INTERNATIONAL STANDARD

ISO/IEC 18000-63

Third edition
2021-11

Information technology — Radio frequency identification for item management —

Part 63:
Parameters for air interface communications at 860 MHz to 960 MHz Type C

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Technologies de l'information — Identification par radiofréquence (RFID) pour la gestion d'objets —

ISO/IEC 18000-63:2021
https://standards.iteh.ai/catalog/standards/sist/d03c843b-b898-44fc-97c5-
91d325a40069/iso-iec-18000-63-2021

Partie 63: Paramètres de communications d'une interface radio entre 860 MHz et 960 MHz, Type C

COPYRIGHT PROTECTED DOCUMENT

Contents

Foreword

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.

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 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 or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 18000-63:2015), which has been technically revised.

The main changes are as follows:

— incorporation of the Technical Corrigendum;

— incorporation of a new sensor class for snapshot sensors.

A list of all parts in the ISO/IEC 18000 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document defines the physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), radio-frequency identification (RFID) system operating in the 860 MHz to 960 MHz frequency range. The system comprises Interrogators, also known as Readers, and Tags, also known as Labels or Transponders.

An Interrogator transmits information to a Tag by modulating an RF signal in the 860 MHz to 960 MHz frequency range. The Tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the Interrogator's RF signal.

An Interrogator receives information from a Tag by transmitting a continuous-wave (CW) RF signal to the Tag; the Tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the Interrogator. The system is ITF, meaning that a Tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an Interrogator.

Interrogators and Tags are not required to talk simultaneously; rather, communications are half-duplex, i.e. Interrogators talk and Tags listen, or vice versa.

The described backscatter radio frequency identification (RFID) system that supports the following system capabilities:

— identification and communication with multiple tags in the field;

— selection of a subgroup of tags for identification or with which to communicate;

— reading from and writing to or rewriting data many times to individual tags;

— user-controlled permanently lockable memory;

— data integrity protection;

— Interrogator-to-tag communications link with error detection;

— tag-to-Interrogator communications link with error detection;

— support for both passive back-scatter tags with or without batteries.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. ISO and IEC shall not be held responsible for identifying any or all such patent rights.Information on the declared patents may be obtained from:

Contact details
Patent Holder:
Legal Name   Atmel Automotive GmbH
Contact for license application:
Name & Department   Leo Merken, Legal Department, ATMEL Corporation
Address 2325 Orchard Parkway
Address San Jose, CA 95131 USA
Tel.   +1 408 436 4251
Fax   +1 408 487 2615
E-mail   leo.merken@atmel.com
URL (optional)
Patent Holder:
Legal Name   CISC Semiconductor Design+Consulting GmbH
Contact for license application:
Name & Department   Markus Pistauer, CEO
Address Lakeside B07
Address 9020 Klagenfurt, Austria
Tel.   +43(463) 508 808
Fax   +43(463) 508 808-18
E-mail   m.pistauer@cisc.at
URL (optional)   www.cisc.at
Patent holder:
ETRI (Electronics Telecommunication Reseach Institute)
Contact for license application:
Name & Department: Min-Sheo Choi, Intellectual Property Management Team
Address: 138 Gajeongno, Yuseong-gu
Address: Daejeon, 305-700, Korea
Tel.   +82-42-860-0756
Fax   +82-42-860-3831
E-mail   choims@etri.re.kr
URL (optional)   www.etri.re.kr
Patent Holder:
Legal Name   Impinj, Inc.
Contact for license application:
Name & Department   Chris Diorio, CTO
Address 701 N. 34th Street, Suite 300
Address Seattle, WA 98103, USA
Tel.   +1 206 834 1115
Fax   +1 206 517.5262
E-mail   diorio@impinj.com
URL (optional)   www.impinj.com

