



IEEE Guide for EMF Exposure Assessment of Internet of Things (IoT) Technologies and Devices

STANDARDS

Developed by the
IEEE Standards Coordinating Committee 39
on
Electromagnetic Safety

IEEE Std 1528.7™-2020

IEEE Guide for EMF Exposure Assessment of Internet of Things (IoT) Technologies and Devices

Developed by the

IEEE Standards Coordinating Committee 39
on
Electromagnetic Safety

Approved 24 September 2020

IEEE SA Standards Board

Abstract: In the wireless communication field, 5G and Internet of Things (IoT) solutions are the main emerging technologies and future wireless communication will rely on them. A methodology for classifying IoT devices based on radio frequency (RF) exposure characteristics is provided. Classification is based on frequency, bandwidth, radiated power, and typical installation configuration. Links between device class and available measurement/computational standards are provided. A framework criterion for exclusion classes for exposure assessment and criteria for addressing situations where exposure assessment is unavailable are included.

Keywords: exposure to electromagnetic fields, IEEE 1528™, Internet of Things devices, multiple IoT devices

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 11 January 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-7078-0 STD24419
Print: ISBN 978-1-5044-7079-7 STDPD24419

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the

IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE guide was completed, the following persons contributed to the development of this standard:

Andrea Schiavoni, *Chair*

Sami Gabriel, *Vice Chair*

Quirino Balzano
Giorgi Bit-Babik
David Case
Kwok Chan
J. C. Chen
Andreas Christ
C-K. Chou
Valerio De Santis
Martin Doczkat

Mark Douglas
Walid El Hajj
Antonio Faraone
Tyler Glembo
Tim Harrington
Jafar Keshvari
Niels Kuster
Benjamin Loader
Vikass Monebhurrn
Kai Niskala

Kaitlin O’Keefe
Teruo Onishi
Yi Pan
Robert Paxman
Alexander Prokop
John Roman
Greguy Saint-Pierre
Ma Wenhua
Mike Wood

The following members of the individual Standards Association balloting group voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

Reza Arefi
Matthew Butcher
William Byrd
David Case
Pin Chang
C-K. Chou
Mark Douglas
Donald Dunn
Kenneth Foster
Avraham Freedman
Sami Gabriel

Kevin Graf
Donald Haes
Werner Hoelzl
Robert Johnson
Kenneth Joyner
Efthymios Karabetsos
Piotr Karocki
Nam Kim
Jim Kulchisky
Arthur H. Light
Albert Livshitz
Vikass Monebhurrn

Maryna Nesterova
Teruo Onishi
Branimir Petosic
Ghery Pettit
Katja Pokovic
Alexander Prokop
Ion Radu
Gary Smullin
Walter Struppler
Artnarong Thansandote
Raul Velazquez

When the IEEE SA Standards Board approved this guide on 24 September 2020, it had the following membership:

Gary Hoffman, *Chair*

Jon Walter Rosdahl, *Vice Chair*

John D. Kulick, *Past Chair*

Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*

David J. Law
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Dorothy Stanley

Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1528.7-2020, IEEE Guide for EMF Exposure Assessment of Internet of Things (IoT) Technologies and Devices.

This project was sponsored by IEEE-SASB Coordinating Committees/SCC39—International Committee on Electromagnetic Safety (SASB/SCC39)¹ and SASB/SCC39/TC34 SC1 (TC 34 Chair: Dr. Teruo Onishi; TC 34 Vice-chair: Dr. Mark Douglas; TC 34 SC1 Chair: Dr. Mark Douglas).

This guide provides a methodology for classifying IoT devices based on RF exposure characteristics. Classification is based on frequency, bandwidth, radiated power, and typical installation configuration. Links between device class and available measurement/computational standards are provided. A framework criterion for exclusion classes for exposure assessment and criteria for addressing situations where exposure assessment is unavailable are included.

In the wireless communication field, 5G and IoT solutions are the main emerging technologies that will drive the future wireless communication.

¹ Online: <https://www.ices-emfsafety.org/committees/tc34-subcommittees/>.

Contents

1. Overview	10
1.1 Scope	10
1.2 Word usage	10
2. Normative references	11
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions	12
3.2 Acronyms and abbreviations	14
4. Internet of Things (IoT) technology: survey and state of the art	18
4.1 Defining Internet of Things devices for the purposes of exposure assessment	18
4.2 Survey of Internet of Things technologies	19
5. Operating and usage condition of Internet of Things devices	20
5.1 General	20
5.2 Internet of Things environments	20
5.3 Population of devices	21
5.4 Verification of the exposure	22
6. Considerations and exclusions for exposure assessment	22
6.1 General	22
6.2 Radiated power and installation configuration	23
6.3 Criteria for exclusion from assessment	23
6.4 Exposure assessments	25
7. Identified gaps in compliance standards	30
7.1 General	30
7.2 Existing exposure assessment framework	30
7.3 Criteria for exclusion from assessment	31
7.4 Exposure from Internet of Things devices that individually transmit below the power exclusion limit	31
7.5 Methods for defining, a priori, if specific absorption rate or power density patterns overlap	31
7.6 Methods for characterizing reflecting surfaces, indoor and outdoor	31
Annex A (informative) Survey of Internet of Things radio frequency technologies	32
A.1 Introduction	32
A.2 Short-range technologies	38
A.3 Long-range technologies	56
Annex B (informative) Survey of exposures from multiple devices	65
Annex C (informative) Exposure from multiple Internet of Things radio frequency sources	67
C.1 General	67
C.2 Example 1	68
C.3 Example 2	70
C.4 Conclusion	71
Annex D (informative) Bibliography	74

