

Guideline for Testing and Certification Requirements on Healthcare and Wellness Devices



Organiser:



Funding Organisation:



Sponsor:



Supporting Organisations:



Disclaimer

Any opinions, findings, conclusions, or recommendations expressed in this material/event (or by members of the project team) do not reflect the views of the Government of the Hong Kong Special Administrative Region, the Innovation and Technology Commission, or the General Support Programme Vetting Committee of the Innovation and Technology Fund.

This Guidebook is for information purpose only. Whilst every effort has been made to ensure the accuracy of the information provided herein, the publisher of this Guidebook and the associated organisations in the project should not be held responsible for any damage resulting from the use of such information.

Hong Kong Productivity Council

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong

Tel: (852) 2788 5678

Fax: (852) 2788 5900

Website: <https://www.hkpc.org>

E-mail: hkpcenq@hkpc.org

Innovation and Technology Fund

General Support Programme

“To Promote the Awareness of Compliance Requirements for Healthcare and Wellness Device Industry”

About this Guideline

This project “To Promote the Awareness of Compliance Requirements for Healthcare and Wellness Device Industry” is supported by the Innovation and Technology Fund - General Support Programme (GSP) and is organised by Hong Kong Productivity Council (HKPC).

To support local startups, SMEs, and other technical solution and service providers in meeting the testing requirements for healthcare and wellness devices, a variety of activities have been conducted as part of this project. These activities include a series of technical workshops, promotional seminars, and guideline experience sharing sessions. Additionally, the Guideline aims to enhance the understanding of product testing and certification, thereby assisting startups, SMEs, and other technical solution and service providers in shortening their development cycles and reducing development costs. Ultimately, this initiative seeks to mitigate liability risks by ensuring the provision of high-quality and reliable smart solutions and services in their healthcare and wellness devices.

Acknowledgements

We would like to extend our gratitude to the following organisations and parties for their support on this project (listed in alphabetical order of names).

Hong Kong Medical and Healthcare Device Industries Association Limited (HKMHDIA)

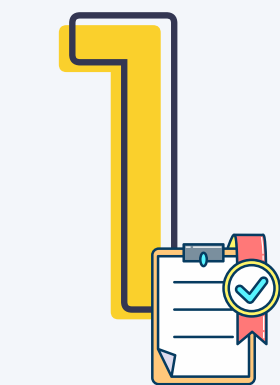
Hong Kong Association for Testing, Inspection and Certification Limited

Hong Kong Electronic Industries Association (HKEIA)

Hong Kong Productivity Council

Rohde & Schwarz Hong Kong Limited

TABLE OF CONTENTS



INTRODUCTION OF STANDARDS,
CERTIFICATION SCHEMES AND
TECHNOLOGIES FOR HEALTHCARE
AND WELLNESS DEVICES

4



HEALTHCARE AND WELLNESS
DEVICES TEST REQUIREMENTS IN
EMC REQUIREMENT

28



HEALTHCARE AND WELLNESS
DEVICES TEST REQUIREMENTS IN
CYBERSECURITY

36



HEALTHCARE AND WELLNESS
DEVICES TEST REQUIREMENTS IN
ELECTRICAL SAFETY

46



HEALTHCARE AND WELLNESS
DEVICES TEST REQUIREMENTS IN
QUALITY MANAGEMENT SYSTEMS
AND RISK MANAGEMENT

54



HEALTHCARE AND WELLNESS
DEVICES TEST REQUIREMENTS IN
RADIO FREQUENCY REQUIREMENT

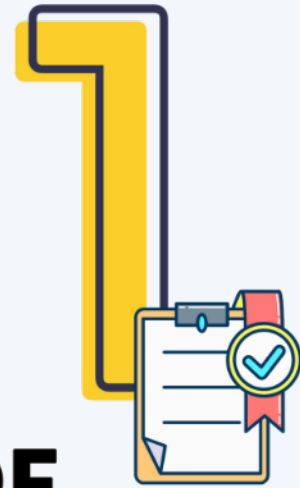
60



PRACTICAL INTERPRETATIONS AND
CASES SHARING FOR HEALTHCARE
AND WELLNESS DEVICES

70

INTRODUCTION OF STANDARDS, CERTIFICATION SCHEMES AND TECHNOLOGIES FOR HEALTHCARE AND WELLNESS DEVICES



Chapter 1 – Introduction of Standards, Certification Schemes & Technologies for Healthcare and Wellness Devices

In this chapter, we will introduce the communication authorities and approval and certification schemes for various countries and regions. The latest technologies for healthcare and wellness devices will also be introduced in this section.

Part A: Asia

	China	Japan	S. Korea	Singapore	Thailand	Indonesia	India
Approval Scheme	CCC / NAL / SRRC	MIC	KC	IDA	NBTC	SDPPI	MCITT
Based on	National	National	National	CENELEC / ETSI	National / CENELEC / ETSI	National	CENELEC / ETSI / National
Duration of Approval	3-5 yrs	Perm	Perm	5 yrs	Perm	3 yrs	Perm
Approval Label	Y	Y	Y	Y	Y	Y	N
Regulator	Ministry of Industry and Information Technology (MIIT)	Ministry of Internal Affairs and Communications (MIC)	Korea Communications Commission (KCC)	IMDA - Infocomm Media Development Authority	National Broadcasting and Telecommunications Commission (NBTC)	Indonesian Telecommunications Regulatory Authority (BRTI)	Telecom Regulatory Authority of India (TRAI)

	Australia	New Zealand
Approval Scheme	Regulatory Compliance Mark	Regulatory Compliance Mark
Based on	CENELEC / ETSI / FCC / National	National / CENELEC / ETSI
Duration of Approval	Perm	Perm
Approval Label	Y	Y
Regulator	Australian Communications and Media Authority (ACMA)	Commerce Commission of New Zealand (ComCom)

Part B - Americas

	Canada	U.S.A.	Mexico	Colombia	Venezuela	Guyana	Ecuador
Approval Scheme	ISED	FCC	IFT	CRC	CONATEL	NFMU	Arcotel
Based on	National	FCC	National / FCC	National / FCC	FCC / CENELEC / ETSI / National	FCC / National	CENELEC / ETSI / FCC
Duration of Approval	Perm	Perm	1 yr to Perm	Perm	Perm	Perm	Perm
Approval Label	Y	Y	Y	Y**	N	NN,YF	N
Regulator	Canadian Radio-television and Telecommunications Commission (CRTC)	Federal Communications Commission (FCC)	Instituto Federal de Telecomunicaciones (IFT)	Comisión de Regulación de Comunicaciones (CRC)	Comisión Nacional de Telecomunicaciones (CONATEL)	Guyana Public Utilities Commission (PUC)	Agencia de Regulación y Control de las Telecomunicaciones

	Peru	Brazil	Bolivia	Paraguay	Uruguay	Argentina	Chile
Approval Scheme	MTC	Anatel	ATT	Asuncion	URSEC	Enacom	SUBTEL
Based on	FCC / National	National	CENELEC / ETSI / FCC	National / CENELEC / ETSI / FCC	FCC / CENELEC / ETSI	FCC / National	FCC / National / CENELEC / ETSI
Duration of Approval	Perm	1 yr to Perm	5 yrs	5 yrs	15 yrs	3 yrs	Perm
Approval Label	N	Y	N	Y	N	Y	N
Regulator	Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)	Agencia Nacional de Telecomunicaciones (ANATEL)	Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT)	Comision Nacional de Telecomunicaciones (CONATEL)	Unidad Reguladora de Servicios de Telecomunicaciones (URSEC)	Comisión Nacional de Comunicaciones (CNC)	Subsecretaría de Telecomunicaciones (SUBTEL)

Part C - Europe

	Belgium Denmark France Germany Italy Spain Sweden	Switzerland	United Kingdom of Great Britain
Approval Scheme	CE	OFCOM	UKCA
Based on	CENELEC & ETSI	CENELEC & ETSI	BSI
Duration of Approval	Perm	Perm	Perm

China

Certification Schemes

- China Compulsory Certificate (also known as CCC or “3C” certificate)
- SRRC certification
- NAL certification
- CCC Self-Declaration
- Voluntary certification



Certifications are performed according to Guobiao (GB) standards, or in English, the National Standards.

The tests are largely similar to those required under CE standards, but the Chinese authority does not recognise test results or reports issued by other countries. It means that only the results or reports from tests conducted in China are qualified for CCC certification. The test reports are issued in Chinese, while the certificates are issued in English and Chinese.

Relevant Chinese Authorities

CCC Mark Administration Authorities

Certification and Accreditation Administration (CNCA) and General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ)

Certification Authority

Chain Quality Certification (CQC) performs certification for all kinds of products (voluntary)

Details of Certification Schemes

CCC certification

The CCC mark is a compulsory safety mark for many products imported, sold or used in the Chinese market. Products in the catalogue cover a range of areas from human health and safety, as well as that of animals and plants, to environmental protection and public safety. It is issued by the responsible government agency in China and is in principle comparable with the CE marking in Europe.

List of products under mandatory certification *only electrical devices are included

1. Electric cables and wiring
2. Electrical switches, protective devices, and connection devices
3. Low voltage electrical equipment
4. Small power motors
5. Electric tools
6. Electric welding machines
7. Household and similar electrical appliances
8. Electronic products and safety accessories
9. Lighting apparatuses
10. Motor vehicles and safety accessories
11. Agricultural machineries
12. Fire service equipment
13. Security system products
14. Construction materials
15. Children's products
16. Explosion-proof electrical products
17. Household gas appliances

SRRC certification

The State Radio Regulation of China (SRRC) Type Approval is mandatory for radio related products and it is also a pre-condition for receiving the Network Access License (NAL). The necessary tests need to be carried out in a test laboratory accredited by the Ministry of Industry and Information Technology (MIIT). The aim of the SRRC Type Approval is to identify the parameters and functions of radio transmission equipment, such as frequency range, frequency band, transmitting power, and many more. Products that require to obtain the Type Approval include mobile phones (GSM or CDMA), wireless LAN (WLAN) devices, and devices that use the following technologies:

- 2.4GHz / 5.8GHz WLAN devices
- Radars
- Short-range wireless devices
- Microwave devices
- Broadcasting equipment
- Satellite equipment
- Wireless access systems (WAS)
- Mobile communication equipment
- Other radio equipment

CCC - GB standards (Guobiao Standards)

GB standards, known as Guobiao Standards, are the national standards of China. These standards are categorised into two types: mandatory and recommended. Mandatory standards carry the force of law, similar to that of other technical regulations in China. They are enforced through laws and administrative regulations, addressing the protection of human health, personal property, and safety. Standards that do not fall within these critical areas are classified as recommended standards.

China's GB standards can be distinguished by their prefix codes. Standards with the prefix code "GB" are mandatory, while those with the prefix code "GB/T" are recommended (also referred to as quasi-mandatory standards). Ref: <https://www.gbstandards.org/>

NAL certification

Healthcare or wellness devices with telecommunication functions that are exported to China must obtain a "Network Access License" (NAL). NAL licensing is mandatory for telecommunications equipment that will be connected to the public telecommunications network. This licensing process builds upon the SRRC certification, and no NAL would be issued without an SRRC certificate. The MIIT in China is responsible for the issuance of NAL. This authority oversees the management and interconnection of public telecommunications networks within China.

A NAL application can only be issued once SRRC certification has been successfully granted, since SRRC test results are the basis for the NAL certification. Applicants should apply for the NAL before applying for CCC. Since some tests in the NAL approval process are also relevant for CCC certification, by applying for the NAL first, these tests do not have to be performed twice.

Telecommunication terminal equipment:

1. Fixed telephone terminals;
2. Cordless telephone terminals;
3. Group telephones;
4. Fax machines;
5. Modems;
6. PBX;
7. Mobile user terminals;
8. Wireless pagers;
9. ISDN terminals;
10. Data terminals;
11. Multimedia terminals;
12. Other telecommunication terminal equipment

Radio communication equipment:

1. Wireless base stations (fixed, mobile, paging and repeater, etc.);
2. Microwave communication equipment;
3. Satellite earth stations





Interconnection equipment:






1. Optical transmission equipment;
2. Digital programme control switching systems (fixed and mobile systems, etc.);
3. No.7 signalling equipment (SS7);
4. Intelligent network equipment;
5. Synchronisation equipment;
6. Access network equipment;
7. Frame relay switches;
8. ATM switches;
9. Integrated service switches;
10. Routing equipment;
11. IP networks about gatekeeper;
12. Data communication equipment (multiplexing equipment, access servers, and cross connection equipment, etc.);
13. Call centre equipment

Japan

Schemes

There are several mandatory approval mark and label schemes such as PSE, PSC, Energy Saving, and RoHs which are under the Electrical Appliances and Materials Safety Law regulated by the Ministry of Economy, Trade and Industry (METI). There is also the Radio Certification label and mark scheme which is under the Japan Radio Law regulated by Ministry of Internal Affairs and Communication (MIC). In addition, there are several voluntary approval mark and certification schemes such as S-JQA, VCCI for most household electrical products and low-power, DC-input products.

Scheme	Mark	Product	Link
PSE (mandatory)	Diamond PSE mark for Category A 	Diamond PSE mark (Category A) including 116 items, and other non-specified electrical appliances;	https://www.meti.go.jp/policy/consumer/seian/denan/file/06_guide/denan_guide_ver3_en.pdf
	Circle PSE Mark for Category B 	Circle PSE mark (Category B) including 341 items	
PSC (Voluntary)	Diamond PSC mark  Circle PSC mark 	Diamond PSC mark: Portable lasers Cribs for infants Hot water circulators for baths Lighters Circle PSC mark: Pressure cookers Helmets (for motorised bicycles or motorcycles) Climbing ropes Oil heaters Oil water heaters Oil bath boilers	https://www.jqa.jp/english/safety/service/mandatory/psc/service.html

Radio Certification label and mark (mandatory)	Specified Radio Equipment 	Specified Radio Equipment: <ul style="list-style-type: none">• Bluetooth• Wi-Fi• LTE• GSM• ZigBee• Wireless mics• RFID (2.4 GHz, 920 MHz)• Telemeters• UWB radio systems	https://www.tele.soumu.go.jp/e/sys/equ/tech/index.htm
	High-Frequency Devices 	High-Frequency Devices: <ul style="list-style-type: none">• IH cooking devices• Microwaves• Electrode-less discharge lamps• Welders• RFID (13.56 MHz)• Ultrasonic devices• Other equipment over 10 kHz (including industrial and medical devices)	
	Extremely Low-Power Devices 		
S-Mark (Voluntary)			http://www.s-ninsho.com/
VCCI (Voluntary)		For products not covered by the PSE Law or Radio Law: low-power, DC-input products	https://www.vcci.jp/english/index.html

Energy Conservation Law (Mandatory)		Air-conditioners, electric refrigerators, and TV sets, electric toilet seats, lighting equipment, electric freezer	https://perspectives.se.com/blog-stream/revision-of-japan-s-act-on-rationalising-energy-use-energy-conservation-act-effective-april-2023
RoHs (Mandatory) JIS C 0950: 2021		<p>[Scope of products]</p> <p>Personal computers Unit-type air conditioners Television sets Refrigerators Washing machines Clothes dryers Microwaves</p> <p>[Specific chemical substances]</p> <p>Lead Mercury Cadmium Hexavalent chromium Polybrominated biphenyl Polybrominated diphenyl ether</p>	https://home.jeita.or.jp/eps/jmoss_en.htm

South Korea

Official Certification Authorities

The Korean Agency for Technology and Standards (KATS) is a government agency under the Ministry of Trade, Industry and Energy (MOTIE). KATS oversees the development and implementation of standards and certification schemes for various product groups to ensure safety, quality, and compliance with regulatory requirements in South Korea. The product groups under the KATS scheme encompass a wide range of categories. It is also a member of the International Organization for Standardization (ISO), as well as the [International Electrotechnical Commission](#) (IEC).

Certification Scheme

KC Certification (KC Mark) is similar to the CE mark scheme, including the Quality Management and Safety Control of Industrial Products Act and the Electric Appliances Safety Act.

Korea Standard: K standard



Product Groups:

- I. Electrical and Electronic Products:
 - Household appliances (e.g., refrigerators, washing machines)
 - Consumer electronics (e.g., televisions, audio equipment)
 - Information technology equipment (e.g., computers, printers)
 - Lighting equipment (e.g., LED lamps, fluorescent lamps)
- II. Machinery and Industrial Equipment:
 - Industrial machinery (e.g., manufacturing equipment, construction machinery)
 - Agricultural machinery (e.g., tractors, harvesters)
 - Safety equipment (e.g., protective gear, firefighting equipment)
- III. Chemical Products:
 - Household chemicals (e.g., cleaning agents, detergents)
 - Industrial chemicals (e.g., adhesives, coatings)
 - Hazardous substances (e.g., flammable materials, corrosive substances)

IV. Construction and Building Materials:

- Structural materials (e.g., steel, concrete)
- Insulation materials (e.g., thermal, acoustic)
- Plumbing and sanitary products (e.g., pipes, fixtures)

V. Textiles and Apparel:

- Clothing and garments
- Home textiles (e.g., bedding, curtains)
- Industrial textiles (e.g., geotextiles, protective fabrics)

VI. Toys and Children's Products:

- Toys and games
- Childcare articles (e.g., strollers, car seats)
- School supplies (e.g., stationery, backpacks)

VII. Medical Devices and Health Products:

- Diagnostic equipment (e.g., thermometers, blood pressure monitors)
- Therapeutic devices (e.g., physiotherapy equipment, surgical instruments)
- Health supplements and personal care products

VIII. Automotive Products:

- Motor vehicles (e.g., cars, motorcycles)
- Automotive parts and accessories (e.g., tires, batteries)
- Safety systems (e.g., airbags, seat belts)

IX. Food and Beverages:

- Processed foods (e.g., snacks, canned goods)
- Beverages (e.g., soft drinks, alcoholic beverages)
- Food additives and ingredients

X. Environmental Products:

- Waste management equipment (e.g., recycling systems, waste bins)
- Water treatment products (e.g., filters, purifiers)
- Renewable energy products (e.g., solar panels, wind turbines)

India

Official Certification Authorities

Automotive Research Association of India (ARAI)

Bureau of Indian Standards (BIS)

Telecommunication Engineering Centre (TEC)

The Wireless Planning and Coordination of India (WPC) - National Broadcasting Authority and part of Ministry of Communications and Information Technology

Certification Schemes

TAC Type Approval (TAC) and Automotive Indian Standards (AIS) are mandatory certification schemes for vehicles and vehicle components and automotive products in India. TAC/AIS certification will not be discussed in this Guidebook.