Contact details
Patent Holder:
Legal Name: Magellan Technology Pty. Limited
Contact for license application:
Name & Department: Ms Jean Angus
Address: 65 Johnston St
Address: Annandale, NSW 2038, Australia
Tel. +61 2 9562 9800
Fax +61 2 9518 7620
E-mail: license@magellan-technology.com
URL (optional):
Patent Holder:
Legal Name NXP B.V.
Contact for license application:
Name & Department Aaron Waxler – IP Licensing & Claims
Address 411 East Plumeria,
Address San Jose, CA 95134-1924, USA
Tel. +1 914 860-4296
Fax
E-mail Aaron.Waxler@nxp.com
URL (optional)
Patent Holder:
Legal Name SATO VICINITY Pty. Limited
Contact for license application:
Name & Department Mr. Hiromasa Konishi, Managing Director
Address 8 Guihen Street, Annandale, NSW 2038, Australia
Address
Tel. +61 295 629 800
Fax +61 295 187 620
E-mail hiromasa.konishi@sato-glo bal . com
URL (optional) www.satovicinity.com
Patent Holder:
Legal Name TAGSYS SAS
Contact for license application:
Name & Department Mr. Alain Fanet President
Address 785 Voie Antiope, TI Athélia 3
Address F-13600 La Ciotat
Tel. +33 332188900
Fax +33 332188900
E-mail alain.fanet@tagsysrfid.com
URL (optional) www.mojix.com

Contact details
Patent Holder:
Legal Name   University of Pittsburgh - Of the Commonwealth of Pennsylvania
Contact for license application:
Name & Department   Marc S. Malandro, PhD, CLP, RTIP
AddressUniversity of Pittsburgh, 200 Gardner Steel Conference Center
AddressThackeray & O'Hara Streets, Pittsburgh, PA 15260
Tel.   412-624-8787
Fax   412-648-2259
E-mail mmalandro@innovation.pitt.edu
URL (optional)
Patent Holder:
Legal Name   Zebra Technologies Corporation
Contact for license application:
Name & Department   Glenn Frankenberger, Sr. IP Counsel, Legal Department
AddressOne Motorola Plaza
AddressHoltsville, NY 11742
Tel.   631-738-5570
Fax   631-738-4110
E-mail glenn.frankenberger@zebra.com
URL (optional)

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

The latest information on IP that may be applicable to this document can be found at www.iso.org/patents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Information technology — Radio frequency identification for item management —

Part 63:
Parameters for air interface communications at 860 MHz to 960 MHz Type C

1 Scope

This document defines the air interface for radio frequency identification (RFID) devices operating in the 860 MHz to 960 MHz industrial, scientific, and medical (ISM) band used in item management applications. It provides a common technical specification for RFID devices that can be used to develop RFID application standards. This document is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace.

It defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum effective isotropic radiated power (EIRP), spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and, where appropriate, operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. It further defines the communications protocol used in the air interface.

This document specifies the physical and logical requirements for a passive-backscatter, Interrogator-Talks-First (ITF) systems. The system comprises Interrogators, also known as readers, and tags, also known as labels. An Interrogator receives information from a tag by transmitting a continuous-wave (CW) RF signal to the tag; the tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the Interrogator. The system is ITF, i.e. a tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an Interrogator.

This document specifies

— physical interactions (the signalling layer of the communication link) between Interrogators and tags;

— logical operating procedures and commands between Interrogators and Tags;

— the collision arbitration scheme used to identify a specific tag in a multiple-tag environment;

— optional security commands that allow the use of crypto suites of ISO/IEC 29167.

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 15961 (all parts), *Information technology — Data protocol for radio frequency identification (RFID) for item management*

ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

ISO/IEC 15963-1, *Information technology — Radio frequency identification for item management — Part 1: Unique identification for RF tags numbering systems*

ISO/IEC 18000-61, *Information technology — Radio frequency identification for item management — Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

ISO/IEC 18000-64, *Information technology — Radio frequency identification for item management — Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

EPC Tag Data Standard available at https://www.gs1.org/standards/epc-rfid/tds

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and the following 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
air interface
complete communication link between an Interrogator and a Tag including the physical layer, collision-arbitration algorithm, command and response structure, and data-coding methodology

3.2
authenticated communication
communication in which message integrity is protected

3.3
battery assisted mode
working mode of battery assisted tags with non-empty battery

3.4
crypto superuser
key with an asserted CryptoSuperuser privilege

3.5
data element
low-level, indivisible data construct

3.6
XTID
extended tag identifier
memory construct that defines a Tag's capabilities and which may include a Tag serial number

Note 1 to entry: Further specified in the EPC Tag Data Standard.

3.7
extended temperature range
temperature range between –40 °C to +65 °C

Note 1 to entry: See *nominal temperature range* (3.18).

3.8
file type
8-bit string that specifies a file's designated type

3.9
file superuser
access password or key with a 0011_2 **secured**-state file privilege value

3.10
full-duplex communications
communications channel that carries data in both directions at once

Note 1 to entry: See *half-duplex communications* (3.11).