IEEE Guide for EMF Exposure Assessment of Internet of Things (IoT) Technologies and Devices

1. Overview

1.1 Scope

This guide provides references to the appropriate methodology for classifying Internet of Things (IoT) devices based on radio frequency (RF) exposure characteristics. The use and operating modes for a wide variety of devices are considered by grouping them into several deployments and following an appropriate assessment route. Classification of devices is based on frequency, bandwidth, radiated power, and typical installation configuration. The methodology applies to both the short-range (from less than 1 m to 1 km) and long-range (greater than 1 km) technologies that operate from 0 Hz up to 300 GHz frequency range. The available standards and documents applicable for the compliance assessment of IoT technologies/solutions are identified in this guide. Links between device class and available measurement/computational standards are provided. Included within this document is guidance for exclusion classes, exposure assessments, and solutions to address situations where guidance is unavailable.

This guide does not specify measurement and computational methods to assess the exposure of IoT devices, even in the cases there are no appropriate assessment methods. Instead, this guide indicates gaps in available assessment methods, but is not intended to establish the assessment methodology.

1.2 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{2, 3}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

² The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

³ The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

Canada RSS-102, Radio Frequency (RF) Exposure Compliance of Radiocommunication Apparatus (All Frequency Bands).

FCC KDB Publication 447498 D01 v06, RF exposure procedures and equipment authorization policies for mobile and portable devices.

FCC 19-126, “Proposed Changes in the Commission’s Rules Regarding Human Exposure to Radiofrequency Electromagnetic Fields,” U.S. Federal Communications Commission (FCC), docket no. 03-137; Second Report and Order; 34 FCC Record 11687-11855; 85 FR 18131-18151 (Federal Register), 1 Apr. 2020.

ICNIRP-2020, “International Commission on Non-Ionizing Radiation Protection (ICNIRP), guidelines for limiting exposure to electromagnetic fields (100 kHz to 300 GHz).” *Health Physics*, vol. 118, no. 5, pp. 483–524, 2020. DOI: 10.1097/HP.0000000000001210.^{4, 5}

IEC 62209-1:2016, Measurement procedure for the assessment of specific absorption rate of human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices—Part 1: Devices used next to the ear (Frequency range of 300 MHz to 6 GHz).^{6, 7}

IEC 62209-2:2010, Human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices—Human models, instrumentation, and procedures—Part 2: Procedure to determine the specific absorption rate (SAR) for wireless communication devices used in close proximity to the human body (frequency range of 30 MHz to 6 GHz).⁸

IEC 62209-2:2010/AMD1:2019, Amendment 1—Human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices—Human models, instrumentation, and procedures—Part 2: Procedure to determine the specific absorption rate (SAR) for wireless communication devices used in close proximity to the human body (frequency range of 30 MHz to 6 GHz).

⁴ Available at: (https://journals.lww.com/health-physics/Fulltext/2020/05000/Guidelines_for_Limiting_Exposure_to.2.aspx); see also (<https://www.icnirp.org/en/activities/news/news-article/rf-guidelines-2020-published.html>).

⁵ The ICNIRP document is also commonly referred to as the “RF EMF guidelines”; for conciseness it is referred to as ICNIRP-2020 in this document.

⁶ IEC 62209-1:2016 will be substituted by IEC/IEEE 62209-1528 ED1, Measurement procedure for the assessment of specific absorption rate of human exposure to radio frequency fields from hand-held and body-worn wireless communication devices—Part 1528: Human models, instrumentation and procedures (Frequency range of 4 MHz to 10 GHz), as soon as it is published; the latter is in FDIS stage and publication is expected in 2020.

⁷ IEC publications are available from the International Electrotechnical Commission (<https://www.iec.ch>) and the American National Standards Institute (<https://www.ansi.org/>).

⁸ IEC 62209-2:2010 and IEC 62209-2:2010/AMD1:2019 will be substituted by IEC/IEEE 62209-1528 ED1, Measurement procedure for the assessment of specific absorption rate of human exposure to radio frequency fields from hand-held and body-worn wireless communication devices—Part 1528: Human models, instrumentation and procedures (Frequency range of 4 MHz to 10 GHz), as soon as it is published; the latter is in FDIS stage and publication is expected in 2020.

IEC 62209-3:2019, Measurement procedure for the assessment of specific absorption rate of human exposure to radio frequency fields from hand-held and body-mounted wireless communication devices—Part 3: Vector measurement-based systems (Frequency range of 600 MHz to 6 GHz).

IEC 62232:2017, Determination of RF field strength, power density and SAR in the vicinity of radiocommunication base stations for the purpose of evaluating human exposure.

IEC 62311:2019, Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz to 300 GHz).

IEC 62479:2010, Assessment of the compliance of low-power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz).

