GUIDELINE FOR TESTING AND CERTIFICATION REQUIREMENT ON 5G/IOT DEVICES

Organiser: hkpc 生產力局

Sponsor: ROHDE&SCHWARZ Make ideas real

SupportingO rganisations: HKEIA 香港電子業商會 · HK TIC · HONG KONG ETA HONG KONG ELECTRONICS & TECHNOLOGIES ASSOCIATION 香港電子科技商會

Funding Organisation: 創新科技署 Innovation and Technology Commission

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 supplied herein, the publisher of this guidebook and the associated organizations in the project cannot be held responsible for any damage resulting from the use of information.

Innovation and Technology Fund

General Support Programme

"Promote Awareness on 5G and IoT Test Requirements"

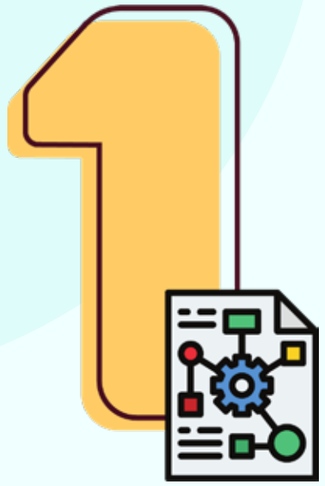
About this Guideline

This project "Promote Awareness on 5G and IoT Test Requirements" is supported by the Innovation and Technology Fund - General Support Programme (GSP) and is organized by Hong Kong Productivity Council (HKPC). To assist the startups, SMEs, other technical solution providers and service providers in meeting the 5G and IoT testing requirements, various activities including a series of technical workshops, promotion seminars and guidebook experience sharing have been carried out in this project. In addition, this guideline which aims to enrich the knowledge of product testing and certification for supporting the startups, SMEs, other technical solution providers and service providers to shorten development cycle and enhance product reliability on 5G and IoT product.

Acknowledgements

We would like to thank the following organizations and party for their support on this project (The names are arranged in alphabetical order).
Hong Kong Association for Testing, Inspection and Certification Limited
Hong Kong Electronics & Technologies Association
Hong Kong Electronic Industries Association (HKEIA)
Hong Kong Productivity Council
Rohde & Schwarz Hong Kong Limited

TABLE OF CONTENTS



INTRODUCTION OF STANDARDS, CERTIFICATION SCHEMES & WIRELESS TECHNOLOGIES FOR IOT AND 5G DEVICES

Chapter 1 – Introduction of standards, certification schemes & wireless technologies for IoT and 5G devices

In this chapter, we will introduce the communication authority and approval and certification scheme for various countries and regions. The latest wireless technologies for IoT and 5G devices will also introduce in this section.

Part A: Asia

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

	Australia	New Zealand
Approval Scheme	Regulatory Compliance Mark	Regulatory Compliance Mark
Based on	RED/FCC/National	National/RED
Duration of approval	Perm	Perm
Approval Label	Y	Y
ICT 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/RED/ National	FCC/ National	RED/FC C
Duration of approval	Perm	Perm	1yr to Perm	Perm	Perm	Perm	Perm
Approval Label	Y	Y	Y	Y**	N	NN,YF	N
ICT Regulator	Canadian Radio-television and Telecommunications Commission (CRTC)		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	RED/FCC	National/ RED/FCC	FCC/RED	FCC/ National	FCC/ National /RED
Duration of approval	Perm	1yr to Perm	5yrs	5yrs	15yrs	3yrs	Perm
Approval Label	N	Y	N	Y	N	Y	N
ICT Regulator	Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)	Agencia Nacional de Telecomunicaoes (ANATEL)		Comision Nacional de Telecomunicaciones (CONATEL)	Unidad Reguladora de Servicios de Telecomunicaciones (URSEC)	Comisión Nacional de Comunicaciones (CNC)	Subsecretaria de Telecommunicacaiones (SUBTEL)

Part C - Europe

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

China

Certification Scheme

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

Certifications are performed according to Guo Biao (GB) standards or in English – National Standards.
The tests are largely similar to CE standards, but Chinese authority does not recognize the test results or reports issued by other countries. It means that only those conducted in China are qualified for CCC certification. Test report is issued in Chinese, certificate is 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 Authorities

China Certification Centre for Automotive Products (CCAP) performs the certification for Automotive suppliers
Chain Quality Certification (CQC) performs the certification for all kinds of products (voluntary)

Details of Certification Scheme

CCC certification

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

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

1. Electrical wires and cables (5)
2. Circuit switches, electric devices for protection or connection (6)
3. Low-voltage electrical apparatus (8)
4. Low power motors (1)
5. Electric tools (16)
6. Welding machines (15)
7. Household and similar electrical appliances (18)
8. Audio and video apparatus (16)
9. Information technology equipment (13)
10. Lighting apparatus (2)
11. Telecommunication terminal equipment (37)
12. Motor vehicles and motor vehicle tires (7)
13. Agricultural machinery (4)
14. Medical devices (7)
15. Fire fighting equipment (12)
16. Safety protection products (11)
17. Home decor and remodeling products (3)
18. Safety parts and accessories of vehicles and motorcycles (14)
19. Toys (6)
20. IT products
21. Ex-products (20)