The Bureau of Indian Standards (BIS) is mandatory safety certification for specific electronic products. The ISI mark and the standard mark are shown below:



TEC designed Mandatory Testing and Certification of Telecom Equipment (MTCET) which covers 46 types of telecom products.



WPC certificate is mandatory for LPWAN (e.g., ZigBee, Lora), Bluetooth, Wi-Fi, and other wireless products. This certification scheme also accepts RF test report for EN300328.

WPC issues:

*Equipment Type Approval (ETA) - relevant to most cases

Import Licences for radio equipment



Details of Certification Schemes

Test reports from other accredited laboratories may also be accepted for certain types of products (which will have to be considered on an individual basis).

BIS

The Bureau of Indian Standards (BIS) has published the “List of Products and Associated Indian Standards” on its official website: <https://bis.gov.in/>. Only electronics related items are listed below.

- Transformers
- Ceiling fans and fan regulators
- Circuit breakers
- Flameproof enclosures
- Three-phase and single-phase A.C. motors
- Plugs, sockets and switches
- PVC cables
- Geysers
- Electrical energy metres
- Luminaires, LED bulbs, modules
- Hearing aids
- Camera devices for video surveillance systems
- Optical fibre cables
- Coaxial cables

TEC-MTCTE

Any electronic or telecommunication equipment that is used or capable of being implemented/deployed/used by any telecommunication establishment have to undergo MTCTE as per the respective essential requirements (ERs) published by the telegraph authority from time to time.

Products listed under TEC-MTCTE:

- Networks (2-wire telephone equipment, modems, cordless telephones, etc.)
- IoT/M2M (smart devices, IoT gateways, etc.)
- Fixed accesses
- Information technology (switches, routers, servers, etc.)
- Mobile devices
- Radios (VHF, UHF, equipment operating in 2.4 GHz and 5 GHz, satellite systems, etc.)
- PON families of broadband equipment
- Transmission terminal equipment
- Feedback devices

WPC

Products with a WPC-approved radio module do not require additional testing, but those products should be registered via WPC.

- Aerials
- Antennas
- Directional radio microwave links
- Feeders
- Network objects (channel switches, base telecommands, etc.)
- Radio navigational apparatuses (beacons, navigation management, etc.)
- Receivers (GPS, VHF receivers, communication receivers, etc.)
- Transceivers (modems, radar transponders, Wi-Fi equipment, WLAN, etc.)
- Transmitters (wireless access points, routers, etc.)

Australia and New Zealand

The Regulatory Compliance Mark (RCM) is a trademark owned by the electrical regulator (Regulatory Authorities (RAs)) and Australian Communications Media Authority (ACMA). The RCM is a certification mark used in Australia and New Zealand to indicate that a product complies with the relevant electrical safety, electromagnetic compatibility (EMC), and wireless telecommunication standards. The RCM is administered by the ACMA and is recognised across both countries as a symbol of regulatory compliance.

The RCM replaces the old A-Tick and C-Tick compliance marks. It is mandatory requirement for electrical and electronic products sold into the Australian and New Zealand markets. Under the RCM scheme, there are five main labelling notices based on product groupings: telecommunications, radiocommunications, EMC, safety, and EMR. Each notice group has specific technical standards for testing and documentation and serves as a guide for designing and implementing compliance programmes.



Here are the key aspects of the RCM:

1. Scope:
 - The RCM applies to a wide range of products, including electrical and electronic devices, telecommunications equipment, and radio communications products.
2. Compliance Requirements:
 - Electrical Safety: Products must meet the electrical safety standards as specified by the relevant regulatory authorities in Australia and New Zealand.
 - EMC: Products must comply with the electromagnetic compatibility requirements to ensure they do not cause or are not susceptible to electromagnetic interference.
 - Radio and Telecommunication: Products with wireless communication functions must comply with the relevant radio frequency and telecommunication standards.
3. Use of the RCM:
 - The RCM can be used only by suppliers who have demonstrated compliance with the applicable regulations and have registered with the ACMA.
 - The mark must be affixed to the product, packaging, or accompanying documentation in a visible and durable manner.
4. Supplier's Declaration of Conformity (SDoC):
 - Suppliers must complete a Supplier's Declaration of Conformity, indicating that the product meets the relevant standards.
 - This declaration must be supported by evidence of compliance, such as test reports and certification documents.
5. Registration:
 - Suppliers must register with the Electrical Regulatory Authorities Council (ERAC) for electrical safety and with the ACMA for telecommunications and EMC compliance.
 - Registration involves providing details about the supplier and the products they intend to market.
6. Enforcement:
 - Regulatory authorities conduct market surveillance and compliance checks to ensure that products bearing the RCM meet the required standards.
 - Non-compliance can result in penalties, product recalls, or other enforcement actions.

Europe

"CE" originated from the French abbreviation of the European Community, "Conformité Européenne", which is a safety conformity mark widely recognised in Europe (not limited to EU member states). In the EU market, the CE mark is a compulsory certification mark. Whether it is products produced by companies in the EU or products produced in other countries/regions, if you want your product to circulate freely on the EU market, you must affix the CE mark. The CE marking is only obligatory for products for which EU specifications exist and require the affixing of CE marking.

CE is composed of multiple directives, the common ones are RED directive, LVD directive, EMC directive, RoHS directive, REACH, and so on. The CE marking is required in 29 European Economic Area (EEA) Countries:

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Iceland
15. Ireland
16. Italy
17. Latvia
18. Lithuania
19. Luxembourg
20. Malta
21. Netherlands
22. Norway
23. Poland
24. Portugal
25. Romania

26. Slovakia
27. Slovenia
28. Spain
29. Sweden



Radio Equipment Directive (RED):

Refers to wireless communication equipment, such as: SRD products, mobile communication products, wireless smart terminal equipment, cordless phones, ISDN equipment, PMR equipment, wireless broadcast receiving equipment, etc.

Electromagnetic Compatibility Directive (EMC):

Refers to Electromagnetic Compatibility Directives, such as: household appliances, IT/AV equipment, multi-media equipment, medical and scientific equipment, aviation and navigation wireless equipment, lamps, etc.

Low Voltage Directive (LVD):

Refers to the Low Voltage Directive, including:

1. All electrical equipment that require alternating current with a rated voltage range of 50 to 1000 volts;
2. Electrical equipment, with a rated voltage range of 75 to 1500 volts, DC.

Restriction of the use of certain hazardous substances (RoHS):

This directive restricting the use of certain hazardous substances covers a wide range of products, including electronic, electrical, medical, communications, toys, security information, and other products, as well as the parts, raw materials, and packaging used in the production of completed machines.

United States

The Federal Communications Commission (FCC) regulates the use of radio frequency (RF) devices in the United States, including healthcare and wellness devices that incorporate wireless communication technologies. These devices must comply with FCC requirements to ensure they do not cause harmful interference and meet specific safety standards.



Equipment Authorisation:

Healthcare and wellness devices that use RF communication must undergo an equipment authorisation process before they can be marketed or sold in the United States. The FCC has three main types of equipment authorisation:

- **Certification:** This is the most stringent approval process and is required for most RF devices, including those used in healthcare. It involves testing the device in an FCC-recognised accredited laboratory and submitting the test results to a Telecommunication Certification Body (TCB) for review and approval.
- **Declaration of Conformity (DoC):** This process applies to certain digital devices and involves testing the device in an accredited lab, followed by a supplier's declaration that the device meets FCC standards.
- **Verification:** This is a self-approval process where the manufacturer tests the device to ensure it complies with FCC standards. This method is generally used for devices with less potential for causing interference.

Labelling and User Information:

Devices that have been authorised by the FCC must be properly labelled with the FCC ID number and any other required information. Additionally, the user manual must include information about the device's compliance with FCC rules, instructions on how to operate the device without causing interference, and information on RF exposure compliance, if applicable.

Importation and Marketing:

Manufacturers and importers must ensure that all healthcare and wellness devices comply with FCC requirements before they are imported into or offered for sale in the United States. Non-compliant devices can be subject to enforcement actions, including fines and product seizures.

Canada

Healthcare and wellness devices that incorporate wireless communication technologies or emit radio frequency (RF) energy must comply with the requirements set by Innovation, Science and Economic Development Canada (ISED), formerly known as Industry Canada. These requirements ensure that devices do not cause harmful interference and meet safety standards.

Medical devices shall comply the list of recognised standards of ISED. The list of recognised standards can be referred to on the website of the list of recognised standards of ISED as follows:

<https://www.canada.ca/en/health-canada/programs/consultation-proposed-changes-medical-devices-directorate-list-recognized-standards-medical-devices/document.html>



Certification:

Healthcare and wellness devices that use RF communication must undergo a certification process before they can be marketed or sold in Canada. The certification process involves:

- **Testing:** Devices must be tested for compliance with ISED standards by an ISED-recognised accredited testing laboratory.
- **Technical Standards:** Devices must comply with the relevant Radio Standards Specifications (RSS) and Interference-Causing Equipment Standards (ICES). For example, RSS-210 covers licence-exempt radio apparatus, and RSS-102 covers RF exposure compliance.
- **Submission:** Test results and other required documentation must be submitted to ISED or a Certification Body (CB) recognised by ISED for review and approval.

Labelling and User Information:

Devices that have been certified by ISED must be properly labelled with the ISED certification number and any other required information. Additionally, the user manual must include information about the device's compliance with ISED rules, instructions on how to operate the device without causing interference, and information on RF exposure compliance, if applicable.

Importation and Marketing:

Manufacturers and importers must ensure that all healthcare and wellness devices comply with ISED requirements before they are imported into or offered for sale in Canada. Non-compliant devices can be subject to enforcement actions, including fines and product recalls.

United Kingdom of Great Britain

The UK Conformity Assessed (UKCA) marking is the product marking used for goods being placed on the market in Great Britain (England, Scotland, and Wales) to indicate that they conform to the relevant UK regulations. Healthcare and wellness devices, including medical devices, must comply with specific requirements to bear the UKCA marking.



Medical Devices Regulations:

Healthcare and wellness devices that qualify as medical devices must comply with the UK Medical Devices Regulations 2002 (as amended), which transpose the EU Medical Devices Directives into UK law. Covered in the Regulations are:

- General Medical Devices: These are covered under the UK Medical Devices Regulations 2002.
- In Vitro Diagnostic Medical Devices (IVDs): These are also covered under the UK Medical Devices Regulations 2002.
- Active Implantable Medical Devices: These are covered under the Active Implantable Medical Devices Regulations 2002.

Labelling and Instructions for Use:

Devices must be labelled with the UKCA marking and include necessary information such as:

- Manufacturer's name and address
- Device name and model
- Batch or serial number
- Instructions for use

Registration with MHRA:

Manufacturers must register their devices with the MHRA before placing them on the market. This includes providing information about the device, its intended use, and the conformity assessment procedure followed.

HEALTHCARE AND WELLNESS DEVICES TEST REQUIREMENTS IN EMC REQUIREMENT



Chapter 2 - Healthcare and Wellness Devices Test Requirements in EMC Requirement

Introduction of Electromagnetic Compatibility (EMC):

- Emission Tests: Measurement of electromagnetic emissions to ensure they do not exceed the specified limits. The tests measures both conducted emissions (emissions through power lines) and radiated emissions (emissions through the air).
- Immunity Tests: Assessment of the device's immunity to electromagnetic interference from external sources. Such tests include tests for electrostatic discharge (ESD), radiated immunity, conducted immunity, and other relevant immunity tests.

China:

The China Compulsory Certificate (CCC or 3C) certification is a mandatory certification system in China that applies to a wide range of products, including certain healthcare and wellness devices. The CCC certification ensures that products meet the Chinese standards for safety, quality, and electromagnetic compatibility (EMC). Here are the key EMC requirements and standards for the CCC certification of healthcare and wellness devices:

Applicable EMC Standards: Emission Requirements:

GB/T 4824-2019 《工业、科学和医疗设备射频骚扰特性限值和测量方法》

(equivalent to CISPR 11: 2016)

GB/T 9254.1-2021 《資訊技術設備、多媒體設備和接收器的電磁相容性第 1 部分：傳輸要求》

(equivalent to CISPR 32:2015)

GB17625.1-2022 《電磁相容限值諧波電流發射限值（設備每相輸入電流 $\leq 16A$ ）》

(equivalent to IEC 61000-3-2:2020)

GB17625.2-2007 《电磁兼容限值对每相额定电流 $\leq 16A$ 且无条件接入的设备在公用低压供电系统中产生的电压变化、电压波动和闪烁的限制》

(equivalent to IEC 61000-3-3: 2005)

Immunity Requirements:

GB/T 9254.2-2021 《信息技术设备、多媒体设备和接收机电磁兼容第 2 部分：抗扰度要求》

(equivalent to CISPR 35: 2016)

Japan

In Japan, healthcare and wellness devices that incorporate electronic components must comply with specific Electromagnetic Compatibility (EMC) requirements and standards to ensure they do not cause harmful interference and are immune to certain levels of electromagnetic disturbances. The key EMC requirements and standards for Japan certification of healthcare and wellness devices are as follows:

1. Regulatory Bodies:

Ministry of Internal Affairs and Communications (MIC): Responsible for the regulation of radio frequency (RF) emissions and EMC for electronic devices

Ministry of Health, Labour and Welfare (MHLW): Oversees the regulation of medical devices, including their safety and performance standards

2. EMC Standards:

Healthcare and wellness devices must comply with the following Japanese Industrial Standards (JIS) and other relevant standards:

JIS T 0601-1-2: 医用電気機器－第 1 － 2 部：基礎安全及び基本性能に関する一般要求事項－副通則：電磁妨害－要求事項及び試験

Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests

Emission Requirements:

J55032(H29) マルチメディア機器の電磁両立性－エミッション要求事項－

(equivalent to CISPR 32: 2015:2nd)

JIS C 61000-3-2:2019 電磁両立性-第 3-2 部：限度値-高調波電流発生限度値

(1 相当たりの入力電流が 20 A 以下の機器)

(equivalent to IEC 61000-3-2: 2018 (MOD))

South Korea

In South Korea, healthcare and wellness devices that incorporate electronic components must comply with specific Electromagnetic Compatibility (EMC) requirements and standards to ensure they do not cause harmful interference and are immune to certain levels of electromagnetic disturbances. The regulatory framework for EMC in South Korea involves several key standards and certification processes.

EMC Standards:

KS C 9812: Electromagnetic compatibility requirements for medical electrical equipment, which aligns with IEC 60601-1-2

Emission Requirements:

KS C 9811:2019 - Electromagnetic compatibility requirements for medical electrical equipment, which aligns with IEC 60601-1-2

KS C 9832: 2019 멀티미디어기기 전자파 장애방지 시험 (equivalent to CISPR 32)

KS C 9610-3-2:2020 공공 저압 배전망에서의 고조파 전류 방출 측정 (equivalent to IEC 61000-3-2)

KS C 9610-3-3:2020 공공 저압 배전망에서의 전압변동 및 플리커 측정 (equivalent to IEC 61000-3-3)

Immunity Requirement:

KS C 9835:2019 멀티미디어기기 전자파 내성 시험 (equivalent to CISPR 35)

Australia and New Zealand

In Australia and New Zealand, Electromagnetic Compatibility (EMC) requirements for medical and healthcare devices are governed by regulations that ensure these devices operate safely and effectively without causing or being affected by electromagnetic interference. The Therapeutic Goods Administration (TGA) is responsible for regulating medical devices, including their EMC requirements, in Australia. Medsafe, under the Ministry of Health, is the regulatory authority for medical devices in New Zealand. Manufacturers must ensure that their healthcare or medical devices meet the essential principles of safety and performance as outlined by the TGA and Medsafe.

Standard Requirements:

IEC 60601-1-2: "Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests"

Emission Limits: Medical devices must not emit electromagnetic disturbances that could interfere with other equipment. The limits are specified in IEC 60601-1-2.

Immunity Requirements: Medical devices must have adequate immunity to electromagnetic disturbances to ensure they function correctly in their intended environment. This includes immunity to electrostatic discharge, radiated radio-frequency electromagnetic fields, electrical fast transients, surges, conducted disturbances, and voltage dips and interruptions.

Risk Management: Manufacturers must conduct a risk assessment to determine the potential risks associated with electromagnetic disturbances and implement appropriate measures to mitigate these risks.