IEC/IEEE 62704-1:2017, Determining the peak spatial-average specific absorption rate (SAR) in the human body from wireless communications devices, 30 MHz to 6 GHz—Part 1: General requirements for using the finite difference time-domain (FDTD) method for SAR calculations.

IEC/IEEE 62704-4, Recommended practice for determining the Peak Spatial Average Specific Absorption Rate (SAR) in the human body from wireless communications devices, 30 MHz to 6 GHz—Part 4: General requirements for using the Finite-Element Method (FEM) for SAR calculations and specific requirements for modelling vehicle-mounted antennas and personal wireless devices.⁹

IEC TR 62630:2010, Guidance for evaluating exposure from multiple electromagnetic sources.

IEEE Std 1528TM-2013, IEEE Recommended Practice for Determining the Peak Spatial-Average Specific Absorption Rate (SAR) in the Human Head from Wireless Communications Devices: Measurement Techniques.^{10, 11}

IEEE Std C95.1TM-2019, IEEE Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz.

IEEE Std C95.3TM-2002, IEEE Recommended Practice for Measurements and Computations of Radio Frequency Electromagnetic Fields With Respect to Human Exposure to Such Fields, 100 kHz–300 GHz.

ISO/IEC 20924:2018, Internet of Things (IoT)—Vocabulary.¹²

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.¹³

close proximity: A separation distance of 200 mm or less from a device antenna to a bystander or a user.

⁹ IEC/IEEE 62704-4 is in FDIS stage and publication is expected in 2020.

¹⁰ The IEEE standards or products referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

¹¹ IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

¹² ISO publications are available from the International Organization for Standardization (<http://www.iso.org/>) and the American National Standards Institute (<http://www.ansi.org/>).

¹³ *IEEE Standards Dictionary Online* is available at: <http://ieeexplore.ieee.org/>.

collocated devices: Devices installed in the same area at a given site.

NOTE—For purposes of this guide, collocation implies interaction between devices that could cause interference depending on configuration. Collocation is limited to electromagnetic fields (EMFs) within this guide.¹⁴

device: An apparatus consisting of single or multiple radio frequency (RF) transmitters (or transceivers).

general public: People who have no knowledge or control of their exposure and are not permitted in a restricted environment. The unrestricted tier exposure limit applies to the general public.

NOTE—Some documents and regulations use the term *general population* rather than *general public*.

heterogeneous devices: Devices that perform different functions, for example, safety and communications.

homogeneous devices: Devices that perform the same function for different applications and owners.

host device: A device that includes one or several radio device(s) of different characteristics, type, and manufacturer that operates as an Internet of Things (IoT) device.

Internet of Things (IoT): Infrastructure of interconnected entities, systems, and information resources together with services that process and react to information from the physical world.

Internet protocol: Set of rules and procedures to be followed by members of a net to maximize the orderly exchange of information or data.

IoT device: (A) Digital entity that bridges physical entities and digital entities of an Internet of Things (IoT) system. An IoT device can be a standalone device or equipped with one or several radio devices to accomplish various tasks. (B) For the purposes of this guide, the IoT device definition is extended as follows: A device that performs a detecting, monitoring, or measuring function, and is part of a wireless network. The IoT device interacts, establishes communication links, and communicates with other devices. It could implement one or more wireless interfaces for communication using internet protocols or protocols other than the internet protocol.

NOTE 1—An IoT-device can be hand-held, wearable, portable, or installed in a fixed location. It can be powered by batteries or mains connection; batteries can be charged by wireless power transmission techniques. The IoT device, equipped with at least one or more systems of communication via RF signals, can operate in time frames that can be continuous, periodic, or sporadic.

NOTE 2—The device can implement one or more wired interfaces for communication, but their presence is not considered for the scope of this guide.

IoT system: System involving Internet of Things (IoT) devices that bridge real-world physical entities and digital entities, interacting with those digital entities via one or more networks. (Adapted from ISO/IEC 20924:2018)

multiple sources: Several radio frequency (RF) transmissions operating at the same or different frequencies that can be emitted from a single or multiple device(s).

¹⁴ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

restricted environment: An environment in which exposure is subject to the occupational limits and having additional controls in place limiting access.

NOTE 1—Effective radio frequency (RF) safety programs, such as per IEEE Std C95.7™ [B140], should be implemented so that persons are not exposed above the dosimetric reference limit (DRL) or exposure reference level (ERL) for the restricted environment. The terms *basic restrictions* and *reference levels* used in International Commission on Non-Ionizing Radiation Protection (ICNIRP) 2020 are the same as the terms DRLs and ERLs used in IEEE Std C95.1™-2019.

NOTE 2—In some documents exposure in restricted environments is referred to as *upper tier* or *controlled environment* or *occupational exposure*.

NOTE 3—The general public is not permitted in restricted environments unless they become subject to the applicable safety program and are aware of and can control their exposure.

single source: A single radio frequency (RF) transmitter, where a transmitter is an emitter of RF fields.

unrestricted environment: An environment in which exposure is subject to the general public limits.