3.11
half-duplex communications
communications channel that carries data in one direction at a time rather than in both directions at once

Note 1 to entry: See *full-duplex communications* (3.10).

3.12
handle
16-bit tag identifier

3.13
hibernate
state of energy saving when the device is not required to be used

3.14
interrogator authentication
means for a Tag to determine, via cryptographic means, that an Interrogator's identity is as claimed

3.15
keyID
numerical designator for a single key

3.16
MAC
message authentication code
code, computed over bits in a message, that an Interrogator or a Tag may use to verify the integrity of the message

3.17
mutual authentication
means for a Tag and an Interrogator to each determine, via cryptographic means, that the others' identity is as claimed

3.18
nominal temperature range
temperature range between –25 °C to +40 °C

Note 1 to entry: See *extended temperature range* (3.7).

3.19
nonremovable Tag
Tag that a consumer cannot physically detach from an item without special equipment or without compromising the item's intended functionality

Note 1 to entry: See *removable Tag* (3.24).

3.20
password
secret value sent by an Interrogator to a Tag to enable restricted Tag operations

Note 1 to entry: Passwords are not keys.

Note 2 to entry: The only passwords defined by this protocol are the kill and access passwords.

3.21
private key
undisclosed or non-distributed key in an asymmetric, or public-private key pair, cipher

Note 1 to entry: A private key is typically used for decryption or digital-signature generation.

Note 2 to entry: See *public key* (3.22).

3.22
public key
disclosed or distributed key in an asymmetric, or public-private key pair, cipher

Note 1 to entry: A public key is typically used for encryption or signature verification.

Note 2 to entry: See *private key* (3.21).

3.23
Q
parameter that an Interrogator uses to regulate the probability of Tag response

Note 1 to entry: An Interrogator instructs Tags in an inventory round to load a Q-bit random (or pseudo-random) number into their slot counter; the Interrogator may also command Tags to decrement their slot counter. Tags reply when the value in their slot counter, i.e. their slot (3.30), is zero. Q is an integer in the range (0,15); the corresponding Tag-response probabilities range from $2^0 = 1$ to $2^{-15} = 0,000031$.

3.24
removable Tag
Tag that a consumer can physically detach from an item without special equipment and without compromising the item's intended functionality

Note 1 to entry: See nonremovable Tag (3.19).

3.25
secure communication
communication in which message confidentiality is protected

3.26
security
degree of protection against threats identified in a security policy

Note 1 to entry: A system is secure if it is protected to the degree specified in the *security policy* (3.27).

Note 2 to entry: See *security policy* (3.27).

3.27
security policy
definition, either explicit or implicit, of the threats a system is intended to address

Note 1 to entry: See *security* (3.26).

3.28
session key
temporary key generated by one or both of Tag and Interrogator and typically used for authenticated and/or secure communications

3.29
simple sensor functionality
functionality whereby a sensor provides a valid Simple Sensor data address and transmits Simple Sensor data subsequent to the UII as part of the reply to the *ACK* command

3.30
slot
point, in an inventory round, at which a Tag may respond

Note 1 to entry: Slot is the value output by a Tag's slot counter; Tags reply when their slot (i.e. the value in their slot counter) is zero.

Note 2 to entry: See *Q* (3.23).

3.31
snapshot sensor
sensor that makes a measurement during power-up or on demand from an Interrogator

3.32
tag authentication
means for an Interrogator to determine, via cryptographic means, that a Tag's identity is as claimed

3.33
traceable
not restricting the identifying information that a Tag exposes and/or the Tag's operating range

Note 1 to entry: See *untraceable* (3.36).

3.34
untraceable privilege
privilege given to the access password or to a key that grants an Interrogator using the access password or key the right to access untraceably hidden memory and/or to issue an *Untraceable* command

34.35
untraceably hidden memory
memory that an untraceable tag hides from Interrogators with a deasserted untraceable privilege

3.36
untraceable
restricting the identifying information that a Tag exposes and/or the Tag's operating range

Note 1 to entry: See *traceable* (3.33).

4   Symbols, abbreviated terms and notation

4.1   Symbols

C	computed-response indicator
F	file-services indicator (whether a Tag supports the *FileOpen* command)
FrT	frequency tolerance
FS	full function sensor indicator
FT	frequency tolerance
H	hazmat indicator
INACT_T	inactivity threshold