Saudi Arabia

In Saudi Arabia, the regulatory requirements for Electromagnetic Compatibility (EMC) of medical and healthcare devices are governed by the Saudi Food and Drug Authority (SFDA). The SFDA ensures that medical devices meet specific safety, performance, and EMC standards to prevent electromagnetic interference that could affect the device's operation or other equipment. The SFDA is the main regulatory body overseeing medical devices, including their EMC requirements. Manufacturers must ensure that their devices meet the essential principles of safety and performance as outlined by the SFDA.

Standard Requirements:

The SFDA mandates compliance with international EMC standards, particularly those developed by the International Electrotechnical Commission (IEC). The primary standard for EMC in medical devices is:

IEC 60601-1-2: "Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests"

Emission Limits: Medical devices must not emit electromagnetic disturbances that could interfere with the operation of other equipment. The limits for emissions are specified in IEC 60601-1-2.

Immunity Requirements: Medical devices must have adequate immunity to electromagnetic disturbances to ensure they function correctly in their intended environment. This includes immunity to electrostatic discharge, radiated radio-frequency electromagnetic fields, electrical fast transients, surges, conducted disturbances, and voltage dips and interruptions.

Risk Management: Manufacturers must conduct a risk assessment to identify potential risks associated with electromagnetic disturbances and implement appropriate measures to mitigate these risks.

Europe

The European Commission of Electromagnetic Compatibility (EMC) Directive 2014/30/EU ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance. The EMC directive limits electromagnetic emissions from equipment in order to ensure that, when used as intended, such equipment does not disturb radio and telecommunication, as well as other equipment. The directive also governs the immunity of such equipment to interference and seeks to ensure that this equipment is not disturbed by radio emissions, when used as intended.

The Medical Device Regulation (MDR) (EU) 2017/745 is a comprehensive regulatory framework established by the European Union (EU) to ensure the safety, performance, and quality of medical devices marketed and used within the EU. The MDR replaces the previous Medical Device Directive (MDD) (93/42/EEC) and the Active Implantable Medical Devices Directive (AIMDD) (90/385/EEC), bringing significant changes to the regulatory landscape for medical devices.

The main objectives of the directives are to regulate the compatibility of equipment regarding EMC to ensure that healthcare equipment, IoT apparatus, and medical devices comply with EMC requirements when it is placed on the market or taken into service.

Emission Requirements:

Healthcare and wellness devices must comply with the following:

EN 55032:2015/A11:2020 Electromagnetic compatibility of multimedia equipment - Emission Requirements

EN 61000-3-2:2014 Electromagnetic compatibility (EMC) – Part 3-2: Limits - Limits for harmonic current emissions (equipment input current ≤ 16 A per phase)

EN 61000-3-3:2013 Electromagnetic compatibility (EMC) – Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low voltage supply systems, for equipment with rated current ≤16 A per phase and not subject to conditional connection

Immunity Requirements:

Healthcare and wellness devices must comply with the following:

EN 55035:2017/A11:2020 Electromagnetic compatibility of multimedia equipment - Immunity requirements

Medical devices/equipment must comply with the following:

IEC 60601-1-2: "Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral Standard: Electromagnetic disturbances – Requirements and tests"

United Kingdom:

In the United Kingdom, the Electromagnetic Compatibility (EMC) requirements for medical and healthcare devices are governed by regulations that ensure these devices operate safely and effectively without causing or being affected by electromagnetic interference. Following Brexit, the UK has established its own regulatory framework, although it largely mirrors the European Union's standards. The applicable regulations are: Medical Devices Regulations 2002 (SI 2002 No 618, as amended) – incorporating EU MDR/IVDR principles and Electromagnetic Compatibility Regulations 2016 (SI 2016 No 1091) – which implement EMC requirements.

Emission Requirements:

Healthcare and wellness devices must comply with the following:

EN 55032:2015/A11:2020 Electromagnetic compatibility of multimedia equipment - Emission Requirements

EN 61000-3-2:2014 Electromagnetic compatibility (EMC) – Part 3-2: Limits - Limits for harmonic current emissions (equipment input current ≤ 16 A per phase)

EN 61000-3-3:2013 Electromagnetic compatibility (EMC) – Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low voltage supply systems, for equipment with rated current ≤ 16 A per phase and not subject to conditional connection

Immunity Requirements:

EN 55035:2017 Electromagnetic compatibility of multimedia equipment - Immunity requirements

Medical devices must meet harmonised EMC standards under UK law. The key standards include:

EN/IEC 60601-1-2: Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic disturbances – Requirements and tests

Covers immunity to electromagnetic disturbances (e.g., RF interference, electrostatic discharge) and emissions

EN 55011 / CISPR 11: For industrial, scientific, and medical (ISM) equipment radio disturbance characteristics

United States:

In the United States, the Electromagnetic Compatibility (EMC) requirements for medical and healthcare devices are governed by the Food and Drug Administration (FDA). The FDA ensures that medical devices are safe and effective, including their ability to operate without causing or being susceptible to electromagnetic interference. The Federal Communications Commission (FCC) regulates electromagnetic emissions under Title 47 of the Code of Federal Regulations (CFR) for devices that intentionally or unintentionally emit radiofrequency (RF) energy. The FDA recognises several international and national standards for EMC, with the primary standard for medical devices being:

ANSI/AAMI/IEC 60601-1-2: Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic disturbances – Requirements and tests

FCC Regulations (For Devices with RF Emissions):

FCC Part 15 (47 CFR Part 15) – For unintentional radiators (e.g., digital circuitry)

FCC Part 18 (47 CFR Part 18) – For industrial, scientific, and medical (ISM) equipment that intentionally generates RF energy (e.g., diathermy, MRI)

FDA Guidance Documents: "Electromagnetic Compatibility (EMC) of Medical Devices" (2016, updated 2021) provides recommendations for testing and risk management.

Canada:

In Canada, the Electromagnetic Compatibility (EMC) requirements for medical and healthcare devices are governed by Health Canada, the federal department responsible for national health policy. Health Canada ensures that medical devices marketed in Canada are safe, effective, and comply with relevant standards, including those related to EMC.

Medical devices must comply with:

a) CAN/CSA-IEC 60601-1-2: Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic disturbances – Requirements and tests

b) Industry Canada (ISED) Requirements (if applicable)

Devices with radiofrequency (RF) emissions (e.g., wireless medical devices) must comply with Innovation, Science and Economic Development Canada (ISED) regulations:

RSS-210 (for license-exempt RF devices)

RSS-102 (RF exposure compliance)

HEALTHCARE AND WELLNESS DEVICES TEST REQUIREMENTS IN CYBERSECURITY



Chapter 3 - Healthcare and Wellness Devices Test Requirements in Cybersecurity

1. Introduction

The healthcare and wellness devices market continues to expand rapidly. According to Gartner, the market for these devices is projected to grow significantly, reaching millions of endpoints in the coming years. As more healthcare and wellness devices connect to the Internet, research indicates that a substantial portion of active connected devices worldwide will be dedicated to this sector. With these growing trends, healthcare and wellness device connections are set to become a significant part of the Internet cyberspace.

Cybersecurity has long been a critical concern in information technology (IT) systems, and the landscape of cyberattacks is constantly evolving. Threat actors continually adapt their tactics, employing phishing attacks themed around current affairs and trending topics. Ransomware has also evolved, targeting critical infrastructure and expanding to multiple extortions. To defend against cyberattacks, IT systems can adopt internationally recognised standards, and a variety of IT security solutions are available. However, unlike traditional IT systems, healthcare and wellness devices present unique challenges in implementing security measures. Their hardware limitations and specific characteristics make them inherently vulnerable, posing distinct challenges and constraints to overcome in cybersecurity.

This chapter will provide an overview of cybersecurity threats to healthcare and wellness devices and explore the current status of the latest security requirements, best practices, and standards in this field.

2. Cyber Security Threats to Healthcare and Wellness Devices

2.1 Landscape of Healthcare Cybersecurity

To understand the cyber security threats to healthcare and wellness devices, we first have to look at the landscape of healthcare cybersecurity. The landscape of healthcare cybersecurity is built with four key elements, namely information assurance, cyber physical systems & operational technology, Internet of Things (IoT) devices and IT infrastructure.

The healthcare cybersecurity landscape encompasses various technologies and systems that handle sensitive patient data and critical medical operations. Key components include:

Information Assurance: Focuses on protecting patient paper records and electronic Protected Health Information (ePHI) under regulations like HIPAA, ensuring confidentiality, integrity, and availability

Cyber-Physical Systems and Operational Technology: Includes medical devices (e.g., pacemakers), surgical implants, robotics, and medical software. These systems are vulnerable to cyberattacks that could disrupt patient care or compromise safety

Internet of Things (IoT): Covers fitness devices and wellbeing applications, which collect health data but often lack robust security, posing privacy risks

IT Infrastructure: Manages ePHI and other digital records, requiring strong cybersecurity measures to prevent breaches and ransomware attacks

The healthcare and wellness devices sector faces unique cybersecurity challenges due to the convergence of IT, operational technology, and IoT. Protecting ePHI, securing medical devices, and ensuring the resilience of critical systems are paramount. As cyber threats evolve, healthcare organisations must adopt comprehensive security frameworks, employee training, and advanced technologies to safeguard patient data and maintain trust. The landscape underscores the need for collaboration between regulators, manufacturers, and providers to mitigate risks effectively.

2.2 Cyber Security Threats

The healthcare and wellness industry is increasingly reliant on digital technologies to improve patient care, streamline operations, and enhance connectivity. However, this digital transformation has also made the sector a prime target for cybercriminals. Healthcare organisations handle vast amounts of sensitive data, including personal health information (PHI), financial records, and critical infrastructure, making them attractive to attackers. The consequences of cyber threats in this sector are severe, ranging from compromised patient safety to financial losses and reputational damage.

This section examines the top cyber threats facing the healthcare and wellness sector. These threats include phishing, data breaches, ransomware, DDoS attacks, insider threats, vulnerabilities on the Internet of Medical Things (IoMT), and supply chain risks. Additionally, this section also explores the root causes of ransomware attacks and common initial access methods used by cybercriminals. By understanding these threats, healthcare organisations can implement robust security measures to protect their systems and patients.

2.2.1 Phishing

Phishing remains one of the most prevalent cyber threats in healthcare. Attackers use deceptive emails, messages, or links to trick employees into revealing sensitive information or downloading malware. In 2023, phishing—particularly via malicious links—was the most common initial access method for healthcare cyberattacks, accounting for 23% of incidents (as per the attached slide). Successful phishing attacks can lead to unauthorised access to patient records, financial fraud, and further malware infections.

2.2.2 Data Breaches

Data breaches involve unauthorised access to confidential information, such as patient records, insurance details, and employee data. The healthcare sector is particularly vulnerable due to the high value of PHI on the black market. The attached slide on healthcare data breaches (2009–2024) shows a fluctuating but persistent trend, with peaks in certain years (e.g., 715 breaches in 2011 and 745 in 2012). Causes include weak encryption, unsecured databases, and insider negligence.

2.2.3 Ransomware

Ransomware attacks encrypt critical data and demand payment for its release. Healthcare is a frequent target because disruptions can directly impact patient care. The root causes of ransomware attacks highlight several contributing factors, including:

- Unpatched vulnerabilities: Failure to update software exposes systems to exploits
- Human error: Employees may inadvertently download malware
- Phishing: A common delivery method for ransomware

The financial and operational impact of ransomware can be devastating, forcing hospitals to revert to manual processes or pay hefty ransoms.

2.2.4 DDoS Attacks

Distributed Denial of Service (DDoS) attacks overwhelm healthcare networks with traffic, rendering systems unusable. These attacks can disrupt telehealth services, appointment scheduling, and access to electronic health records (EHRs). While not always aimed at data theft, DDoS attacks can serve as smokescreens for other malicious activities.

2.2.5 Insider Threats

Insider threats arise from employees, contractors, or partners who misuse their access to systems. These threats can be malicious (e.g., stealing data for profit) or accidental (e.g., falling for phishing scams). The slide on initial access methods notes that 8% of incidents in 2023 involved valid insider accounts. Proper access controls and monitoring are essential to mitigate this risk.

2.2.6 Internet of Medical Things (IoMT) Vulnerabilities

IoMT devices, such as insulin pumps, heart monitors, and MRI machines, are increasingly connected to networks. However, many lack robust security features, making them easy targets. Compromised IoMT devices can lead to:

- Data interception: Attackers can steal real-time patient data.
- Device manipulation: Malicious actors may alter settings, endangering lives.
- Network infiltration: Weak devices can serve as entry points for broader attacks.

2.2.7 Supply Chain Risks

Healthcare organisations rely on third-party vendors for software, hardware, and services. A breach in a vendor's system can cascade to healthcare providers. For example, the 2020 SolarWinds attack affected multiple sectors, including healthcare. Ensuring vendor compliance with security standards is critical.

3. Classification of Internet of Medical Things (IoMT)

The Internet of Medical Things (IoMT) has revolutionised healthcare by enabling connected devices to monitor, diagnose, and treat patients more efficiently. However, the increasing reliance on these technologies has also exposed critical vulnerabilities, making them prime targets for cyberattacks. This section explores the different types of IoMT devices, their ecosystems, and the growing cybersecurity threats they face. It also highlights real-world vulnerabilities, attack methods, and the exposure of medical assets on public networks, emphasising the urgent need for robust security measures in healthcare technology.

3.1 Types of Internet of Medical Things (IoMT) Devices

The Internet of Medical Things (IoMT) encompasses a wide range of connected devices that enhance patient care, diagnostics, and treatment. These devices are categorised based on their functionality and application in healthcare:

- **Connected Imaging Devices:** These include MRI machines, X-ray systems, and ultrasound devices that transmit diagnostic images to healthcare providers, enabling remote consultations and faster diagnoses.
- **Smart Medical Devices:** Advanced tools like AI-powered diagnostic assistants, robotic surgery systems, and smart inhalers improve precision in treatment while collecting real-time patient data.
- **Implantable Medical Devices:** Pacemakers, neurostimulators, and insulin pumps fall under this category, offering life-saving functions but also posing risks if hacked.
- **Patient-monitoring Devices:** Wearables like ECG monitors, pulse oximeters, and continuous glucose monitors (CGMs) track vital signs, alerting medical staff to emergencies.
- **Ingestible Sensors:** Pill-sized sensors monitor medication adherence and internal health metrics, transmitting data to physicians.
- **Fitness Trackers:** While not strictly medical, devices like smartwatches and activity bands contribute to preventive healthcare by tracking heart rate, sleep patterns, and physical activity.

These IoMT devices improve efficiency and patient outcomes but also introduce cybersecurity risks, as many lack robust encryption and are vulnerable to hacking, data breaches, and ransomware attacks. Ensuring their security is critical to safeguarding patient health and privacy.

3.2 IoMT Ecosystems

The Internet of Medical Things (IoMT) ecosystem is a complex network of interconnected components that enable seamless communication between medical devices, healthcare providers, and patients. This ecosystem consists of several critical elements:

- **Networks:** Secure communication channels, including Wi-Fi, Bluetooth, and 5G, facilitate real-time data exchange between devices and healthcare systems.
- **Middleware & Applications:** These act as intermediaries, ensuring interoperability between different IoMT devices and electronic health record (EHR) systems. Middleware also processes and filters data before transmission to reduce latency and errors.
- **Smart Medical Devices:** Equipped with embedded sensors and trackers, these devices collect patient data (e.g., heart rate, blood pressure) and transmit them for analysis. Examples include wearable monitors, infusion pumps, and connected ventilators.
- **Gateways:** These serve as security checkpoints, encrypting data before they move from local networks to cloud-based storage or hospital servers. Gateways also prevent unauthorised access by filtering malicious traffic.

The IoMT ecosystem enhances remote patient monitoring, telemedicine, and predictive analytics, improving healthcare efficiency. However, its interconnected nature introduces risks—unsecured networks, outdated middleware, and vulnerable gateways can be exploited by cybercriminals. Strengthening encryption, access controls, and regular firmware updates is essential to protect sensitive medical data and ensure uninterrupted care.

3.3 State of Cybersecurity in Medical Devices

The cybersecurity landscape for medical devices presents growing concerns as connectivity increases vulnerability to sophisticated threats. Recent trends reveal:

- **Escalating Vulnerabilities:**
 - A 300% increase in reported medical device vulnerabilities since 2018
 - Average of 6 critical vulnerabilities discovered per device model
 - 40% of vulnerabilities allowing remote code execution
- **Active Threat Landscape:**
 - Ransomware attacks targeting healthcare increased by 94% in 2023
 - Medical devices account for 53% of compromised healthcare endpoints
 - Average dwell time of 287 days before detection
- **Regulatory Challenges:**
 - FDA reports 60% of medical devices operate on legacy OS (Windows 7 or older)
 - Only 35% of manufacturers provide timely security patches
 - 72% of hospitals lack dedicated medical device security teams
- **High-Risk Device Categories:**
 - Imaging systems (CT/MRI) - 42% vulnerable to DICOM exploits
 - Infusion pumps - 75% susceptible to wireless hijacking
 - Patient monitors - 68% vulnerable to false data injection

The convergence of outdated systems, complex networks, and life-critical functions creates a perfect storm for cyber threats, demanding urgent action from manufacturers and healthcare providers alike.

3.4 Cybersecurity Threats and Exposures in Internet of Medical Things (IoMT)

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a growing number of Industrial Control System (ICS) medical advisories, with a 140% increase from 2019-2024. These alerts predominantly address critical vulnerabilities in infusion pumps, patient monitors, and imaging systems, with 68% rated as high-severity threats requiring immediate remediation.