3.2 Acronyms and abbreviations

3GPP	The 3rd Generation Partnership Project
6LoWPAN	IPv6 over low-power wireless personal area networks
ac	alternating current
AIDC	automatic identification and data capture
ANT	Advanced and Adaptive Network Technology
AP	access point
ASK	amplitude shift keying
BLE	Bluetooth Low Energy
BPSK	binary phase shift keying
BSS	basic service set
CCK	complementary code keying
CEPT	European Conference of Postal and Telecommunications Administrations
CSMA/CA	carrier-sense multiple access with collision avoidance
CSS	chirp spread spectrum
CW	continuous wave
D8PSK	differential 8-phase shift keying
DFS	direct feed system; dynamic frequency selection
DL	downlink
DPBPSK	differential binary phase shift keying
DQPSK	differential quadrature phase shift keying
DRL	dosimetric reference limit
DSB-ASK	double-sideband amplitude shift keying
DSSS	direct sequence spread spectrum

DTLS	Datagram Transport Layer Security
EC-EGPRS	Extended Coverage Enhanced General Packet Radio Service
EC-GSM	extended coverage Global System for Mobile Communications
ECMA	European Computer Manufacturers Association
EFC	electrical field communication
EGPRS	Enhanced General Packet Radio Service
EIRP	effective isotropic radiated power
EMF	electromagnetic field
eMTC	enhanced machine-type communication
EPC	electronic product code
ERC	Electronic Communications Committee
ERP	effective radiated power
ERL	exposure reference level
ESS	extended service set
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
FDMA	frequency division multiple access
FHSS	frequency hopping spread spectrum
FM-UWB	frequency modulation ultra-wide band
FSK	frequency shift keying
FWA	fixed wireless access
GFSK	Gaussian frequency shift keying
GMSK	Gaussian minimum shift keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
H2M	human to machine
HART	Highway Addressable Remote Transducer
HBC	human body communication
HCF	HART Communications Foundation
HD	high-definition
HF	high frequency
HKIA	Hong Kong International Airport
IBSS	independent basic service set
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force

IoT	Internet of Things
IR-UWB	impulse radio ultra-wide band
ISA	International Society of Automation
ISM	industrial, scientific, and medical
ISO	International Organization for Standardization
KDB	Knowledge Database (Federal Communications Commission [FCC])
LDC	low duty cycle
LF	low frequency
LoRa	long range
LOS	line of sight
LP	low power
LPWAN	low-power wide-area network
LTE	long-term evolution
M2M	machine to machine
MAC	medium access control
MBAN	medical body area network
MICS	Media Implant Communication Service
MIMO	multiple-input multiple-output
MPE	maximum permissible exposure
MW	microwave
NB	narrowband
NB-CIoT	narrowband cellular IoT
NB-IoT	narrowband IoT
NB-M2M	narrowband machine to machine
NFC	near field communication
NFCIP	Near Field Communication—Interface and Protocol
NLOS	non-line-of-sight
OFDM	orthogonal frequency-division multiplexing
OFDMA	orthogonal frequency-division multiple access
OOK	on-off keying
OQPSK	offset quadrature phase shift keying
OSI	Open Systems Interconnection
P2P	peer to peer
PCD	proximity coupling device
PD	power density
PHY	physical layer
PICC	proximity integrated circuit card

PR-ASK	phase reversal amplitude shift keying
PSK	phase shift keying
psSAR	peak spatial-average specific absorption rate
QAM	quadrature amplitude modulation
QPSK	quadrature phase shift keying
RC	radio configuration
RF	radio frequency
RFID	radio frequency identification
RLAN	radio local area network
RPMA	random phase multiple access
SAR	specific absorption rate
SC	single carrier
SC-FDMA	single-carrier frequency-division multiple access
SIG	Bluetooth Special Interest Group
SOFDMA	scalable orthogonal frequency-division multiple access
SRD	short-range device
SSB-ASK	single sideband amplitude shift keying
TDMA	time-division multiple access
TER	total exposure ratio
TIM	traffic identification map
TPC	transmit power control
TWT	target wakeup times
TX	transmit
UDP	user datagram protocol
UE	user equipment
UHF	ultra-high frequency
UL	uplink
ULD	unit load device
UMTS	Universal Mobile Telecommunications System
UNB	ultra narrowband
U-NII	unlicensed national information infrastructure
VCD	vicinity coupling device
VICC	vicinity integrated circuit card
WBAN	wireless body area network
Wi-Fi	wireless fidelity
Wi-Fi HaLow™	Wi-Fi technology based on IEEE Std 802.11ah™
WiMAX	Worldwide Interoperability for Microwave Access

WirelessHART	Wireless Highway Addressable Remote Transducer
WirelessMAN	wireless metropolitan area network
WLAN	wireless local area network
WMTS	Wireless Medical Telemetry Service
WPAN	wireless personal area network

4. Internet of Things (IoT) technology: survey and state of the art

4.1 Defining Internet of Things devices for the purposes of exposure assessment

When evaluating exposures to electromagnetic fields from IoT devices, the following aspects should be addressed to give a dimension to the problem for defining a possible assessment and compliance path:

- What is an IoT device?
- In which contexts are the IoT devices expected to operate and which types of interactions do the IoT devices have with human beings?

