IEEE 802.11 family of standards, such as IEEE 802.15.4 based specifications for Bluetooth®[1)], for example.

This document describes existing wireless technology on sensor to telematic device communication and defines a list of those communication types which can be perceived as "open protocols", non-proprietary license free technology. Non-proprietary technology implemented on both "ends", sensor and devices/gateway, enables diversity in manufacturing origin of wirelessly communicating active hardware items within one container environment. Therefore, this document specifically focuses on wireless and short-range communication. The goal of this document is to enable interoperability among different IoT/telematic hardware manufacturers and encourage the diversification of the applicable to the CTU environment digital solutions. The anticipated effects and benefits are as follows:

— diversification of connected products available for short-range communication within one container environment;

— interoperability between hardware items of different origin, used and applied to one freight container;

— improved safety of freight container and quality of the transported goods through digital supervision and monitoring of the transportation conditions;

1) Bluetooth is the trademark of a product supplied by the Bluetooth Special Interest Group. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO/IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

— improved transparency of freight container transportation condition among the modalities of the supply chain.

Short-range wireless sensor to device communication

1 Scope

This document specifies short-range wireless active communication between two active IoT/telematic hardware items, such as a gateway device and/or a sensor.

NOTE Active hardware item in this document refers to devices and sensors, which have capacity to record and transmit measurements, i.e. data, without external activation through extra accessories, e.g. readers or scanners.

The application of such communications is based on equipment and container type. This document covers the following:

— wireless technology choices for wireless communication involving active hardware items, i.e. sensor to device communication;

— critical design factors of containers and hardware items intended to be used within one container environment;

— parameters for open protocol communication and possible applications (use cases).

This document does not define installation locations for devices and sensors; however, it is expected that the hardware items are installed on or in the container, based on the following considerations:

— existing regulations and standards;

— container design, and specification of the material it is made of;

— best possible connection, which enables interoperable communication between sensor and device;

— cargo and personnel safety.

Due to the pace of technology development, the number of connected sensors to one gateway device are not defined in this document. This document assumes that at least one sensor can be connected to at least one gateway device wirelessly.

2 Normative references

There are no normative references in this document.

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:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
Internet of things hardware
IoT hardware
entity (device) of an IoT system that communicates with other devices and systems over the Internet or other communication systems

Note 1 to entry: It can have sensors or actuators incorporated or interact with other entities.

3.2
container tracking device
CTD
device, attached to an integral part of a container, powered by an embedded battery or external source of power

Note 1 to entry: A CTD can communicate with back-end systems (e.g. cloud computing) over the Internet or other communication systems.

Note 2 to entry: A CTD can have the ability to communicate with other devices, process data and relay messages between back-end and connected devices, in which case it becomes a gateway.

Note 3 to entry: A CTD can also have sensors or an actuator incorporated on its own.

3.3
sensor
measuring instrument which detects or measures a physical property and can convert the signal for further processing or transmission

3.4
short-range wireless communication
communication between two or more devices within a local wireless network

3.5
container environment
space limited by one container entity, including internal space, i.e. cargo cavity, its structure, embedded technology and external installations, i.e. vents, devices or sensors attached to the exterior, locks and seals

4 Abbreviated terms

BLE	Bluetooth® low energy
CTD	container tracking device
CTU	cargo transport unit
IoT	Internet of Things
ISM frequency band	industrial, scientific and medical frequency band
ITU	international telecommunication union
NFC	near field communications
WiFi	wireless fidelity

5 General information

5.1 General requirements

Type and technical requirements of the proposed communication shall conform to the declared goal of the specification: non-proprietary nature of the layout. The proposed communication shall fit the container