- Exploiting Medical Device Vulnerabilities

Security researchers have demonstrated alarming attack vectors against connected medical devices:

- Real-world cases show patient monitors can be manipulated to display false vitals
- Infusion pumps vulnerable to dosage alteration attacks
- Imaging systems susceptible to data manipulation
- Ransomware can encrypt life-critical devices during procedures
- Notably, 83% of these exploits require minimal technical skill, leveraging default credentials or unpatched vulnerabilities. The FDA has recalled 17 devices since 2020 due to uncompensable security flaws, highlighting the life-or-death stakes of medical device cybersecurity.

- Medical Asset Internet Exposure

Shodan scans reveal over 150,000 exposed medical assets globally:

- 42,000 PACS/DICOM servers with patient images
- 28,000 EHR/EMR interfaces
- 15,000 medical IoT gateways. Particularly concerning are:
 - 12% of exposed systems contain unencrypted PHI
 - 23% use deprecated protocols (FTP/Telnet)
 - 7% still run Windows XP

The healthcare sector averages 3.5x more exposed assets than financial services, with hospital networks the most frequent targets. These exposures enable everything from data theft to potential device manipulation, emphasising the urgent need for network segmentation and access controls.

4. Cybersecurity Standards for Healthcare and Wellness Devices

The cybersecurity of healthcare and wellness devices is governed by three foundational international standards that establish rigorous requirements for risk management, software development, and product security:

4.1 ISO 14971:2019 - Medical Device Risk Management:

- Provides a comprehensive framework for identifying potential hazards associated with medical devices

- Requires manufacturers to implement risk control measures proportional to the severity of potential harm
- Mandates ongoing post-production monitoring and risk reassessment
- Explicitly includes cybersecurity risks in its scope since the 2019 update
- Aligns with FDA guidance on cybersecurity risk management

4.2 IEC 62304:2006 - Medical Device Software Lifecycle Processes

- Establishes a risk-based classification system (Class A-C) for medical software
- Defines stringent requirements for software development processes
- Requires comprehensive documentation including software requirements, architecture, and verification plans
- Includes specific provisions for legacy software maintenance and updates
- Mandates software risk management aligned with ISO 14971

4.3 UL 2900 Series - Cybersecurity Certification Programme

- Provides testable cybersecurity requirements for network-connectable devices
- UL 2900-2-1 specifically addresses healthcare and medical systems
- Evaluates critical security aspects including:
 - Authentication and authorisation controls
 - Secure communications and encryption
 - Vulnerability and patch management
 - Malware protection capabilities
- Includes requirements for secure software update mechanisms

4.4 Best Practices (HKCERT) for Securing IoMT Devices

Securing Internet of Medical Things (IoMT) devices requires a comprehensive, multi-layered approach that integrates technical controls, operational policies, and continuous monitoring. The foundation begins with device hardening and configuration management, where secure-by-design principles are implemented during development to eliminate vulnerabilities. This includes enforcing strong authentication measures such as complex password policies and role-based access controls, while systematically disabling unnecessary services and ports that could serve as attack vectors. For software integrity, a rigorous Secure Software Development Lifecycle (SDLC) must be maintained, incorporating threat modelling techniques like STRIDE methodology and regular code analysis to identify and remediate vulnerabilities early. Maintaining a detailed software bill of materials enables effective tracking of components for vulnerability management, complemented by secure, cryptographically-signed update mechanisms to ensure only authenticated patches are deployed.

Network security demands specialised protections tailored to medical environments, including strict segmentation of device traffic through VLANs and next-generation firewalls. Continuous monitoring via intrusion detection systems and comprehensive encryption of data both in transit and at rest are essential to protect sensitive patient information. For operational resilience, healthcare organisations should conduct regular penetration testing, maintain air-gapped backups of critical configurations, and provide targeted cybersecurity training for clinical staff who interact with these devices. Physical security controls must not be overlooked, as unauthorised physical access could compromise even well-secured systems.

To maintain ongoing protection, organisations should align their security programmes with established frameworks like the NIST Cybersecurity Framework while actively monitoring regulatory bulletins and participating in threat intelligence sharing communities. Establishing a formal vulnerability disclosure programme encourages responsible reporting from security researchers, creating a proactive defence posture. This holistic strategy addresses the unique challenges of medical device security by combining technical safeguards with robust policies and continuous improvement processes, ensuring both regulatory compliance and protection against evolving cyber threats in healthcare environments. The approach balances security requirements with clinical functionality needs, recognising that patient safety remains the ultimate priority in medical device cybersecurity.

4.5 Summary

To mitigate growing cyber threats in healthcare and wellness devices, adherence to international standards (ISO, IEC, UL) and best practices (HKCERT) is critical. Key takeaways include:

- Risk Management (ISO 14971) ensures device safety from design to decommissioning
- Secure Software Development (IEC 62304) prevents vulnerabilities in medical software
- Network Security (UL 2900-2-1) protects connected devices from exploitation
- Proactive Measures (Updates, Encryption, Access Controls) reduce attack surfaces

By implementing these solutions, providers and manufacturers can enhance cybersecurity resilience, protect patient data, and ensure compliance in an increasingly connected healthcare and wellness devices landscape.

5. Cybersecurity Solutions and Advice for Healthcare and Wellness IoT Devices

The healthcare industry's rapid adoption of Internet of Medical Things (IoMT) devices has introduced unprecedented connectivity in patient care while simultaneously expanding the attack surface for cyber threats. This section presents critical security solutions and strategic advice for both healthcare, wellness and medical device manufacturers and healthcare organisations, addressing the unique challenges of protecting connected medical ecosystems. From implementing Zero Trust frameworks to adopting defence-in-depth strategies, the recommendations outlined here provide actionable guidance to secure sensitive patient data, ensure device integrity, and maintain continuous care delivery in an increasingly hostile cyber landscape.

5.1 Security Advice for Device Manufacturers

Healthcare, wellness and medical device manufacturers must embed security throughout the entire product lifecycle, beginning with secure design principles and extending through post-market surveillance. This involves leveraging cloud-based IoT platforms for scalable device management to ensure seamless deployment of security patches and firmware updates. Manufacturers should establish robust processes for ongoing maintenance,

including regular vulnerability assessments and timely updates to address newly discovered threats. A proactive approach to lifecycle management helps mitigate risks associated with device obsolescence and ensures long-term protection against evolving cyber threats.

5.2 Security Products and Solutions for Healthcare Organisations

Healthcare providers require specialised solutions to manage their growing IoMT ecosystems effectively. Healthcare, wellness and medical device job management systems help organisations maintain an accurate inventory of connected assets while monitoring for anomalous behaviour. As recommended by Gartner Market Guide, institutions should implement advanced event detection systems capable of identifying potential security incidents in real-time. These solutions should integrate with existing healthcare IT infrastructure to provide comprehensive visibility across all connected medical devices, from infusion pumps to MRI machines.

5.3 Defence-in-Depth Strategy for Healthcare

Traditional perimeter-based security models have become inadequate in modern healthcare environments. A defence-in-depth approach combines multiple protective layers including network segmentation, endpoint security solutions, continuous monitoring systems, and comprehensive user awareness programmes. This strategy acknowledges that breaches may occur and focuses on containing potential damage through micro-segmentation of networks and strict access controls. Healthcare organisations must move beyond assumed trust models and implement verification protocols for all users, devices, and network traffic.

5.4 Implementing Zero Trust for Medical Devices

The Zero Trust model represents a paradigm shift in healthcare cybersecurity, operating on the principle of "never trust, always verify". Implementation requires three key components: First, identity management systems to control user access to sensitive resources. Second, comprehensive device discovery and continuous monitoring solutions to maintain visibility of all IoMT assets. Third, intelligent network policies that govern data flows and enforce strict segmentation between device types and clinical networks. This approach significantly reduces the attack surface by eliminating implicit trust in any element of the healthcare ecosystem.

5.4 Summary

Protecting healthcare IoT environments demands a multifaceted approach combining manufacturer responsibilities and organisational security measures. Device manufacturers must prioritise security throughout the product lifecycle, while healthcare providers need specialised solutions for asset management and threat detection. The transition from traditional perimeter defences to Zero Trust architectures reflects the evolving nature of cyber threats in medical environments.

By implementing defence-in-depth strategies and adopting continuous verification principles, healthcare organisations can better protect sensitive patient data and ensure the uninterrupted operation of critical medical devices. These combined efforts create a more resilient healthcare infrastructure capable of withstanding modern cyber threats while maintaining the highest standards of patient care and data privacy.



HEALTHCARE AND WELLNESS DEVICES TEST REQUIREMENTS IN ELECTRICAL SAFETY

Chapter 4 - Healthcare and Wellness Devices Test Requirements in Electrical Safety

Electrical Safety Always Matters in Healthcare and Wellness Devices

The safety of healthcare, wellness and medical electrical equipment is paramount in healthcare settings, where device failures could have life-threatening consequences. IEC 60601 represents the international benchmark for ensuring the safety and essential performance of medical electrical equipment. These standards have become increasingly critical as medical devices grow more complex and interconnected in our digital healthcare ecosystems.

More Smart Products, More Safety Concerns

Modern healthcare relies heavily on networked medical equipment ranging from patient monitors to robotic surgical systems. This connectivity revolution brings tremendous clinical benefits but also introduces new safety challenges. The IEC 60601 series addresses these evolving risks through comprehensive requirements covering electrical safety, electromagnetic compatibility, software reliability, and mechanical safety. As medical technology advances, compliance with these standards becomes not just a regulatory necessity but also a fundamental patient safety requirement.



Only Comprehensive Testing Can Ensure Medical Device Safety

Medical electrical equipment presents unique safety challenges due to its direct patient contact and critical healthcare functions. The IEC 60601 standards provide a systematic framework for evaluating everything from leakage currents to software validation processes. Proper testing according to these standards is the most effective way to:

- Prevent electrical hazards to patients and operators
- Ensure reliable performance of life-sustaining equipment
- Mitigate risks from electromagnetic interference
- Verify safety under both normal and single-fault conditions

Typical Requirements for Electrical Safety for Overseas Markets

EUROPE

● Medical Devices Regulation (Regulation (EU) 2017/745)

Achieving electrical safety compliance with the Medical Devices Regulation (MDR) (Regulation (EU) 2017/745) is an important part of the CE marking process. Manufacturers must demonstrate compliance with the MDR to place a CE mark on medical devices intended for sale in the European market:

■ Scope

The MDR applies to a broad range of products and activities, including:

- Medical Devices: Any instrument, apparatus, appliance, software, implant, reagent, material, or other article intended by the manufacturer to be used for human beings for specific medical purposes, such as diagnosis, prevention, monitoring, treatment, or alleviation of disease
- Accessories for Medical Devices: Products specifically intended by the manufacturer to be used together with a medical device to enable the device to be used in accordance with its intended purpose
- Certain Products Without an Intended Medical Purpose: The regulation also covers certain products that do not have a medical purpose but are similar to medical devices in terms of characteristics and risk profile, such as cosmetic contact lenses and equipment for liposuction.

■ Product Types and Classifications

The MDR classifies medical devices into four classes based on risk:

- Class I: Low risk (e.g., bandages, non-invasive instruments)
- Class IIa: Medium risk (e.g., hearing aids, surgical drapes)
- Class IIb: Higher risk (e.g., long-term corrective contact lenses, infusion pumps)
- Class III: Highest risk (e.g., implantable devices like pacemakers)

■ Standards

The MDR requires compliance with harmonised standards and common specifications to demonstrate conformity with the regulation. These standards cover various aspects, including:

- **Safety and Performance Requirements:** Devices must meet general safety and performance requirements, including chemical, physical, and biological properties, infection and microbial contamination, and construction and environmental properties. Medical devices shall comply with IEC60601 series.
- **Quality Management Systems:** Manufacturers must implement a quality management system that complies with standards such as ISO 13485.
- **Clinical Evaluation:** Devices must undergo clinical evaluation to demonstrate safety and performance, including clinical investigations for higher-risk devices.

■ Risk Assessment Requirements

Risk assessment is a critical component of the MDR, involving:

- **Risk Management Plan:** Manufacturers must establish and maintain a risk management plan throughout the product lifecycle, identifying and mitigating risks associated with the device.
- **Risk Analysis and Evaluation:** A thorough analysis and evaluation of risks must be conducted, considering the intended use and foreseeable misuse of the device.
- **Risk Control Measures:** Appropriate risk control measures must be implemented to reduce risks as far as possible without adversely affecting the benefit-risk ratio.
- **Post-Market Surveillance:** Continuous monitoring of the device's performance and safety after it has been placed on the market is required, with data used to update the risk management process.

These elements collectively ensure that medical devices placed on the EU market are safe, effective, and of high quality, protecting patient health and safety.

United States

● Safety Certifications for the United States (US) Market

In the US, the regulation and certification of medical devices are primarily governed by the Food and Drug Administration (FDA). The FDA ensures that medical devices are safe and effective for their intended use. Below are the key aspects related to the scope of safety certifications, the certification process, and the relevant standards for medical devices in the US:

■ Scope of Safety Certifications:

The FDA regulates a wide range of medical devices, which are categorised based on their intended use and the level of risk they pose to patients and users. The scope covers:

- **Medical Devices:** Instruments, apparatuses, implements, machines, contrivances, implants, in vitro reagents, or other similar or related articles, including components, parts, or accessories, intended for use in the diagnosis, treatment, mitigation, or prevention of disease or other conditions in humans or animals
- **Combination Products:** Products that combine a medical device with a drug or biological product
- **In Vitro Diagnostic Devices (IVDs):** Reagents, instruments, and systems intended for use in the diagnosis of disease or other conditions

■ Standards

Medical devices in the US must comply with various standards to ensure safety and effectiveness. Key standards include:

- **Quality Management Systems:**
ISO 13485: Medical devices—Quality management systems—Requirements for regulatory purposes
- **Risk Management:**
ISO 14971: Medical devices—Application of risk management to medical devices
- **Biocompatibility:**
ISO 10993 series: Biological evaluation of medical devices

- **Electrical Safety:**
IEC 60601 series: Medical electrical equipment—General requirements for basic safety and essential performance
- **Software:**
IEC 62304: Medical device software—Software life cycle processes
- **Usability:**
IEC 62366: Medical devices—Application of usability engineering to medical devices
- **Clinical Evaluation:**
ISO 14155: Clinical investigation of medical devices for human subjects—Good clinical practice

These standards, along with FDA regulations and guidance documents, provide a framework for ensuring that medical devices in the US are safe, effective, and of high quality.

■ **Certification Process:**

The certification process for medical devices in the US involves several steps, depending on the device classification:

Device Classification:

- Class I (Low Risk): General controls (e.g., dental floss)
- Class II (Moderate Risk): General and special controls (e.g., contact lenses)
- Class III (High Risk): Premarket approval (e.g., pacemakers)

Premarket Submission:

- **Class I Devices:** Most are exempt from premarket notification (510(k)) but must comply with general controls.
- **Class II Devices:** Typically require 510(k) clearance, demonstrating that the device is substantially equivalent to a legally marketed device
- **Class III Devices:** Require Premarket Approval (PMA), which involves a rigorous review of clinical data to ensure the device's safety and effectiveness

510(k) Clearance:

- Submit a 510(k) premarket notification to the FDA
- Demonstrate substantial equivalence to a predicate device
- FDA review and clearance

Premarket Approval (PMA):

- Submit a PMA application, including clinical trial data
- FDA review of scientific evidence to assess safety and effectiveness
- Approval granted if the device meets the necessary requirements

De Novo Classification:

- For novel devices with no predicate device, submit a De Novo request to classify the device based on risk
- FDA review and classification

Quality System Regulation (QSR):

- Comply with QSR (21 CFR Part 820), which outlines requirements for the design, manufacture, packaging, labelling, storage, installation, and servicing of medical devices

Labelling Requirements:

- Ensure labelling complies with FDA regulations, providing adequate directions for use and warnings

Post-Market Surveillance:

- Implement a post-market surveillance plan to monitor the device's performance and report adverse events

HEALTHCARE AND WELLNESS DEVICES TEST REQUIREMENTS IN QUALITY MANAGEMENT SYSTEMS AND RISK MANAGEMENT



Chapter 5 – Healthcare and Wellness Devices Test Requirements in Quality Management Systems and Risk Management

In the global healthcare, wellness and medical device industry, ensuring product safety, efficacy, and quality is paramount. Regulatory bodies across the world have established rigorous frameworks to oversee these aspects, often leveraging internationally recognised standards such as ISO 13485 for Quality Management Systems (QMS) and ISO 14971 for Risk Management. These standards provide a structured approach to managing quality and risk, thereby enhancing patient safety and facilitating international trade. This section provides an in-depth look into how different countries incorporate these standards into their regulatory practices.

Global Adoption of ISO 13485 and ISO 14971

1. European Union:

Regulatory Framework:

The European Union (EU) is known for its comprehensive regulatory framework governing medical devices, primarily through the Medical Device Regulation (MDR) (EU 2017/745) and the In Vitro Diagnostic Regulation (IVDR) (EU 2017/746). These regulations aim to ensure high standards of quality and safety for medical devices marketed in the EU.

Quality Management Systems:

ISO 13485 is harmonised under the MDR and IVDR, making it an essential standard for demonstrating compliance with EU regulatory requirements. The standard specifies requirements for a QMS that can be used by an organisation involved in the design, production, installation, and servicing of medical devices. It emphasises the importance of meeting customer and regulatory requirements while maintaining effective processes throughout the product lifecycle.