Answering the first question is not easy (see Chapter 2.b “Describing IoT” in NTIA [B177]), due to the variety of present and future applications of IoT technology. An IoT device should be defined based on its functionality and context of its application; if either change, then the IoT device could take on a different meaning. As an example, an IoT device could be defined as a sensing device when used to sense parameters, but the device could be defined as a gateway when acting as a bridge between other IoT devices within its network.

IoT devices operations are generally machine-to-machine oriented with little human intervention. IoT devices considered in this guide have the property to communicate with other devices and/or with the network by means of wireless technologies. As such, they have the following three key features:

- a) Connectivity: the ability to interact with various devices having different functions and user interfaces, which enables data-driven decision making.
- b) Sensing: monitoring of external events, such as recognizing surrounding objects or environmental monitoring (e.g., light, temperature).
- c) Autonomy: independent operation with minimal human intervention. Some technologies operate with low power consumption to avoid frequent battery recharging.

IoT technologies can be divided into short-range (from less than 1 m to 1 km) and long-range (greater than 1 km) technologies. IoT devices will generally operate up to 300 GHz and include technologies such as:

- Short-range technologies provide connectivity within local networks such as home, office, or industrial settings. They include near field communication (NFC), wireless body area network (WBAN), ultra-high frequency (UHF) radio frequency identification (RFID), Bluetooth Low Energy (BLE), ZigBee, Thread, Advanced and Adaptive Network Technology (ANT), Z-wave, wireless fidelity (Wi-Fi), and Wi-Fi HaLow™.
- Long-range technologies provide gateways between local networks to provide coverage over larger areas (e.g., cities, countries). They include long range (LoRa), Sigfox, Ingenu, Worldwide Interoperability for Microwave Access (WiMAX), narrowband Internet of Things (NB-IoT), enhanced machine-type communication (eMTC), and extended coverage Global System for Mobile Communications (EC-GSM).

The definition of an IoT device in the context of this guide is given in Clause 3, with the aspect under consideration within this guide being the transmission of electromagnetic fields. In this context of an IoT device, this increases the variety of devices that should be taken into consideration and may lead to different device types than seen in the past. In some cases, the exposure assessment will fall into a known or published method or framework, while in other scenarios further analysis and specific device or deployment functionality may need to be understood or may need to develop criteria for excluding IoT devices from exposure assessment when not required.

4.2 Survey of Internet of Things technologies

IoT technology is expected to be pervasive in each field of our personal and professional life. Many studies have been published recently indicating forecasts for the number of devices all around the world each year, e.g., NTIA ([B177] Chapter 2 “The Internet of Things Landscape”), Ofcom 2017 ([B181], Chapter 6 “The Internet of Things”), and Gremban [B90].¹⁵

IEEE White Paper ([B124], Figure 1), International Electrotechnical Commission (IEC) White Paper ([B122], Figure 2-1 and Figure 6-2) show what is the field of application of IoT devices at present, briefly summarized and commented as follows:

- a) Transportation and vehicles: In EC “Internet of Things” ([B56] Chapter 2) there is a list of applications of IoT, ranging from traffic management to wellbeing of the driver or people inside the vehicle. All types of interaction need exchange of information among devices that can communicate via radio at different levels of operations and ranges; from a few centimeters in the case of services inside the vehicles, to some meters for interaction between vehicles, to hundreds of meters or kilometers in the case of connection to the network in mobility. See also FTA [B80].
- b) Industry: In NTIA ([B177] 2C “Benefits of IoT”), EC “Advancing the Internet of Things in Europe” ([B58] Annex 3 “Smart manufacturing”), Devereaux [B43], and EC (“Definition of a research” [B55]) there are analyses of the impact of IoT technology has on manufacturing. All studies indicate that IoT is the enabling technology in the future of the industry, in particular EC (“Definition of a research” [B55]) stated “The concept of hyper-connectivity is closely interwoven with the idea of ubiquitous and pervasive computing where a myriad of sensors, actuators, displays and other technologies are embedded in the everyday objects of our lives, and connected seamlessly with each other through a continuous network. In our view, users will heavily tap into advanced and uninterrupted networking capabilities (supported/extended by other technologies such as cloud and big data) to generate viable business opportunities.”
- c) Energy: In DOE [B48] and EC (“Advancing the Internet of Things in Europe” [B58] Annex 4 “Smart Energy”) there are analyses how the use of the IoT technology has applied in the management, control, and optimization of energy supply and demand.
- d) Agriculture: In EC (“Advancing the Internet of Things in Europe” [B58] Annex 7 “Smart Farming”), FAO [B68], and Digital Transformation Monitor (“Industry 4.0” [B44]) there are lists of applications for smart farming and links for further reading.
- e) Wearables: EC (“Advancing the Internet of Things in Europe” [B58] Annex 2 “Personal Wellness and Wearables”), Bachmann [B16], Bigelow [B17], GSMA (“Wearables” [B97]), Digital Transformation Monitor (“The Internet of Things” [B45]).
- f) Healthcare: GSMA (“Health” [B99]), EC (“Smart health” [B57]), EC (“Communication” [B54]), NSW [B176] and HHS [B111].
- g) Smart cities: EC (“Advancing the Internet of Things in Europe” [B58] Annex 5 “Smart cities”), GSMA (“Smart cities” [B100]), and FTA [B80].