SRRC certification

The SRRC Type Approval (State Radio Regulation of China) is mandatory for radio type products and also a pre-condition before 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 the identification of parameters and functions of radio transmission equipment like frequency range, frequency band, transmitting power and many more. Including mobile phones (GSM or CDMA), wireless LAN (WLAN) devices, and devices that use the following technologies:

- 2.4GHz / 5.8GHz WLAN devices
- Radar
- Short-range wireless devices
- Microwave devices
- Broadcasting equipment

- Satellite equipment
- Wireless access system (WAS)
- Mobile communication equipment
- Other radio equipment

CCC Standards
https://qai.org/zh-t/ccc%e4%b8%ad%e5%9b%bd%e5%bc%ba%e5%88%b6%e8%ae%a4%e8%af%81/

NAL certification

The Network Access License (NAL) is certification under MIIT. NAL certification is mandatory for cell phones and mobile wireless devices to connect to the China telecom network. Those are further subdivided into two main groups: The basic and the high-end equipment. 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 of the NAL approval process is also relevant for CCC-Certification, so that these tests do not have to be undertaken twice.

Telecommunication terminal equipment:

1. Fixed telephone terminal;
2. Cordless telephone terminal;
3. Group telephone;
4. Fax machine;
5. Modem;
6. PBX;
7. Mobile user terminal;
8. Wireless pager;
9. ISDN terminal;
10. Data terminal;
11. Multimedia terminal;
12. Other telecommunication terminal equipment

Radio communication equipment:

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

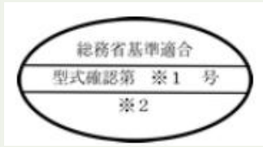
Interconnection equipment:

1. Optical transmission equipment;
2. Digital program control switching system (fixed and mobile system, etc.);
3. No.7 signaling equipment (SS7);
4. Intelligent network equipment;
5. Synchronization equipment;
6. Access network equipment;
7. Frame relay switch;
8. ATM switch;
9. Integrated service switch;
10. Routing equipment;
11. IP network about gatekeeper;
12. Data communication equipment (multiplexing equipment, access server and cross connection equipment, etc.);
13. Call center equipment

Japan

Scheme

There are several mandatory approval mark and label schemes such as PSE, PSC, Energy Saving and RoHs which are under the Electrical Appliances & Materials Safety Law regulated by the Ministry of Economy, Trade and Industry (METI) and Radio Certification label and mark scheme which are under 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  Circle PSE Mark for Category B 	Diamond PSE mark (category A) including 116 items, and other non-specified electrical appliances; Circle PSE mark (category B) including 341 items	https://www.meti.go.jp/policy/consumer/seian/denan/file/06_guide/denan_guide_ver3_en.pdf
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 motorized bicycles or motorcycles) Climbing ropes Oil heaters Oil water heaters Oil bath boilers	
Radio Certification label and mark (mandatory)	Specified Radio Equipment  High-Frequency Devices  Extremely Low-Power Devices  	Specified Radio Equipment: Bluetooth Wi-Fi LTE GSM ZigBee Wireless mics RFID (2.4 GHz, 920 MHz) Telemeters UWB radio systems 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)	https://www.tele.soumu.go.jp/e/sys/equ/tech/index.htm
S-Mark (Voluntary)			http://www.s-ninsho.com/
VCCI (Voluntary)		For 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://www.enecho.meti.go.jp/category/saving_and_new/saving/enterprise/overview/pdf/toprunner2015e.pdf
RoHs (Mandatory) JIS C 0950: 2021	 	[Scope of products] Personal computers Unit-type air conditioners Television sets Refrigerators Washing machines Clothes dryers Microwaves [Specific chemical substances] Lead Mercury Cadmium Hexavalent chromium Polybrominated biphenyl Polybrominated diphenyl ether	https://home.jeita.or.jp/eps/jmoss_en.htm

South Korea (ref: Korea-Certification-Booklet)

Official Certification Authorities

Korean Agency for Technology and Standards (KATS) is a government agency under Ministry of Trade, Industry and Energy (MOTIE). The organization is authorized to regulate and manage the legal measures of South Korea. They are also the member of the International Organization for Standardization (ISO), as well as the International Electrotechnical Commission (IEC).