Risk Management:

ISO 14971 is integral to the risk management processes required by the MDR and IVDR. It provides a systematic approach for identifying hazards, estimating and evaluating risks, controlling those risks, and monitoring the effectiveness of the controls. Manufacturers must implement risk management throughout the lifecycle of their devices, from design to post-market surveillance. This proactive approach helps minimise potential harm to patients and users.

Impact on Manufacturers:

Compliance with these standards is not just a regulatory requirement but also a strategic advantage. It facilitates smoother market entry, enhances product credibility, and builds consumer trust. Manufacturers investing in robust QMS and risk management processes often find it easier to adapt to evolving regulations and technological advancements.

2. United States

Regulatory Framework:

The Food and Drug Administration (FDA) regulates medical devices in the United States through the Code of Federal Regulations (CFR) Title 21, Part 820, known as the Quality System Regulation (QSR). The FDA's regulatory approach is risk-based, focusing on ensuring that devices are safe and effective for their intended use.

Quality Management Systems:

While the QSR has its own set of requirements, it aligns closely with ISO 13485. Compliance with ISO 13485 can facilitate meeting QSR requirements, as both emphasise the importance of maintaining effective quality management processes. The FDA encourages manufacturers to adopt ISO 13485 as it provides a comprehensive framework for managing quality across all stages of production.

Risk Management:

The FDA recognises ISO 14971 as a suitable standard for risk management. Manufacturers are expected to implement robust risk management processes in line with ISO 14971 to ensure device safety and effectiveness. The FDA's guidance documents often refer to ISO 14971 principles, underscoring its importance in the regulatory landscape.

Impact on Manufacturers:

Adhering to these standards helps manufacturers navigate the complex FDA approval process more efficiently. It also enhances product safety and reliability, which are critical factors in gaining consumer confidence and achieving commercial success.

3. Canada

Regulatory Framework:

Health Canada regulates medical devices under the Food and Drugs Act through the Medical Devices Regulations. The Canadian regulatory framework emphasises transparency, safety, and efficacy.

Quality Management Systems:

ISO 13485 is mandatory for obtaining a Medical Device Licence in Canada. Manufacturers must demonstrate compliance with ISO 13485 to meet Canadian regulatory requirements. The standard ensures that manufacturers have a structured approach to managing quality, which is crucial for regulatory approval.

Risk Management:

Health Canada recognises ISO 14971 for risk management, requiring manufacturers to implement comprehensive risk management processes. This involves identifying potential risks, implementing control measures, and continuously monitoring and reviewing the effectiveness of these measures.

Impact on Manufacturers:

Compliance with ISO 13485 and ISO 14971 is essential for market access in Canada. It facilitates smoother regulatory approval and enhances the credibility of medical devices in the eyes of healthcare professionals and patients.

4. Japan

Regulatory Framework:

The Pharmaceuticals and Medical Devices Agency (PMDA) oversees the regulation of medical devices in Japan under the Pharmaceutical and Medical Device Act (PMD Act). The PMDA's regulatory framework is designed to ensure high standards of safety and efficacy.

Quality Management Systems:

Japan has harmonised its QMS requirements with ISO 13485, making it essential for regulatory compliance. The standard provides a structured approach for managing quality, ensuring that devices meet both customer and regulatory requirements.

Risk Management:

ISO 14971 is recognised for risk management, and manufacturers must incorporate risk management practices throughout the product lifecycle. This involves a systematic approach to identifying, evaluating, and controlling risks associated with medical devices.

Impact on Manufacturers:

Compliance with ISO 13485 and ISO 14971 is crucial for market access in Japan. It helps manufacturers navigate the regulatory landscape efficiently, ensuring that their products meet high safety and quality standards.

5. Australia

Regulatory Framework:

The Therapeutic Goods Administration (TGA) regulates medical devices in Australia under the Therapeutic Goods (Medical Devices) Regulations. The TGA's regulatory framework emphasises safety, performance, and quality.

Quality Management Systems:

Compliance with ISO 13485 is required for market authorisation of medical devices in Australia. The standard provides a comprehensive framework for managing quality, ensuring that devices meet regulatory requirements and are safe for use.

Risk Management:

The TGA recognises ISO 14971 for risk management, requiring manufacturers to demonstrate effective risk management practices. This involves identifying potential risks, implementing control measures, and continuously monitoring and reviewing the effectiveness of these measures.

Impact on Manufacturers:

Compliance with ISO 13485 and ISO 14971 is essential for market access in Australia. It enhances product safety and reliability, which are critical factors in gaining consumer confidence and achieving commercial success.

Conclusion

The adoption of ISO 13485 and ISO 14971 by regulatory bodies worldwide highlights the importance of standardised quality management and risk management practices in ensuring the safety and effectiveness of healthcare, wellness and medical devices. These standards provide a robust framework for manufacturers to meet regulatory requirements, manage risks, and ensure high-quality products. The harmonisation of these standards across various regions facilitates global trade and ensures that healthcare, wellness and medical devices meet consistent safety and performance criteria, ultimately benefiting public health and safety.

For manufacturers, investing in compliance with these standards is not just about meeting regulatory requirements but also about enhancing product quality, gaining consumer trust, and achieving commercial success in a competitive global market. As the healthcare, wellness and medical devices industry continues to evolve, embracing these standards will be crucial for navigating regulatory challenges and driving innovation in healthcare.

HEALTHCARE AND WELLNESS DEVICES TEST REQUIREMENTS IN RADIO FREQUENCY REQUIREMENT



Chapter 6 - Healthcare and Wellness Devices Test Requirements in Radio Frequency Requirement

The regulation bodies and authorities of many countries have established regulatory frameworks for placing healthcare and wellness devices with radio or wireless communication function on their market. All healthcare and wellness devices incorporating wireless communication technologies or emitting radio frequency (RF) energy must be compliant with their standards for efficient use of the radio spectrum to be offered on their markets so as to avoid harmful interference with radio and broadcast communications service. The following radio technologies are required to be tested to ensure compliance with the essential requirements. The next section will introduce the global market requirements for the following radio and wireless communication technologies.

- Wi-Fi
- Bluetooth
- Narrowband IoT (NB-IoT)
- LoRa
- Near-Field Communication (NFC)
- Radio Frequency Identification (RFID)
- Sigfox
- Ultra-wideband (UWB)
- 3G/4G/5G

Europe

The regulator is the European Commission. The CE mark must be affixed on radio and wireless products sold in the European market. The CE mark indicates a product's conformity with all applicable requirements when it is imported into and sold in the European market. It is mandatory that such a product must comply with the Radio Equipment Directive (RED). The RED specifies specific transmitter and receiver tests that conform with standards such as EN 300 328 and EN 300 220, e.g., transmit power,

spurious emissions, bandwidth), along with various EMC emissions and immunity tests per EN 301 489 and EN 301 908. Manufacturers or suppliers must complete and sign a Declaration of Conformity (DoC) that lists all the applicable directives and harmonised standards with which their products comply.

EN 50360:2017	Product standard to demonstrate the compliance of wireless communication devices, with the basic restrictions and exposure limit values related to human exposure to electromagnetic fields in the frequency range from 300 MHz to 6 GHz: devices used next to the ear
EN 50566:2017	Product standard to demonstrate the compliance of wireless communication devices with the basic restrictions and exposure limit values related to human exposure to electromagnetic fields in the frequency range from 30 MHz to 6 GHz: hand-held and body-mounted devices in close proximity to the human body
EN 302 208 V3.3.1	Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W and in the band 915 MHz to 921 MHz with power levels up to 4 W; Harmonised Standard for access to radio spectrum
EN 300 328 V2.2.2	Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz band; Harmonised Standard for access to radio spectrum
EN 302 571 V2.1.1	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
EN 300 440 V2.1.1	Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
EN 300 220-2 V3.1.1	Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU for non-specific radio equipment
EN 301 908-1 V13.1.1	IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 1: Introduction and common requirements
EN 301 511 V12.5.1	Global System for Mobile communications (GSM); Mobile Stations (MS) equipment; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU

EN 300 220-3-1 V2.1.1	Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 3-1: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU; Low duty cycle high reliability equipment, social alarms equipment operating on designated frequencies (869,200 MHz to 869,250 MHz)
EN 301 893 V1.8.1	Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
EN 301 893 V2.1.1	5 GHz RLAN; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
EN 302 065-1 V2.1.1	Short Range Devices (SRD) using Ultra Wide Band technology (UWB); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Requirements for Generic UWB applications

United States

The regulator is the Federal Communications Commission (FCC). The FCC label and statement must be affixed on radio and wireless products sold in the US market. Radio and wireless products sold in the US market must comply with relevant sections of the FCC's rules and regulations, such as FCC Part 15.247, based on the product type. The product must also be certified by either the FCC or a designated telecommunication certification body (TCB). The accredited test report and associated technical documentation must be submitted to an FCC designated TCB. Certification will be granted for products with associated FCC ID numbers. The FCC's rules and regulations can be found in Title 47 of the Code of Federal Regulations (CFR). The following list of standards are applicable to the above radio technologies.

47 CFR Part 15 - Radio Frequency Devices
47 CFR Part 18 - Industrial, Scientific, and Medical Equipment
47 CFR Part 22 - Public Mobile Services
47 CFR Part 24 - Personal Communications Services

Canada

The regulator is Innovation, Science and Economic Development (ISED). The ISED logo and an English/French statement must be affixed to radio and wireless products. Radio and wireless products sold in the Canadian market must comply with relevant sections of ISED rules and standards, such as RSS-247, based on the product type. Radio and wireless devices must be certified by ISED or a designated foreign certification body (FCB). The test report and technical documentation must be submitted to ISED or a designated FCB. Certification will be granted for the products with associated ISED ID numbers.

RSS-Gen, Issue 5, General Requirements for Compliance of Radio Apparatus
RSS-102 – Radio Frequency (RF) Exposure Compliance of Radiocommunications Apparatus (All Frequency Bands)
RSS-210 – Licence-Exempt Radio Apparatus: Category I Equipment
RSS-220 – Devices Using Ultra-Wideband (UWB) Technology
RSS-247 – Digital Transmission Systems (DTSs), Frequency Hopping Systems (FHSs), and Licence-Exempt Local Area Network (LE-LAN) Devices
RSS-310 – Licence-Exempt Radio Apparatus: Category II Equipment
RSS-132 – Cellular Telephone Systems Operating in the Bands 824-849 MHz and 869-894 MHz
RSS-134 – 900 MHz Narrowband Personal Communication Service
SPR-004 – Time-Averaged Specific Absorption Rate (TAS) Assessment Procedures for Wireless Devices Operating in the 4 MHz to 6 GHz Frequency Band

Australia

The regulator is the Australian Communications and Media Authority (ACMA). The Regulatory Compliance Mark (RCM) label is the approval scheme for wireless devices in Australia. Alternatively, for suppliers registered under the previous C-tick/A-tick regimes, the C-tick or A-tick label must be affixed to the products. Radio and wireless products sold in the Australian market must be compliant with relevant wireless and standards, such as AS/NZS, EN or FCC, and be labelled with the RCM mark (A-tick/C-tick marks were phased out in 2016). Other general RCM

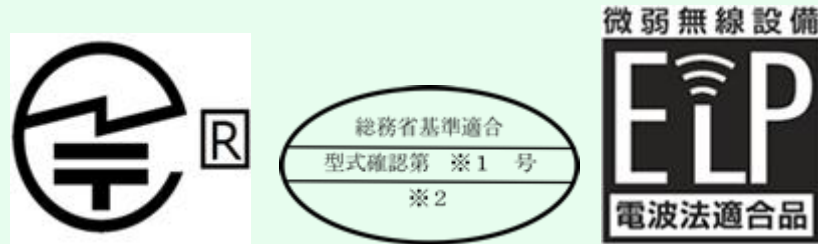
requirements, such as SAR/EMR, EMC, Safety and Telecoms standards, may also apply. Manufacturers and suppliers must complete and sign an RCM Declaration of Conformity (DoC) that lists all the applicable RCM standards with which their products comply.

AS/NZS 4268 specifies the minimum performance requirements and test methods of measurement for short-range devices and low-interference potential devices. If there is no standard applicable to the device specified in Table 1 of AS/NZS 4268, it allows compliance to be demonstrated by using the test method specified in one of the listed generic international standards published by ETSI or applicable FCC Rules.




AS/NZS 4268:2017	Radio equipment and systems - Short range devices - Limits and methods of measurement
------------------	---

Japan

The regulator is the Ministry of Internal Affairs and Communications (MIC). The MIC mark scheme is the approval for radio and wireless devices in Japan. The relevant MIC compliance logo must be affixed to radio and wireless products. Radio and wireless products sold in the Japanese market must comply with relevant MIC regulations in order to comply with the Japanese Radio Law (JRL). Certification through a registered certification body (RCB) is required depending on the product type. JRL’s scope covers all products which emit electromagnetic waves with frequencies under 3 THz. The JRL requires approvals not only for wireless communications devices, but also high-frequency devices such as welders and induction heating (IH) cooking equipment.



Most radio and wireless devices must obtain third-party certification by an MIC-designated RCB such as the Japan Quality Assurance Organization (JQA). Special Specified Radio Equipment (SSRE) must still be tested for compliance, but are subject to a simplified procedure of self-declaration and registration with MIC.

Specified Radio Equipment	Specified Radio Equipment:
	<ul style="list-style-type: none"> • Bluetooth • Wi-Fi • LTE • GSM • ZigBee • Wireless mics • RFID (2.4 GHz, 920 MHz) • Telemeters • UWB radio systems
High-Frequency Devices	High-Frequency Devices:
	<ul style="list-style-type: none"> • High-frequency devices • IH cooking devices • Microwaves • Electrode-less discharge lamps • Welders • RFID (13.56 MHz) • Ultrasonic devices • Other equipment over 10 kHz (including industrial and medical devices)
Extremely Low-Power Devices (ELPs)	Field strength @ 3 m:
	<ul style="list-style-type: none"> • <500 uV/m for products operating under 322 MHz or over 150 GHz • <35 uV/m for 322 MHz – 10 GHz • <3.5x uV/m, where x is the frequency in GHz (or 500 uV/m, which is lower) for 10 GHz – 150 GHz

China

State Radio Regulation of China (SRRC) is a mandatory certification required by the Bureau of Radio Regulation of the Ministry of Industry and Information Technology (the State Radio Office). All radio and wireless products sold and used in China must first obtain the Radio Type Approval Certification (Radio Type Approval Certification). The State Radio Monitoring Center (SRMC) is responsible for radio equipment type approval testing, radio equipment technical specification and standard development and normative study of radio testing laboratory capacity building, and for carrying out technical guidance on national radio equipment testing.

The main content of the radio equipment testing is in accordance with the requirements of manufacturers, user units, operating units, government departments, and other customers, and in accordance with relevant national standards, industry standards, group standards, international standards, and various radio management technical specifications. The radio frequency parameters of transmitting equipment that must be tested, verified, and evaluated mainly include operating frequency, transmitting power, frequency tolerance, occupied bandwidth, spectrum mask, out-of-band emission, spurious emission and other transmitter radio frequency parameters, receiving sensitivity, adjacent channel receiver radio frequency parameters such as selectivity and blocking, as well as other radio frequency parameters related to radio transmission equipment.

The following are products that require China SRRC certification:

- Public mobile communication equipment
- Wireless access systems
- Dedicated network equipment
- Microwave equipment
- Radio and TV equipment
- Satellite equipment
- 2.4 GHz / 5.8 GHz wireless LAN equipment
- Short-range wireless equipment
- Radars
- Other radio equipment
- A product that does not fall within any of the ten categories above may still require certification if it has properties that are similar to the above products.

5G Standards:

The requirements for regulatory tests for devices with 5G technology and the standards for 5G have not yet been finally harmonised. The 3rd Generation Partnership Project (3GPP) is a member-driven standards organisation that develops protocols for mobile telecommunications including 5G NR and related 5G standards. The following standards are developed by 3GPP and ETSI. These standards are currently adopted by most 5G devices in order to satisfy their compliance requirement.

5GS; User Equipment (UE) conformance specification; Part 1: Common test environment

3GPP TS 38.508-1

ETSI TS 138 508-1

5GS; User Equipment (UE) conformance specification; Part 2: Common Implementation Conformance Statement (ICS) proforma

3GPP TS 38.508-2

ETSI TS 138 508-2

5GS; Special conformance testing functions for User Equipment (UE)

3GPP TS 38.509

ETSI TS 138 509

NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 1: Range 1 Standalone

3GPP TS 38.521-1

ETSI TS 138 521-1

NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 2: Range 2 Standalone

3GPP TS 38.521-2

ETSI TS 138 521-2

NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 3: Range 1 and Range 2 Interworking operation with other radios

3GPP TS 38.521-3

ETSI TS 138 521-3

NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 4: Performance requirements

3GPP TS 38.521-4

ETSI TS 138 521-4

NR; User Equipment (UE) conformance specification; Applicability of radio transmission, radio reception and radio resource management test cases

3GPP TS 38.522

ETSI TS 138 522

5GS; User Equipment (UE) conformance specification; Part 1: Protocol

3GPP TS 38.523-1

ETSI TS 138 523-1

5GS; User Equipment (UE) conformance specification; Part 2: Applicability of protocol test cases

3GPP TS 38.523-2

ETSI TS 138 523-2

5GS; User Equipment (UE) conformance specification; Part 3: Protocol Test Suites

3GPP TS 38.523-3

ETSI TS 138 523-3

NR; User Equipment (UE) conformance specification; Radio Resource Management (RRM)

3GPP TS 38.533

ETSI TS 138 533

PRACTICAL INTERPRETATIONS AND CASES SHARING FOR HEALTHCARE AND WELLNESS DEVICES



Chapter 7 – Practical Interpretations and Cases Sharing for Healthcare and Wellness Devices

In this chapter, the practical interpretations for healthcare and wellness devices about test objectives, test set-ups, test parameters, test methods, performance criteria, and test results will be introduced.