¹⁵ There is a plethora of papers reporting forecasts for the growth of IoT technology. It is not in the scope of this guide to give an exhaustive survey of the publication on this topic.

- h) Smart home: EC (“Advancing the Internet of Things in Europe” [B58] Annex 1 “Smart Homes”), GSMA (“Vision of smart home” [B101]), Digital Transformation Monitor (“Smart home” [B46]), and Digital Transformation Monitor (“Smart building” [B47]).
- i) Education: GSMA (“Mobile learning” [B102]).

An extensive and thorough survey of the available technologies used in the IoT domain is given in Annex A.

5. Operating and usage condition of Internet of Things devices

5.1 General

IoT devices are deployed in various scenarios, including bounded, free, and personal environments. Additionally, each environment can have different access restrictions.

Because radio frequency (RF) exposure to people can depend on both the characteristics of the radio devices and how they are housed inside their host, exposure assessments might need to be performed with the host device and all featured radio devices relative to the intended use as specified by the host’s manufacturer.

However, the wide range of possible deployment scenarios and devices means that gaps in assessment methodologies could exist when:

- a) The device does not fall into any of the categories covered by the exposure standards listed in Clause 2.
- b) The intended use of the devices, whatever it might be, requires one or more additional RF communication devices to implement the IoT capabilities.
- c) Usage and any other characteristic of the device do not allow association to standard exposure assessment methods.
- d) If more than one device contributes to the exposure.

Gaps in the existing assessment methodologies for IoT devices are discussed in Clause 7.

5.2 Internet of Things environments

5.2.1 General

Subclause 5.2 provides short descriptions and classifications of environments where IoT devices can be deployed, considering the following topics:

- a) Find a classification of environments where the IoT devices can be deployed to address exposure assessment.
- b) In conjunction with 6.2, address deployments for defining exposure assessment exclusion criteria.

5.2.2 Bounded environment

A bounded environment is one where IoT devices cannot be easily approached by a person even if persons can be within close proximity to the devices. The environment is delimited by a boundary where the devices are confined; the confined environment can be denoted by the following access types.

- a) **Unrestricted access:** environment where devices are confined but where people can approach or stay without any limitation.
- b) **Restricted access:** environment where devices are out of a person's reach or where access is controlled. However, authorized people could approach, linger, or stand at the location of the devices.

5.2.3 Free environment

A free environment is one where the IoT devices are deployed and a person can freely access the devices. The free environment might or might not be identified by boundary signs, markings, or structures of any type and, even if these are present, they do not limit access to devices; the free environment can be denoted by the following access types.

- a) **Unrestricted access:** environment where devices are deployed and where people can access, linger, or stay in close proximity to the devices without any limitation.
- b) **Sporadic access:** environment where devices are deployed and people infrequently access, linger, or stay in the area.
- c) **Restricted access:** environment where devices are deployed and typically authorized people have free access, but devices are located in positions where people cannot normally or easily access, linger, or stand.

5.2.4 Personal environment

A personal environment is one where devices are used in proximity to a person. The usage of these devices can be directly related to the presence of the person since devices are carried on or are situated in close proximity to the space where a person performs normal activities. This environment can be subdivided into two classes:

- a) **Body worn:** devices that are close, in contact with a person's body, or devices that are embedded in clothing.
- b) **Accessible:** devices that are designed to operate in proximity to a person. These devices can be placed at distances so that a person can easily reach or touch them. This region of space can be defined as "the sphere of influence," that is, a sphere having a radius equal to the length of a person's arm, e.g., 1 m.

5.3 Population of devices

A population of devices is a number of IoT devices deployed in a limited volume. The volume is delimited by physical borders, for example the walls of a room, or by nonphysical borders defined by the deployment region.

A population of devices can increase over time because of requirements to have multiple IoT services within an established environment. Each device individually is required to comply with RF exposure limits as specified by regulatory agencies, such as the U.S. Federal Communications Commission (FCC). For

each deployment scenario there can be a multiplicity of homogeneous and/or heterogeneous devices placed close to each other and performing their own functions with or without coordination.

Many studies have been conducted to investigate RF exposure with populations of devices in various environments.

A survey of these studies is reported in Annex B. While further research is ongoing, several of these studies did not find a significant increase in RF exposure for a realistic population of IoT devices.

5.4 Verification of the exposure

Further RF exposure assessment might be needed depending on the installation conditions and system configuration for some IoT devices.

Due to the low-power characteristics of IoT devices, deployment is expected to be in an open environment where there is minimal signal attenuation between the transmitter and receiver, e.g., the main beam of the antennas is generally pointed in directions that are not intercepted by the enclosure of the installation environment. Reflections from walls and metal objects, such as pipes, workbenches, tools, and furniture, could have an influence on RF exposure and should be considered in the assessment. See Annex B for examples.

Installations that follow the manufacturer's guidance should be covered by the manufacturer's RF exposure assessment; installers and site owners are responsible to ensure manufacturer's guidelines are followed. A knowledgeable installer may deviate from manufacturer's installation guidelines and follow work practices that keep the RF exposure below regulatory limits. The site owner should be responsible for the verification of the installer's compliance statements. Verification can entail engaging a RF surveyor to perform exposure measurements in conditions of maximum RF output by the population of devices and at the closest proximity of bystanders.