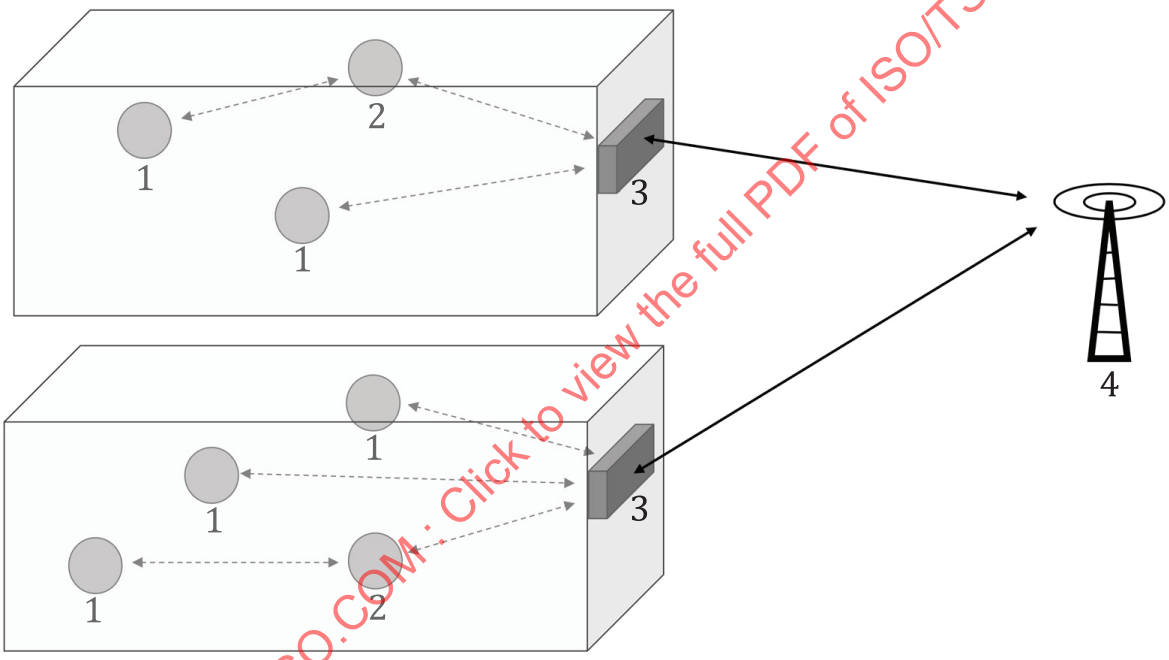
environment and guarantee wireless connectivity between externally and internally fitted container IoT hardware.

5.1.1 Unlicensed frequency spectrum definition

Technical requirements of the proposed communication shall conform to the globally accepted unlicensed radio frequencies to avoid interruptions of local and public infrastructure of the container transportation. This document refers to 2,4 GHz ISM frequency band as globally adopted and populated in different environments. Recommendation in ITU-T K.79 characterizes the typical 2,4 GHz ISM band radiated EM environments for home, office, and commercial locations, as well as for transportation environment.

5.1.2 Wireless sensor network architecture

The nodes of a wireless sensor network consist of sensor and device. The device, that acts as a gateway to external servers, is single in a container environment. The external connection of a device is out of scope of this document. It is supposed to be over cellular links or other long-range communication. The wireless sensor network of a container is independent of wireless sensor networks of other containers, even if they are on the same frequency band (see Figure 1).



Key

1 sensor device
2 relay/sensor device
3 gateway device
4 long range communication network

Figure 1 — Example of two independent wireless sensor networks with external long-range connection

In regard to security, the gateway device is responsible for the connectivity and communication to the cloud computing. There is no direct communication from sensor to the cloud computing.

5.2 Definition of the sensor to device communication

Three main container types, the refrigerated container (see Table 2), tank container (see Table 3) and dry container (see Table 1), can have a variety of sensors wirelessly connected to one or multiple devices, which

act as a gateway to the cloud computing database. Such a device collects the data from related sensors and transmits it to a network for further analysis.

The quality of wireless communication between a sensor (or sensors) and a device within the context of this document is determined by the distance between these items and the environment of a specific container which has both pieces installed. In addition, in cases of the communication between internally installed hardware items (sensor or device) to externally installed, a type of transported cargo and the way it is loaded can influence the quality of communication. In case of permanent installations, or installations for more than one trip, it is difficult to predict which type of cargo will be transported inside the container. The way of packing and loading can change from trip to trip as well. Therefore, this document focuses on installation location as a known parameter, which can be defined in advanced and stay unchanged.

5.2.1 Possible types of interaction between sensor and device based on installation location

Among the existing wireless communication types, the choice of communication between a sensor and the device attached to a container depends on a few parameters.

The container's shape and use cases of data collection through IoT hardware items, i.e. sensors and devices, allow wireless connection for the following installation locations:

a) internally mounted sensor to internally mounted device;

b) internally mounted sensor to externally mounted device;

c) externally mounted sensor to externally mounted device;

d) externally mounted sensor to the internally mounted device.