Four typical areas of healthcare and wellness devices (i.e., wellness, child, elderly, and disabilities) are selected to provide 10 individual cases sharing for healthcare and wellness devices from product markets (i.e., 1. healthcare remote monitoring devices; 2. air-filtering and water-purifying devices; 3. connected inhalers; 4. temperature and ingestible sensors; 5. fitness trackers; 6. wearable healthcare devices; 7. physiological tracking devices; 8. pain & emotional management devices; 9. emergency-care devices; and 10. health recovery devices) for practical interpretations. Before suggesting recommendations, advice and precautions to enhance the design solutions for healthcare and wellness devices on the basis of testing requirements in this chapter, a brief introduction on the Electromagnetic Compatibility (EMC) Test and the Radio Frequency Test is first given to help us better understand the recommendations, advice and precautions.

Part A - Electromagnetic Compatibility (EMC) Test

In general, the EMC test covers two types of tests: emission tests and immunity tests.

- Emission tests – To measure the amount of disturbance in the form of electromagnetic radiation and conduction, voltage fluctuation, and harmonic current generated by a device during normal operation. The purpose of emission tests is to ensure that any disturbance from the electronic device is below the relevant limits defined for that particular type of devices. These tests provide a reasonable assurance that the device will not cause harmful interference to other devices operating within its expected operating environment.
- Immunity tests – To measure how an electronic device reacts to and withstands exposure to electromagnetic and other disturbances. The purpose of these tests is to provide reasonable assurance that the device will operate as intended when used within its expected operating environment.

Emission Tests

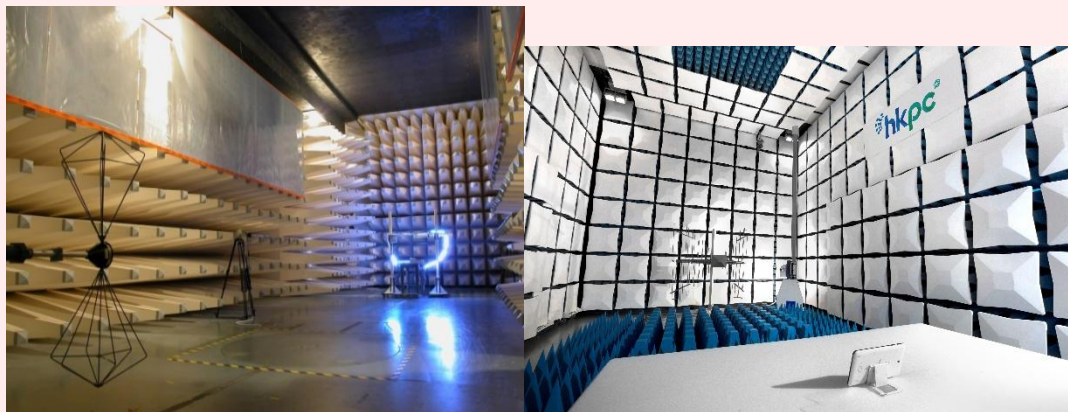
Radiated Emissions (CISPR 16-2-3)

Objective:

Radiated emissions are the intentional and unintentional release of electromagnetic energy from an electronic device. The radiated test is performed to ensure emissions emanating from the DUT or EUT comply with the applicable limits in the standards.

Test environment:

Open area test site (OATS) or its alternative sites (e.g., a so-called semi-anechoic chamber, which is an absorber-lined shielded enclosure (ALSE)), fully-anechoic chamber (FAC) or its alternative sites (i.e., OATS and SAC)



Measuring equipment:

- EMI receivers or spectrum analysers with the peak, quasi-peak, and average detectors pursuant to CISPR 16-1-1



Antennas:

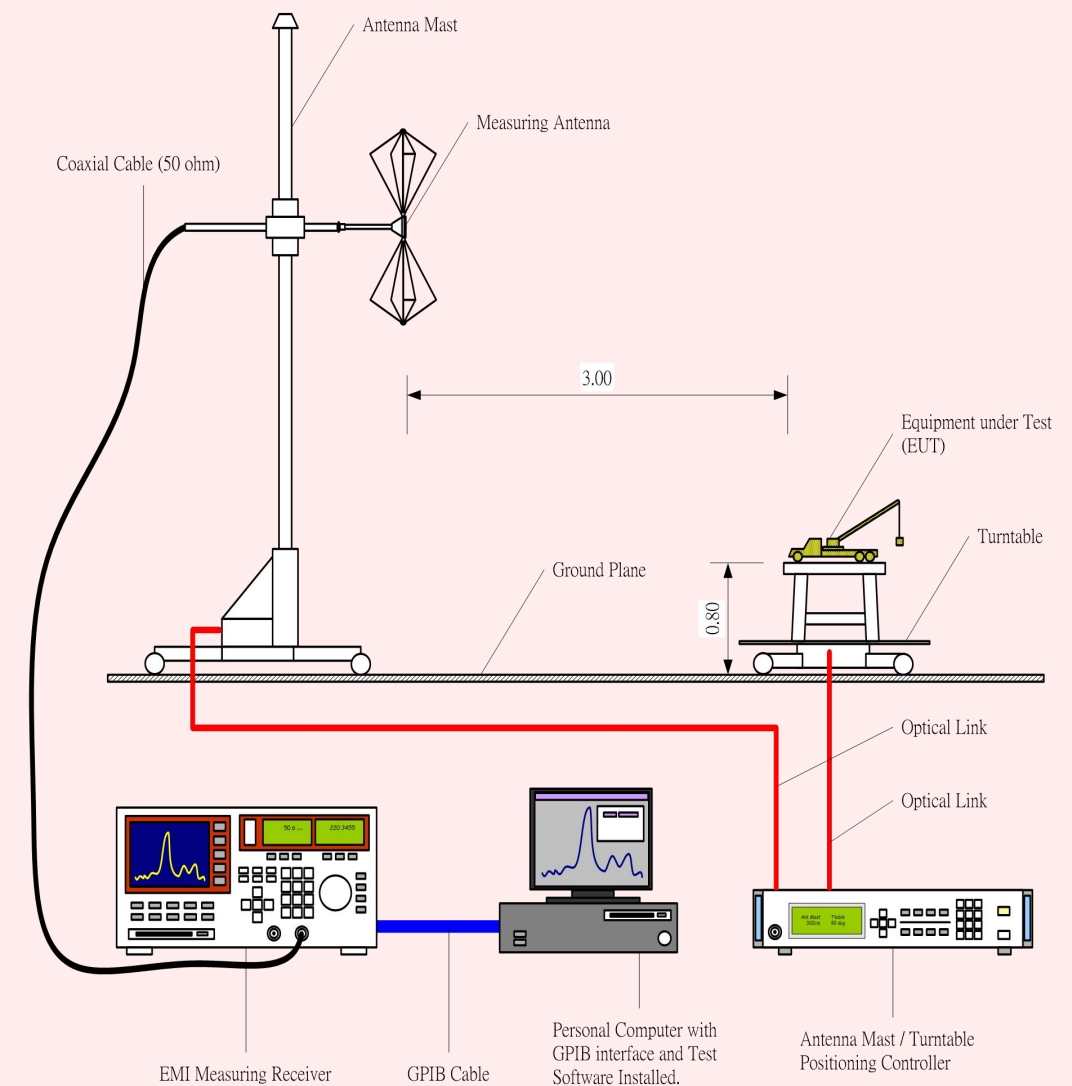
- Tuned dipoles or broadband shortened dipole antenna (e.g., biconical antenna) or dipole array (e.g., log-periodic antenna)



Measurand:

- Maximum E-field component of electromagnetic disturbance signals measured with the measuring antenna at a predefined measurement separation (e.g., 10 m or 3 m)

Test setup:



Conducted Emissions (CISPR 16-2-1)

Objective:

Conducted emissions are the coupling of electromagnetic energy from a device to its power cord. Similar to radiated emissions, the allowable conducted emissions from electronic devices are controlled by different regulatory agencies and tests are performed to ensure the emission levels are below the applicable limits.

Test environment:

- Reference ground plane or a sufficiently large area
- Artificial mains networks (AMN) and / or impedance stabilisation network (ISN) or coupling / decoupling network (CDN) per IEC 61000-4-6



Measuring equipment:

- EMI receivers or spectrum analysers with the peak, quasi-peak, and average detectors per CISPR 16-1-1

Transducers:

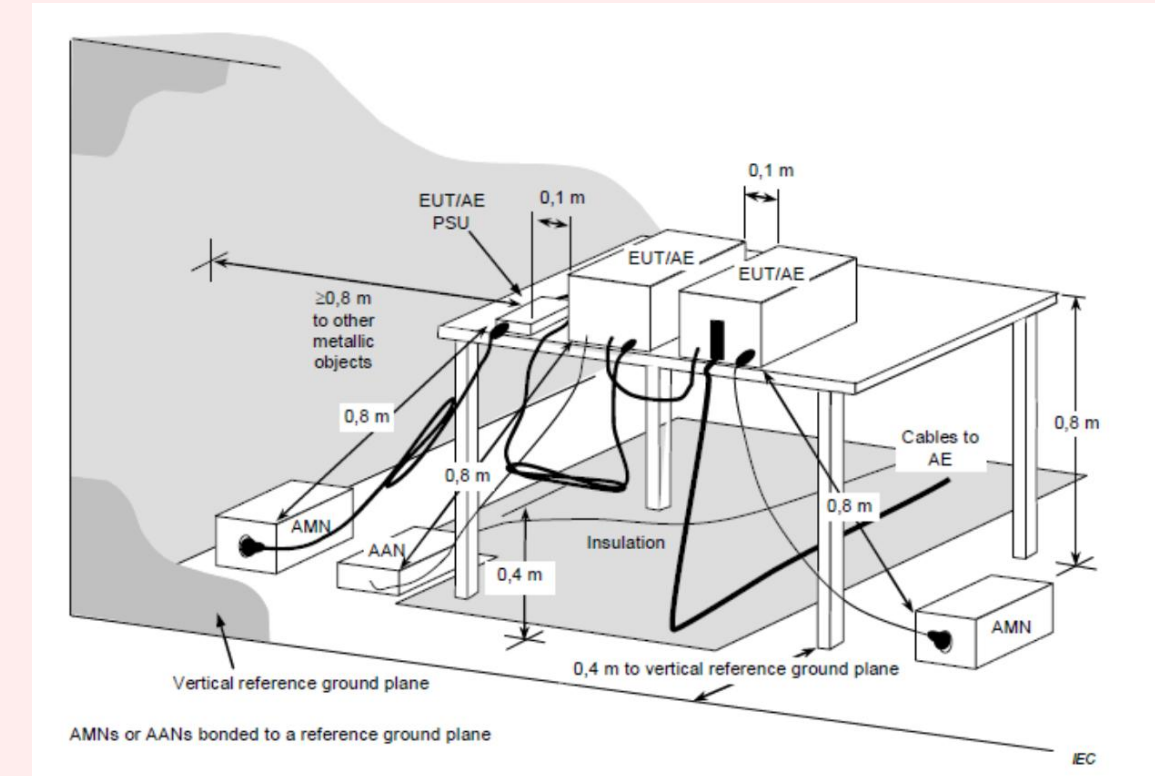
- (Part of) common-mode impedance of AMN or ISN or CDN applied between the port and the reference ground plane, or
- RF voltage probes per CISPR-16-2
- Radio frequency (RF) current probe



Measurands:

- Voltage drop across (part of) the impedance of AMN, ISN or CDN, or
- Current (common-mode) flowing through the AMN, ISN or CDN between the port under test and the reference ground plane

Test setup:



Harmonic Current Emissions & Voltage Changes, Voltage Fluctuations, and Flicker (IEC 61000-3-2 & IEC 61000-3-3)

Objective:

Due to the extensive use of switching mode power supplies in electronic products, while improving power efficiency, a large amount of harmonic current is injected into the power system due to non-linear power conversion, which interferes with other devices in the same power grid and causes neutral current overload that affects transmission capacity. In addition, the phase control of power supply causes changes in the current of the power grid and in turn causes the voltage on the load side to fluctuate, as a result causing lights to flicker.

Therefore, it is necessary to measure the harmonic distortion current as well as voltage fluctuations and flicker generated by the electronic device to assess the product's compliance with the EMC standards.

Measuring equipment:

- Harmonics analysing system and test software

Measurands:

- Voltage and current changes through the analysing system



Immunity Tests

Immunity tests to **continuous** electromagnetic fields:

- Conducted RF immunity (IEC 61000-4-6)
- Radiated RF immunity (IEC 61000-4-3)
- Power frequency magnetic field (IEC 61000-4-8)

Immunity tests to **transient** electromagnetic phenomena:

- Electrostatic discharge (ESD) (IEC 61000-4-2)
- Electric fast transient (EFT) or burst (IEC 61000-4-4)
- Surge (IEC 61000-4-5)
- Voltage dip and short interruptions (IEC 61000-4-11)

Conducted RF Immunity (IEC 61000-4-6):

Objective:

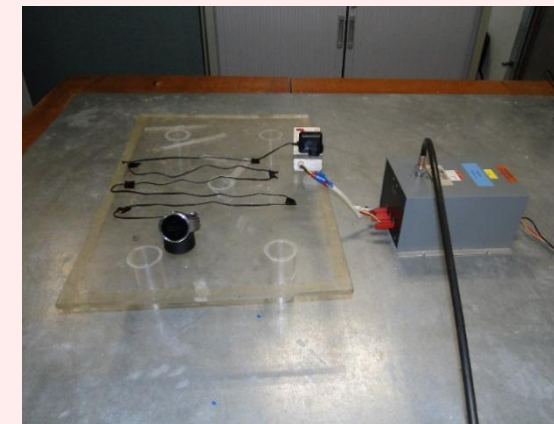
To test electronic products' immunity to Radio Frequency (RF) conducted injected interference. RF conducted interference is a phenomenon as simple as placing a wireless device on or near power cables or data lines that can couple wireless through the shielding of those lines and affect associated equipment.

Ports under test:

- Public network or ports vulnerable to picking up RF signals

Test equipment:

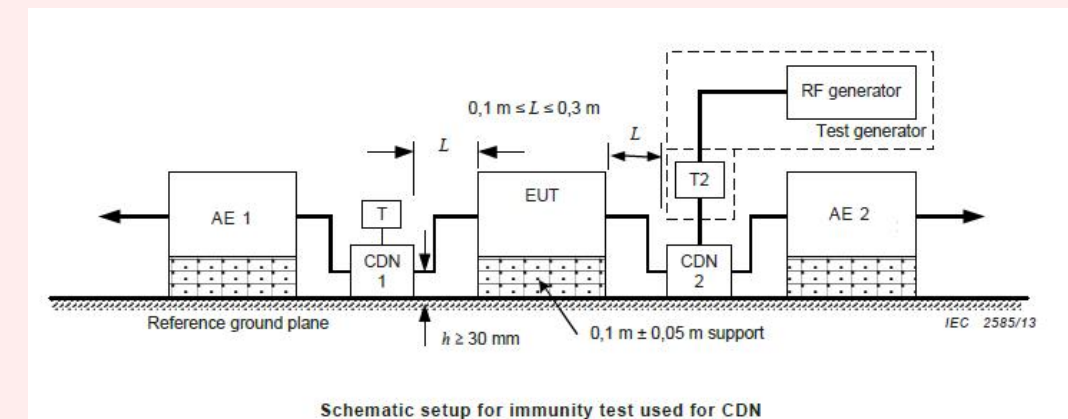
RF immunity test systems



Test method:

- Reference ground plane
- Coupled by CDN or Bulk Current Injection (BCI) current transformer
- Substitution
 - Calibrated against forward power to antenna
 - Specified in unmodulated signal levels
- Performance criteria A or equivalent alternative is required

Test setup:



Radiated RF Immunity (IEC 61000-4-3)

Objective:

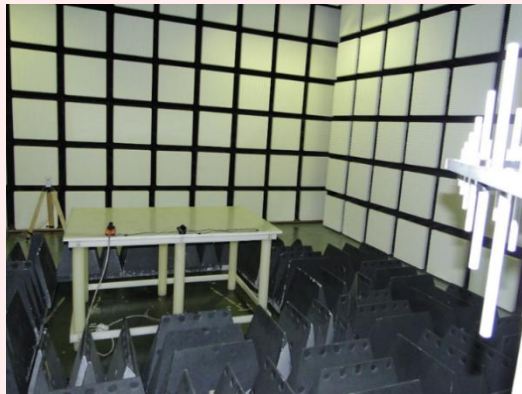
To evaluate the immunity of electrical and electronic equipment exposed to radiated RF electromagnetic fields.