Additional IoT devices added to a preexisting population should follow the same general process:

- a) The installer is responsible for RF exposure compliance at the modified site and new population.
- b) The site owner should verify the RF exposure compliance of the complete installation.

6. Considerations and exclusions for exposure assessment

6.1 General

Clause 6 summarizes and references existing exposure assessment guidance applicable to IoT devices. Consideration of the typical power levels and installation configurations of IoT devices may allow for a simple demonstration of compliance and exclude the need for a more detailed exposure assessment. If a device does not qualify for exclusion from exposure assessment, then several existing standards can help guide the required assessment.

Documents such as IEEE Std C95.3TM-2002 and IEC 62311:2019 provide general guidance and direction to specific standards on the assessment of electronic and electrical equipment related to human exposure to electromagnetic fields. While this document also provides guidance and direction to other standards, guidance is provided specifically to emerging categories of IoT devices and identifies gaps in existing assessment methods related to these emerging technologies: see Clause 7.

6.2 Radiated power and installation configuration

IoT devices typically have very low potential to exceed exposure limits. The amount of data detected, monitored, or measured is typically low per unit time when compared to, e.g., communication devices, leading to limited data transmission.

Aside from the applications that require body-worn usage, IoT devices are usually placed at 1 m distance or more away from persons. Since IoT devices communicate machine to machine rather than requiring human intervention, the distances from a human body are usually greater than those of personal communication devices. Even if a human operates close to an IoT device, the exposure time might be only a fraction of the averaging time of applicable guidelines. For example, International Commission on Non-Ionizing Radiation Protection 2020 (ICNIRP-2020) and IEEE Std C95.1-2019 specify a 6 min averaging time, thus reducing the potential to exceed the exposure limits of the IoT device.

These conditions should be considered in exposure assessments. Therefore, the vast majority of IoT devices might fall under a low-power exposure assessment test exclusion criterion.

Examples of low-power test exclusions include the following. IEC 62479:2010 defines a low-power exclusion level P_{max} based on applicable exposure guidelines and has an informative annex for estimating low-power exclusion levels for wireless devices used close to the body. FCC Knowledge Database (KDB) Publication 447498 D01 v06 lays out general specific absorption rate (SAR) test exclusion guidance including standalone and simultaneous transmission SAR test exclusion considerations. The document defines formulas for calculating power thresholds for test exclusion based on transmission frequency and distance to the user. IEC 62232:2017 defines a limit for exposure evaluation based on the concept of total exposure ratio (TER). Canada RSS-102 also defines power exemption limits for exposure evaluation.

The power level to be used in assessment is the time-averaged conducted or radiated power over the averaging period defined in the applicable exposure guideline.

6.3 Criteria for exclusion from assessment

6.3.1 General

Subclause 6.3 describes exclusion criteria for exposure assessment of IoT devices. The criteria indicated here are not exhaustive for every type of IoT device or any type of deployment or any deployment of a set of IoT devices. Gaps in exposure assessment standards and regulations, which might lead to gaps in exclusion criteria, should be reviewed with the appropriate regulatory body. Due to time-averaged radiated power, pulsed EMF energy, and deployment, exposure assessment might not be required for some devices and scenarios.

NOTE—National regulatory agencies can have different exclusion criteria that override those specified in this document and different low-power limits that override those specified in IEC 62479:2010.

6.3.2 Low radiated power

Low radiated power condition can be summarized as follows:

- a) If the IoT device includes only one radio whose radiated power is below the limit specified in, e.g., IEC 62479:2010, exposure assessment is not required.

- b) If the IoT device includes more than one radio and the total transmitted power of all radios operating independently or in simultaneous transmit mode is below the limit specified in, e.g., IEC 62479:2010, exposure assessment is not required.

NOTE—The applicability of power thresholds as specified in Annex B of IEC 62479:2010 requires investigation where the radiating parts of the DUT are closer than 5 mm to the phantom surface. The definition of new power thresholds for such configurations is needed.

- c) If the IoT device where intended use shows a time-averaged radiated power during the exposure evaluation period that is below the limit specified in, e.g., IEC 62479:2010, exposure assessment is not required, even when the device is transmitting peak power higher than the exclusion criteria described in a) and b). Use of proximity detection or other forms of power control may be permissible for establishing the time-averaged power, depending on regulatory requirements. The averaged power is evaluated as in Equation (1), where $M = 1$ for a single IoT device and $N = 1$ for an IoT device equipped with only one radio device.

$$\bar{P} = \frac{1}{T_{\text{exp}}} \sum_{m=1}^M \sum_{n=1}^N \int_0^{T_{\text{exp}}} P_{n,m}(t) dt \quad (1)$$

where

$\bar{P}$	is the averaged power in W
$P_{n,m}(t)$	is the time-dependent power radiated by the n -th radio device of the m -th IoT device in W
T_{exp}	is the exposure evaluation period in s, as an example 360 s for 6 min exposure time
N	is the number of radio devices inside the same IoT device
M	is the number of devices

6.3.3 Installation configuration

When deployed, located, or installed in an environment or host apparatus where people are not in close proximity the RF sources, or for people at the boundary of the environment, some devices in their intended use produce exposures below limits, even when transmitting a power higher than the limit specified in IEC 62479:2010. The boundary dimensions depend on the deployment scenario and can be established when exposure assessment is performed; for example, the distance R_n in Equation (2) for exposure assessment based on electric field strength.