NOTE In case of refrigerated containers, the installation location of a device can be within the controller box [this applies to a) and d)].

A device can serve both as a gateway and as a sensor or a collection of embedded sensors collecting data with a regular and defined interval. Nevertheless, some use cases of environmental measurements and analysis require additional sensor which are "stand-alone" independent hardware items. This document refers to wireless communication between sensor and device, which requires, at least, a small source of power for such a sensor, to connect to a gateway and transmit data. Any internal mounting of a sensor inside the container shall not reduce the cargo volume and not restrict cargo stacking, securing, or handling.

Based on the sensors' type and the use cases they are serving, the size of the data transmission can be defined.

Within one CTU environment, the following short-range communication types can be recognised:

1) one gateway is connected to one sensor, in this case the sensor is a dependent hardware item (with no connection with the cloud computing);

2) one gateway is connected to one gateway, in this case both hardware items can either serve as independent items (with connection with the cloud computing), reporting on interconnection, and/or one out of two gateways can function as a relay;

3) one gateway is connected to many sensors or relays, in this case sensors are dependent hardware items.

Table 1 — Dry container

Event	Use case	Sensor measurements	Message size in bits	Minimal number of sensors
Authorized/unauthorized door opening	Door open/ close	Open/close	7	1 to 2
Unexpected temperature change inside the container	Temperature outside of the threshold	°C/°F	8 measurement 9 alarm	1
CO_2 measurement outside of the threshold	CO_2	ppm	8 to 9	1
Unauthorized loading	Loading status	Empty/full	n/a	1
Inside temperature	Temperature monitoring	°C/°F	8 measurement	1
Inside humidity	Humidity monitoring	%	7 measurement 8 alarm	1
Battery low — sensor level (sensor internal event)	Sensor battery monitoring	Battery voltage	14	n/a
Unexpected vibration amplitude (can be already embedded within the gateway design)	Vibration monitoring	mm	n/a	1
Connection to a pallet/ single trip device/3rd party hardware	Temporal gateway for 3rd party hardware	Pallet position	n/a	1

Table 2 — Refrigerated container

Event	Use case	Sensor measurements	Message size in bits	Minimal number of sensors
Authorized/unauthorized door opening	Door open/close	Open/close	7	1 to 2
Unexpected temperature change inside the container	Temperature outside of the threshold	°C/°F	9	1
CO_2 measurement outside of the threshold	A range of between 1 and 19,8 %	% or units of micromole	8 to 9	1
Unauthorized loading	Loading status	Empty/full	n/a	1
Connection to a pallet/single trip device/3rd party hardware	Temporal gateway for 3rd party hardware	Pallet position	n/a	1
NOTE In the refrigerated container example, only communication among sensors outside of the controller box wirelessly connected to the IoT gateway device are covered. The readings from the controller box are out of the scope.				

Table 3 — Tank container

Event	Use case	Device location	Sensor measurements	Message size in bits	Minimal number of sensors
Unexpected temperature change inside the container	Temperature outside of the threshold	Internal	°C/°F	9	1
Unexpected pressure change inside the container	Pressure	Internal	MP	9	1
Unauthorized loading	Loading status	External	Empty/full	n/a	1
Unexpected vibration amplitude	Vibration monitoring	External	mm	n/a	1

5.2.2 Sensor to device pairing

One of the main principles of the non-proprietary wireless communication is uncomplicated, so-called "over-air" pairing between two hardware items, independent of their origin. Nevertheless, due to data security issues, such a pairing is not automatic and should not happen in an unauthorized manner. In case a sensor and a device are from distinct manufacturers, a common protocol should be defined to align on their profiles.

Once the first pairing is executed successfully, the connection should stay uninterrupted. In case of connection lost, the previously paired device and sensor(s) should be able to restore the connection automatically.

5.2.3 Firmware updates

Firmware updates happen periodically through the gateway device. The gateway device is the main source of connectivity with the cloud computing and can include either updates related to the devices itself or the connected sensors. Any non-proprietary sensor to device wireless communication that is chosen should withstand the traffic of the updates and remain functional thereafter.

5.2.4 Periodicity of the sending interval and latency of reporting

Latency is a time delay or a time period it takes data to travel between the sender and the receiver or between a specific user action and the response (e.g. latency chain, see Figure 2).

Jitter is the deviation from true periodicity of a presumably periodic signal.

Interval/frequency relates to periodic events.