Port under test:

- Enclosure port

Test environment:

- Absorber-lined shielded enclosure (ALSE), fully-anechoic chamber (FAC) or its alternative sites



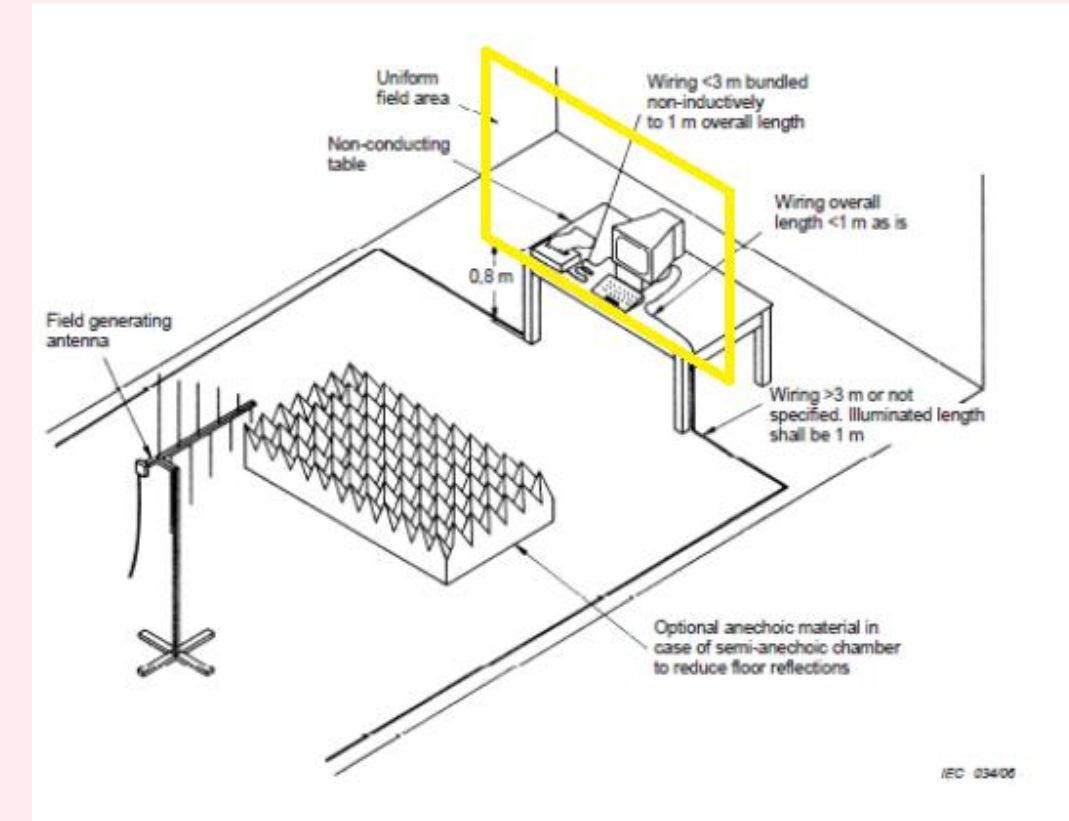
Test equipment:

RF immunity test systems (signal generator, amplifier, antenna, field sensor, power metre)

Test method:

- Coupled with linearly polarised antennas (vertical and horizontal polarisation)
- Substitution
 - Calibrated uniform field area (UFA) of 1.5 x 1.5m (or 0.5 x 0.5 m windowed)
 - Calibrated against forward power to antenna
 - Specified in unmodulated signal levels
- Performance criteria A or equivalent alternative is required

Test setup:



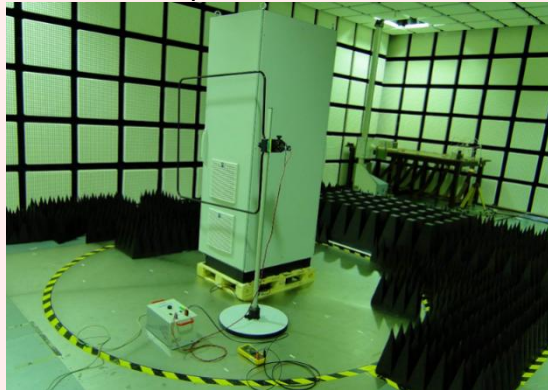
Power Frequency Magnetic Field (IEC 61000-4-8)

Objective:

To evaluate the performance of electrical and electronic equipment for household, commercial, and industrial applications when subjected to magnetic fields at power frequency (continuous and short duration field)

Port under test:

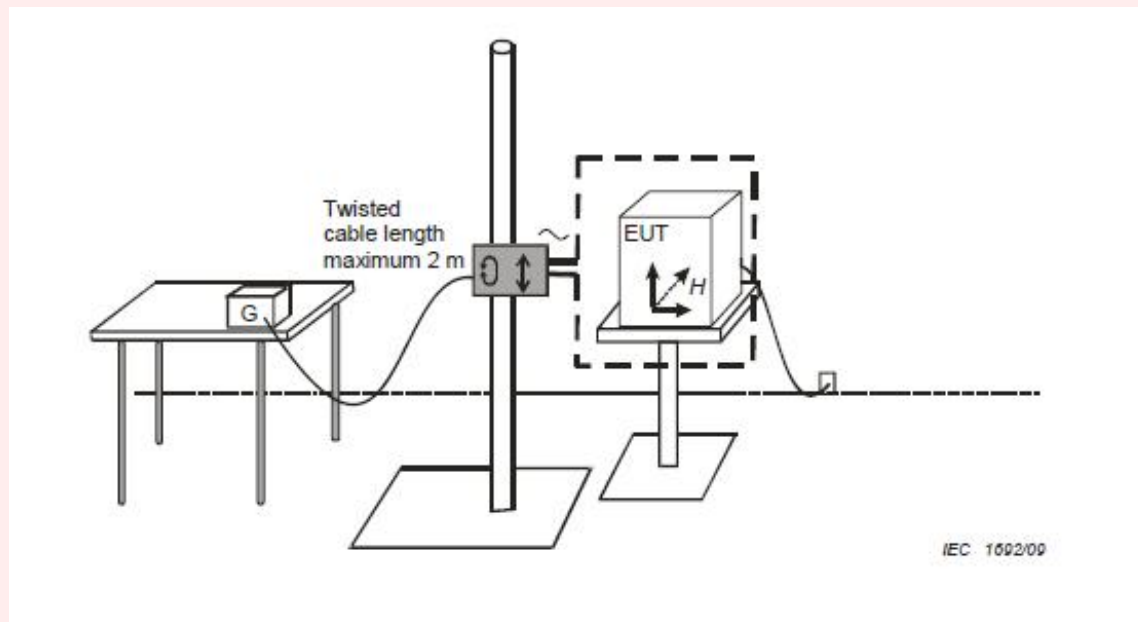
- Enclosure port



Test level:

- 3 A/m or 30 A/m: Continuous field
- 300 A/m or 1000 A/m: Short duration (1 s to 3 s)
- Performance criteria A or equivalent alternative is required

Test setup:



Electrostatic Discharge (ESD) (IEC 61000-4-2)

Objective:

To evaluate the performance of electrical and electronic equipment when subjected to electrostatic discharges, including electrostatic discharges which may occur from personnel to objects near vital equipment.

Port under test:

- Enclosure port



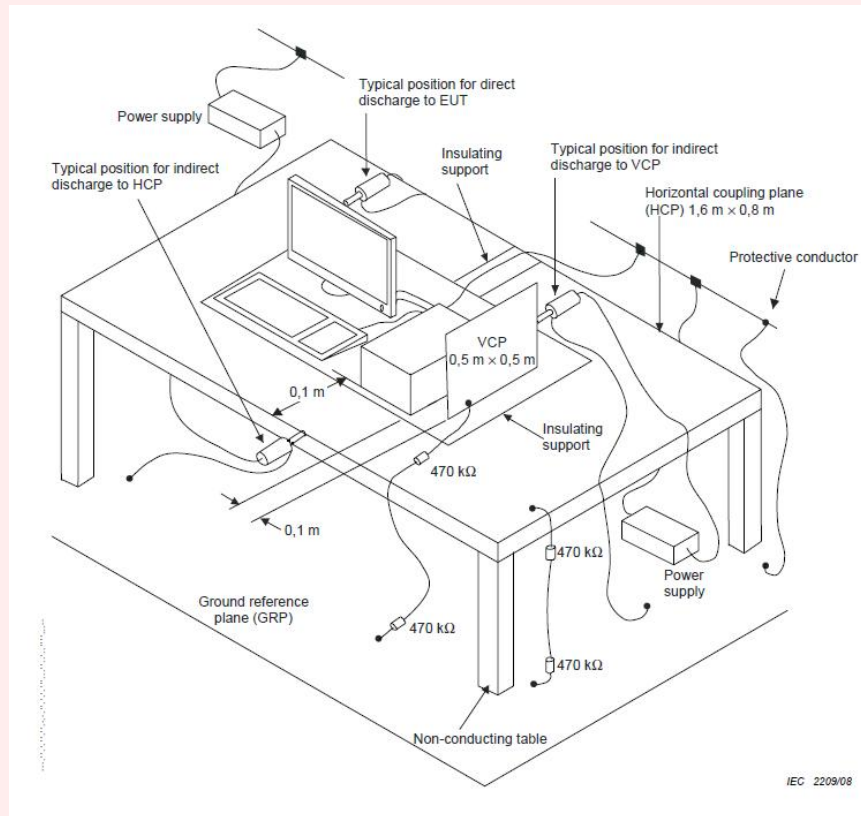
Phenomena:

- ESD generated
 - by an operator or an object touching the EUT (direct discharge)
 - by objects or persons in the vicinity of the EUT (indirect discharge)
- Test level:
 - 2 kV, 4 kV, 6 kV, 8 kV for contact discharge
 - 2 kV, 4 kV, 8 kV, 15 kV for air discharge

Test methods:

- Contact discharge:
 - conductive accessible parts
- Air discharge:
 - non-conductive accessible parts, and
 - conductive non-accessible portion of accessible parts
- No. of each test applied – at least 10 times
- Performance criteria B or equivalent

Test setup:



Electric Fast Transient (EFT) or Burst (IEC 61000-4-4)

Objective:

To evaluate the immunity of electrical and electronic equipment when subjected to electrical fast transient/bursts on supply, signal, control, and earth ports. Electrical fast transient is generated by switching of small inductive loads, relay contacts bouncing (conducted interference), and switching of HV-switchgear (radiated interferences).

Ports under test:

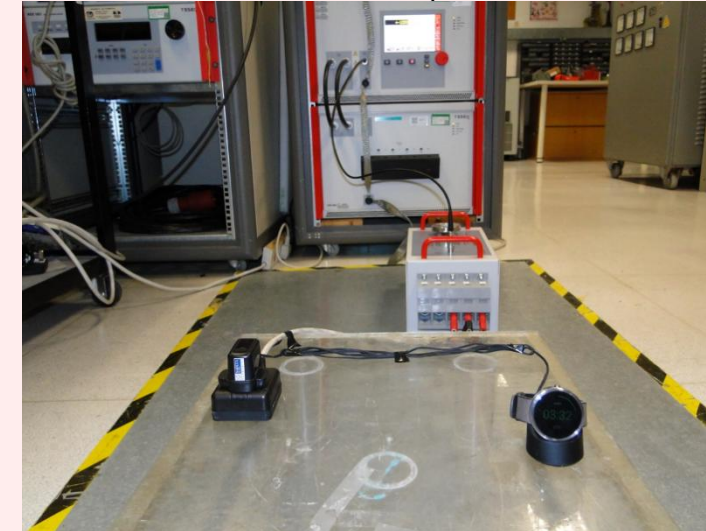
- Power supply, signal, control and earth ports

Test signals:

- Group of double exponential pulses of
- Rise time = 5 ns
- Pulse width = 50 ns
- Repetition = 5 or 2.5 kHz
- Burst period = 300 ms
- Source impedance: 50 ohms

Test method:

- Coupling via CDN or capacitive coupling clamp:
- Test duration – at least 1 minute
- Performance criteria B or equivalent



Surge (IEC 61000-4-5)

Objective:

To evaluate the immunity of electrical and electronic equipment when subjected to surges. General speaking, lightning can produce surges with the energy of several joules by switching (of the capacitor bank) in the power network, faults in the power network, and lightning strokes (direct or indirect)

Ports under test:

- AC mains and public telecom networks

Test signals:

- Unidirectional single pulse
- Dual exponential waveforms
 - Voltage pulse (open circuit) 1.2/50 μs
 - Current pulse (short circuit) 8/20 μs
- Source impedance = 2Ω or 12Ω

Test method:

- Coupling / decoupling network
- Performance criteria B or equivalent



Voltage Dip and Short Interruptions (IEC 61000-4-11):

Objective:

To evaluate the immunity of electrical and electronic equipment when subjected to voltage dip and interruptions. Dips and interrupts are caused by faults in the power network, the installation or sudden large change of load, while voltage variations are caused by continuous varying loads connected to the power network.

Ports under test:

- AC mains

Specific requirements of test equipment:

- High inrush current capacity of test generators
- Performance criteria B or C or equivalent

Part B – Radio Frequency Test

In general, the Radio Frequency Test covers two types of tests: transmitter tests and receiver tests.

- Transmitter tests – To measure the parameters of transmitters. In most standards, RF output power and unwanted emissions in the spurious domain are popular test items for transmitters. Other test items, such as the permitted range of operating frequencies, occupied channel bandwidth, power spectral density, and so on, are not available for all types of wireless technologies and operating frequency ranges. The purpose of transmitter tests is to ensure that output RF power, spurious emissions, and other essential parameters are under control as required by laws and regulations and to fulfil the requirements of the stated measurements. No disturbance from the wireless device is below the relevant limits defined for that type of device. These tests provide a reasonable assurance that the device will not cause harmful interference to other devices operating within its expected operating environment.
- Receiver tests – To measure the parameters of receivers. The test of spurious emissions of receivers is a popular test item for receivers. Besides, how a receiver reacts and withstands exposure to transmitter interferences and low receive sensitivity are also essential test items for receivers. The purpose of these tests is to provide reasonable assurance that the wireless device will operate normally and receive the RF signal as intended when used within its expected operating environment.

Standards:

At present, two institutes are responsible for developing methods for RF measurement in the world. One of them is the European Telecommunications Standards Institute (ETSI) and the other is the American National Standards Institute (ANSI).

General speaking, ETSI is a European Standards Organization (ESO). It is the recognised regional standards body dealing with telecommunications, broadcasting, and other electronic communications networks and services. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognised as European Standards (ENs). Therefore, ETSI standards are used for wireless and RF measurement in Europe.

ANSI is a private, non-profit organisation that administers and coordinates the U.S. voluntary standards and conformity assessment system. The institute works in close collaboration with stakeholders from industry and government to identify and develop standards- and conformance-based solutions to national and global priorities. Therefore, ANSI standards are used for EMC, wireless, and RF measurement in the US.

In Chapter 3, we introduced a number of standards for RF and wireless measurements. The measurement procedures of most of them follow the standards developed by ETSI and ANSI. For example, the measurement procedures of the standards for Europe use ETSI and those for the US and Canada use ANSI. The main difference between ETSI and ANSI is that ETSI have more test requirements and test items for transmitters and receivers, while ANSI is more focussed on transmitters with only few test requirements and test items for receivers. Besides, the measurement units are different in ETSI and ANSI in some test items.

Transmitter Tests:

RF Output Power (ETSI & ANSI)

Objective:

RF output power is defined as the mean equivalent isotropically radiated power (EIRP) of the equipment during a transmission burst.