An IoT device, containing one or more radios and whose quantity taken as reference for evaluating the exposure (e.g., electric field strength, magnetic field strength, or power density) is below the relevant limit, is not required to be subjected to an exposure assessment. The observation point where the exposure is evaluated using Equation (2), must be in the far field of all antennas in the wireless device. Equation (2) is an example where the quantity considered for evaluating the exposure is electric field strength.

$$E_{\text{limit}} \geq E = \sqrt{\frac{\eta}{4\pi T_{\text{exp}}} \sum_{n=1}^N \int_0^{T_{\text{exp}}} \frac{P_n(t) G_n(\vartheta, \varphi)}{R_n^2} dt} \quad (2)$$

where

E_{limit}	is the exposure limit expressed in terms of electric field strength in V/m
E	is the electric field strength generated by the device in the evaluation point in V/m

$P_n(t)$	is the time-dependent power radiated by n -th radio device in W
$G_n(\vartheta, \varphi)$	is the gain by n -th radio device in the direction of the exposure evaluation point
η	is the wave impedance in free space in Ω
R_n	is the distance between the antenna of the n -th radio device and the evaluation point, greater than the far field distance for the radio device, in m
T_{exp}	is the exposure evaluation period measured in s, for example 360 s for 6 min averaging exposure time, or 1800 s for 30 min averaging exposure time
N	is the number of radio devices inside the same IoT host device

In case of multiple devices, exposure is evaluated using the approach for multiple sources, and multiple frequencies described in Annex D of IEEE Std C95.1-2019 or ICNIRP-2020 [subclause “Simultaneous exposure to multiple frequency fields”] or FCC 19-126.

6.4 Exposure assessments

6.4.1 General

The published exposure standard documents address testing in their applicable frequency bands, summarized as follows:

- In case SAR evaluation is applicable, the upper frequency range is limited to 6 GHz by existing assessment standard documents (IEC 62209-1:2016, IEC 62209-2:2010, IEC 62209-2:2010/AMD1:2019, IEC 62209-3:2019, IEC/IEEE 62704-1:2017, IEC/IEEE 62704-4, IEEE Std 1528-2013) and is limited to 10 GHz in IEC/IEEE 62209-1528 [B123].
- In case power density evaluation is applicable, the frequency range for assessment is limited to 6 GHz to 300 GHz by assessment standard documents in preparation (IEC/IEEE 63195-1, IEC/IEEE 63195-2).
- In case electric field strength, magnetic field strength, and incident plane-wave power density evaluation are applicable, depending on the type and usage of the device, from 100 kHz to 300 GHz (IEC 62232:2017).
- For electronic and electrical equipment not covered by any dedicated product standard or product family standard, a generic standard regarding human exposure to electromagnetic fields applies (IEC 62311:2019).

Assessment of a device is addressed by these standard methods unless exclusion criteria apply or there are reasons for which none of the previous standards are applicable, such that a gap in available assessment methods exists (see also Clause 7).

6.4.2 IoT device exposure assessments

Figure 1 provides a flowchart of steps used in exposure assessment of a single IoT device; the steps are also described in the following list:

- Identify the transmitted power of the IoT device:

- 1) If the IoT device meets low-power exclusion principle (e.g., IEC 62479:2010) then assessment is not required.¹⁶
- 2) If the IoT device does not meet low-power exclusion principle (e.g., IEC 62479:2010), go to b).
- b) From a) 2), based on intended use, determine device type, operating frequency, and proximity to the user, and whether device is in scope of the existing product standards:
 - 1) For separation distances less than 200 mm¹⁷:
 - i) At transmit frequencies where SAR assessment is required, use the appropriate standard of item a) in 6.4.1.
 - ii) At transmit frequencies where power density assessment is required, use the appropriate standard of item b) in 6.4.1.
 - iii) If the device transmits at frequencies where SAR assessment is required and simultaneously transmits at frequencies where power density assessment is required, combine simultaneous exposure to multiple frequencies as described in IEC 63195-1, IEC 63195-2, ICNIRP-2020, IEEE Std C95.1-2019, IEC TR 62630:2010, or FCC 19-126.
 - 2) For separation distances greater than 200 mm: assess electric field strength or magnetic field strength or incident plane wave power density, per IEC 62232:2017.
 - 3) If no existing product standard is applicable: perform assessment per IEC 62311:2019.

In the survey in Annex A, at least one application case is described for each IoT technology. For some IoT technologies, pilot or hypothetical applications are described if they are not yet widely used in the market. The conclusions of Annex A also provide information about the maximum duty cycle at which devices under all operational conditions fall under exclusion criteria for exposure assessments.

¹⁶ Other exposure guidelines or standards may be applicable depending on national regulations. Some countries or regions may have lower power exclusion limits.

¹⁷ In some national standards, such as Canada RSS-102, the separation distance used for portable devices is less or equal to 200 mm rather than less than 200 mm.