Port under test:

- Antenna port or enclosure port

Test equipment:

- EMI receiver, power metre, or spectrum analyser

Test method:

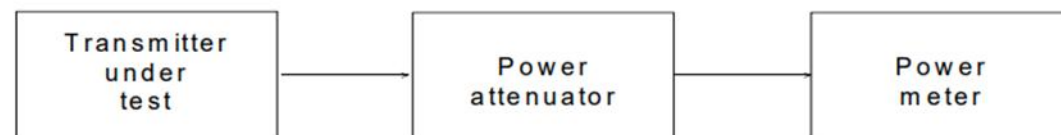
- Conducted measurement for equipment with an antenna port
- Radiated measurement for integral antenna equipment (without antenna connectors)

Measurement units:

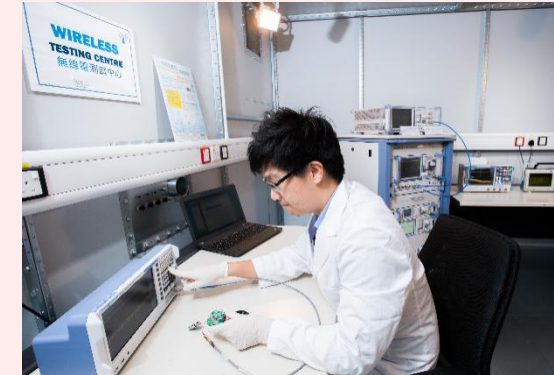
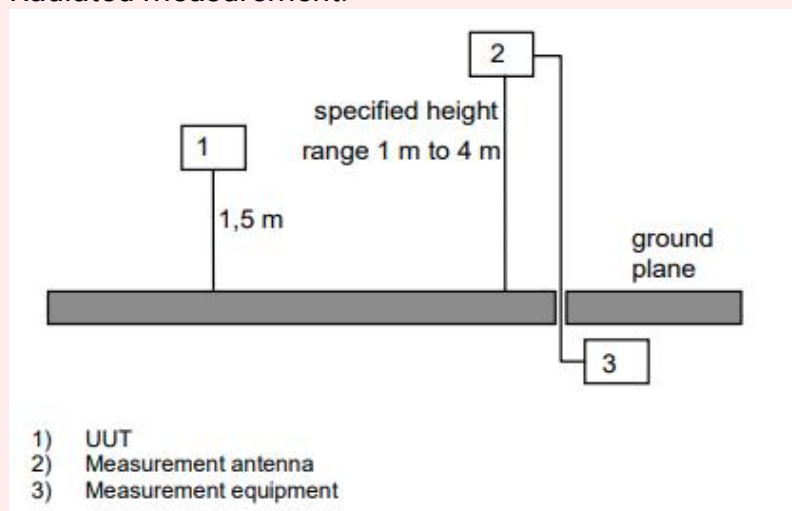
- Conducted measurement: dBm in ETSI and ANSI
- Radiated measurement: dB μ V/m in ANSI and dBm in ETSI

Test setup:

- Conducted measurement:



- Radiated measurement:



Transmitter Unwanted Emissions in the Spurious Domain (ETSI & ANSI)

Objective:

To measure transmitter unwanted emissions in the spurious domain, i.e., emissions outside the allocated band and outside the out-of-band domain

Port under test:

- Antenna port or enclosure port

Test equipment:

- EMI receiver or spectrum analyser, antennas, pre-amplifier, filter

Test method:

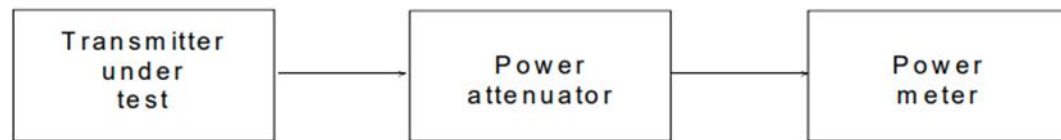
- Conducted measurement for equipment with an antenna port
- Radiated measurement for integral antenna equipment (without antenna connectors)

Measurement units:

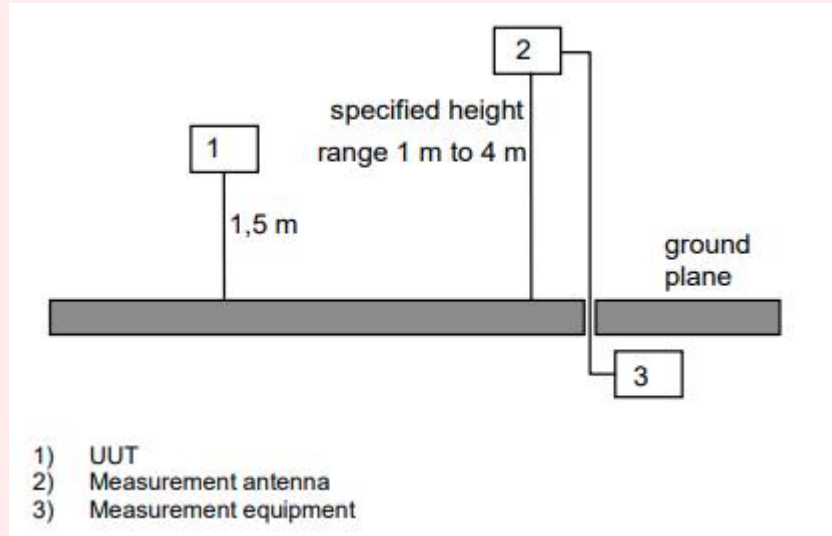
- Conducted measurement: dBm in ANSI and ETSI
- Radiated measurement: dB μ V/m in ANSI and dBm in ETSI

Test setup:

- Conducted measurement:



- Radiated measurement:



Receiver Tests

Receiver Spurious Emissions (ETSI)

Objective:

To measure receiver spurious emissions, i.e., emissions at any frequency when the equipment is in receive mode.

Ports under test:

- Antenna port or enclosure port

Test equipment:

- EMI receiver or spectrum analyser, antennas, pre-amplifier, filter

Test method:

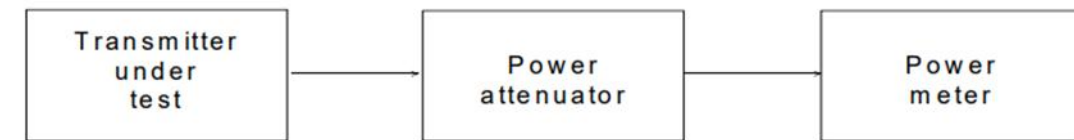
- Conducted measurement for equipment with an antenna port
- Radiated measurement for integral antenna equipment (without antenna connectors)

Measurement units:

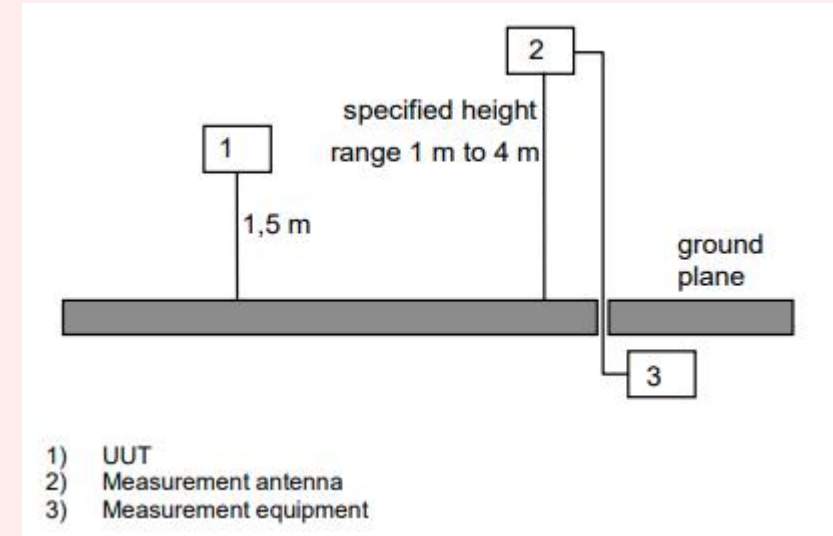
- Conducted measurement: dBm in ETSI
- Radiated measurement: dBm in ETSI

Test setup:

- Conducted measurement:



- Radiated measurement:



Part C - Case Sharing

Cases about 10 individual healthcare and wellness devices: remote monitors, air/water purifiers, connected inhalers, ingestible sensors, fitness trackers, wearable BP monitors, paediatric sensors, TENS units, emergency pendants, and EMS devices, will be shared in this section. The specific requirements for the following 10 individual healthcare and wellness devices are not comprehensively detailed herein. For a thorough understanding of the compliance requirements, consultation with a professional consultancy or a notified body is recommended.

1. Healthcare Remote Monitoring Devices (Elderly – Fall Detection Wearables)

EMC Testing (IEC 60601-1-2)

- Radiated Emissions (CISPR 11): Ensure device emissions ≤ 30 dB μ V/m (30 MHz–1 GHz)
- Immunity (IEC 61000-4-3): Test resistance to 3 V/m RF interference (80 MHz–2.5 GHz)
- ESD (IEC 61000-4-2): ± 8 kV contact discharge (no false alarms)

Cybersecurity (ISO/IEC 27001, UL 2900-2-1)

- Penetration Testing: Simulate attacks on Bluetooth/Wi-Fi (e.g., spoofing emergency alerts)
- Data Encryption: Verify AES-256 encryption for patient data in transit/rest
- Firmware Integrity: Secure boot and OTA updates with digital signatures

Electrical Safety (IEC 60601-1, UL 60601-1)

- Leakage Current: < 10 μ A (patient-contacting parts)
- Battery Safety: Overcharge/over-discharge protection (UN 38.3)

QMS & Risk Management (ISO 13485, ISO 14971)

- Risk File: Document fall detection failure modes (e.g., false negatives)
- Post-Market Surveillance: Track real-world false alarm rates

RF Requirements (FCC Part 15, RED Directive)

- Bluetooth BLE: Verify ≤ 10 m range stability (2.4 GHz band)
- SAR Compliance: < 1.6 W/kg (wearable RF exposure)

2. Air-filtering / Water-purifying Devices (Child – Smart Air Purifiers)

EMC Testing (CISPR 11, IEC 61000-6-3)

- Conducted Emissions: < 46 dB μ V (150 kHz–30 MHz)
- Voltage Dips (IEC 61000-4-11): Test operation during $\pm 20\%$ voltage fluctuations

Cybersecurity (IEC 62443-4-2)

- Cloud API Security: Prevent unauthorised access to air quality data
- Default Password Enforcement: Block factory-default logins

Electrical Safety (IEC 60335-1)

- Insulation Resistance: > 1 M Ω (live parts to chassis)
- Overheating Protection: Thermal cutoffs at 90°C

QMS & Risk Management (ISO 9001, ISO 14971)

- Hazard Analysis: Ozone emission risk (must be < 0.05 ppm)
- Component Traceability: Document filter supply chain

RF Requirements (FCC Part 15 & 18, ETSI EN 300 220, ETSI EN 300 328)

- Wi-Fi Interference: No disruption to medical devices (e.g., pacemakers)

3. Connected Inhalers (Disabilities – Asthma/COPD Smart Inhalers)

EMC Testing (IEC 60601-1-2)

- Radiated Immunity: Functionality maintained under 10 V/m RF fields
- ESD (IEC 61000-4-2): ± 15 kV air discharge (no data corruption)

Cybersecurity (FDA Premarket Guidance, UL 2900-2-1)

- Bluetooth Pairing Security: Prevent man-in-the-middle attacks
- HIPAA Compliance: Encrypt PII (Personal Health Information)

Electrical Safety (IEC 60601-1)

- Battery Safety: Prevent leakage in lithium cells (IEC 62133)

QMS & Risk Management (ISO 13485, ISO 14971)

- Use Error Risks: Misuse scenarios (e.g., incorrect dosing logs)

RF Requirements (FCC Part 15C, Bluetooth SIG)

- BLE Packet Loss: $< 1\%$ in crowded RF environments

4. Temperature & Ingestible Sensors (Wellness – Smart Pills)

EMC Testing (IEC 60601-1-2)

- RF Immunity: No data loss under 10 V/m interference

Cybersecurity (ISO/IEC 27001)

- End-to-End Encryption: Secure data from pill to cloud

Electrical Safety (IEC 60601-1, ISO 10993)

- Biocompatibility: Pass USP Class VI (no toxicity)

RF Requirements (FCC Part 15, ETSI EN 303 978)

- Ingestible RF Safety: SAR <1.6 W/kg (safe for internal use)

5. Fitness Trackers (Wellness – Heart Rate Monitors)

EMC Testing (EN 301 489-1)

- Bluetooth Coexistence: No EMC interference within Wi-Fi or Bluetooth

Cybersecurity (NIST SP 800-53)

- Data Anonymisation: GDPR compliance for EU users

Electrical Safety (IEC 62368-1)

- Battery Explosion Risk: UL 2054 compliance

RF Requirements (FCC ID, CE RED)

- Transmit Power: <10 dBm (BLE)

6. Wearable Healthcare Devices (Elderly – Blood Pressure Smartwatches)

EMC Testing (IEC 60601-1-2, ANSI/AAMI EC11:2021)

- Radiated Emissions (CISPR 11): Limit: ≤ 30 dB μ V/m (30 MHz–6 GHz) to avoid interference with medical equipment
- Immunity (IEC 61000-4-3): Test: 10 V/m RF fields (80 MHz–2.7 GHz) – device must maintain BP measurement accuracy (± 5 mmHg)
- ESD (IEC 61000-4-2): ± 8 kV contact discharge on touchscreen – no false readings or shutdowns

Cybersecurity (UL 2900-2-1, HIPAA)

- Attack Vectors Tested:
 - Bluetooth spoofing (e.g., falsifying BP data)
 - Cloud API penetration (OWASP Top 10 vulnerabilities)
- Data Protection: End-to-end encryption (AES-256) for BP data synchronised to EHR systems

Electrical Safety (IEC 60601-1, UL 60601-1)

- Leakage Current: Patient-applied parts: <10 μ A (Type BF applied part)
- Battery Safety: Overcharge protection (IEC 62133) – no thermal runaway at 120% rated voltage

QMS & Risk Management (ISO 13485, ISO 14971)

- Risk File Requirements:
 - Hazards: Incorrect BP readings leading to misdiagnosis (Severity: 4/Critical)
 - Mitigation: Redundant sensors + clinical validation per AAMI/ISO 81060-2
- Post-Market Surveillance: Monitor FDA MAUDE database for adverse events

RF Requirements (FCC Part 15B, ETSI EN 301 893)

- Bluetooth/Wi-Fi Coexistence: No interference when used near 2.4 GHz medical telemetry systems
- SAR Compliance: ≤ 1.6 W/kg (1 g tissue average) for wrist-worn devices

7. Physiological Tracking Devices (Child – Paediatric Pulse Oximetry Socks)

EMC Testing (IEC 60601-1-2, ASTM F2902)

- Radiated Immunity: Functionality maintained under 3 V/m RF fields (ISM bands: 902 MHz, 2.4 GHz)
- Conducted Emissions: <46 dB μ V (150 kHz–30 MHz) to prevent interference with neonatal ICU equipment

Cybersecurity (FDA Postmarket Guidance, IEC 62443-4-1)

- Secure Pairing: BLE pairing with MITM protection (NIST SP 800-121r2)
- Firmware Integrity: Signed updates with HSM-protected keys (FIPS 140-2 Level 2)

Electrical Safety (IEC 60601-1-11 for Home Use)

- Insulation: Double insulation (2 MOPP) for applied parts (IEC 60601-1)
- Battery Access: Child-resistant battery compartment (IEC 62115)

QMS & Risk Management (ISO 14971, 21 CFR Part 820)

- Risk Control: False SpO₂ alarms (Probability: 3/Occasional) → Algorithm redundancy
- Labelling Risks: Misplacement on infant feet → Clear IFU warnings

RF Requirements (FCC Part 15 Subpart C, ETSI EN 303 348)

- BLE Power Output: ≤0 dBm (1 mW) to minimize RF exposure for infants
- Bandwidth: 2 MHz channel spacing to avoid interference with Wi-Fi

8. Pain & Emotional Management Devices (Disabilities – TENS Units)

EMC Testing (IEC 60601-1-2, IEC 60601-2-10)

- Immunity to RF Fields: No output current fluctuation under 10 V/m (80 MHz–2.5 GHz)
- ESD: ±15 kV air discharge on controls – no unintended stimulation

Cybersecurity (UL 2900-2-1, GDPR)

- App Security: Prevent unauthorised adjustment of pulse intensity (role-based access)
- Data Localisation: Patient pain logs stored in HIPAA-compliant cloud regions

Electrical Safety (IEC 60601-2-10)

- Output Current Limits: ≤30 mA (DC) to prevent tissue damage
- Leakage Current: <50 µA (normal condition), <500 µA (single fault)

QMS & Risk Management (ISO 13485, ISO 14971)

- Hazard Analysis: Skin burns (Severity: 3) → Thermal sensors to cut off at 41°C
- Usability Testing: Clear electrode placement diagrams for users with limited dexterity

RF Requirements (FCC Part 15B, ETSI EN 301 489-1)

- Wireless Models: BLE must not interfere with cardiac pacemakers (1 m separation test)

9. Emergency-Care Devices (Elderly – Medical Alert Pendants)

EMC Testing (IEC 60601-1-2, EN 301 489-1)

- Immunity to Cellular Interference: Maintain SOS functionality under 20 V/m (700 MHz–2.6 GHz LTE bands)
- ESD: ±8 kV contact discharge on panic button – no false triggers

Cybersecurity (ETSI EN 303 645, UL 2900-2-1)

- Jamming Resistance: Detect and alert during GSM/Wi-Fi signal jamming attacks
- Encryption: TLS 1.2 for cellular data transmission

Electrical Safety (IEC 60601-1, UL 60601-1)

- Battery Backup: 72-hour operation during power outages (IEC 62133)
- Ingress Protection: IP67 rating (1 m water immersion, dustproof)

QMS & Risk Management (ISO 13485, ISO 14971)

- Failure Modes: False-negative alerts → Redundant accelerometers (FMEA)
- Post-Market: Monthly false-alarm rate audits (<1%)

RF Requirements (FCC Part 22/24, ETSI EN 301 511)

- Cellular Band Compliance: LTE Band 13 (Verizon) ±0.1 ppm frequency stability

10. Health Recovery Devices (Post-Surgical EMS Machines)

EMC Testing (IEC 60601-1-2, IEC 60601-2-10)

- Radiated Emissions: ≤30 dBµV/m (30 MHz–1 GHz) to avoid disrupting hospital Wi-Fi
- Magnetic Field Immunity: No malfunction near MRI machines (3T static field)

Cybersecurity (IEC 81001-5-1, NIST SP 800-82)

- Network Segmentation: Isolate therapy control system from hospital IT networks
- Audit Logs: Immutable logs of stimulation parameters (per FDA 21 CFR Part 11)

Electrical Safety (IEC 60601-2-10)

- Output Verification: ±5% accuracy on preset current (20–100 mA)
- Isolation: 4 kV reinforced insulation between patient circuits and mains

QMS & Risk Management (ISO 13485, ISO 14971)

- Risk Documentation: Muscle overstimulation → Current limiter with hardware redundancy
- Clinical Validation: 6-month post-market study on recovery rate improvement

RF Requirements (FCC Part 15B, ETSI EN 300 330)

- Wireless Charging: Qi standard compliance (≤15 W) with no interference to implantables