Certification Bodies

Korea Testing and Research Institute - KTR
Korea Testing Laboratory - KTL
Korea Testing Certification - KTC
Other qualified commercial laboratories

Certification Scheme

KC Certification (KC Mark) –is similar to CE mark scheme including Quality Management and Safety Control of Industrial Products Act" & "Electric Appliances Safety Act"
Korea Standard: K standard

Product groups:

- Consumer goods (i.e.: Household devices, audio and video devices, clothing)
- Children's (under age of 13) products (i.e.: Toys, school supplies, children's chairs)
- Electronics products (i.e.: All electronics product that uses more than 30V (AC) or 42V (DC)

I. KC Safety certification
II. KC Safety Check
III. KC Supplier Conformity Check
IV. KC-EMC Certification
V. KCs Certification for machines and Ex-components
VI. Organizations for Energy efficiency regulations – Korea Energy Management Co. - KEMCO

a. Energy Efficiency Label (mandatory)
b. E-Standby Program (mandatory)
c. High- efficiency Appliance Certification Program (voluntary)

India

Official Certification Authorities

Automotive Research Association of India (ARAI)
Bureau of Indian Standards (BIS)
Telecommunication Engineering Center (TEC)
The Wireless Planning & Coordination of India (WPC) - National Broadcasting authority and part of Ministry of Communications and Information Technology

Certification scheme

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

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

TEC designed Mandatory Testing and Certification of Telecom Equipment (MTCTE) 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 Licenses for radio equipment.

WPC
WIRELESS PLANNING & COORDINATION CERTIFICATION

Details of certification scheme

test reports from other accredited laboratories may also be accepted for certain types of products (which has to be checked on an individual basis).

BIS

The Bureau of Indian Standards (BIS) has published the "List of products and Associated Indian Standards" on the official website: https://bis.gov.in/. Only electronics related items are listed below.

Transformer
Ceiling Fans and Fan Regulator
Circuit Breakers
Flameproof Enclosures
Three Phase and Single Phase A.C. Motors
Plugs, Socket and Switches
PVC Cables
Geyser
Electrical Energy Meters
Luminaires, LED bulbs, Modules
Hearing aid
Camera Devices for Video Surveillance System
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 telegraph authority from time to time.

Products listed under TEC-MTCTE:

Network (2-Wire telephone equipment, Modem, Cordless Telephone, etc.)
IoT/M2M (Smart devices, IoT Gateway, etc.)
Fixed Access
Information technology (Switch, Router, Server, etc.)
Mobile devices
Radio (VHF, UHF, equipment operating in 2.4GHz & 5GHz, Satellite system, etc.)
PON family 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.

Aerial
Antenna
Directional Radio Microwave Link
Feeder
Network Object (Channels switch, Base telecommande, etc.)
Radio Navigational apparatus (Beacon, Navigation management, etc.)
Receiver (GPS, VHF Receiver, Communication receiver, etc.)
Transceiver (Modem, Radar Transponder, WiFi Equipment, WLAN, etc.)
Transmitter (Wireless Access Point, Router, etc.)

Australia & 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 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 RCM scheme, there are five main labeling 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 programs.

Europe

CE originated from the French abbreviation of the European Community, "Conformité Européenne", which is a safety conformity mark widely recognized 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 to circulate freely on the EU market, you must affix the CE mark. 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 33 countries: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Liechtenstein, Luxembourg, Malta, Norway, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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 requires 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, covering 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.

U.S.A.

FCC is the abbreviation of Federal Communications Commission, that is, the Federal Communications Commission of the United States. It mainly controls radio, television, telecommunications, satellites and so on to coordinate domestic and international communications in the United States. According to regulations in November 2017, the FCC regulation is now divided into FCC ID certification and FCC Supplier's Declaration of Conformity (sDoC) (combined the original FCC DoC and FCC Verification).

FCC ID certification is a compulsory certification for wireless products in the United States. After the product has been tested, it meets the FCC requirements and can be authorized by the FCC ID number. FCC reports are widely recognized internationally, and are often used for international transfers, which can reduce the time cost and expense of repeated testing, and make products go to market quickly.

FCC requirement covers a wide range of products, common are: wireless terminal products, PCs and peripherals, household appliances, IT/AV products, multimedia equipment, lamps, toys, security products and industrial machinery products, etc.

Canada

The Certification and Engineering Bureau of Innovation, Science and Economic Development (ISED) Canada (formerly Industry Canada (IC)) provides a certification service for radio equipment and a registration service for terminal equipment in Canada. It also regulates the radio spectrum for all transmitters operated in Canada. The Radio Standards Specifications (RSS) detail the technical requirements for radio transmitters.

The ISED regulations covering radio frequency devices are structured with RSS-GEN essentially the equivalent of Code of Federal Regulations (CFR) Title 47 Part 2 of the Federal Communications Commission (FCC) in the US. RSS-GEN covers matters relating to procedures for certification, including technical and administrative requirements. Contrary to popular belief, FCC certification for the US market is not equivalent to the approval of ISED regulations in Canada. For the Canadian market, an approval of the authority ISED (Innovation, Science and Economic Development Canada) is necessary. Without such certification, market access for Canada for manufacturers of products with radio technologies is excluded.

Manufacturers, importers, distributors and vendors shall make sure that all wireless radio equipment and wireline telecommunication equipment which imported into Canada or deployed in the Canadian marketplace, or both, shall comply at all times with ISED's requirements.

Innovation, Science and Economic Development Canada

United Kingdom of Great Britain

The UKCA (UK Conformity Assessed) marking is a new UK product marking that is used for goods being placed on the market in Great Britain (England, Wales and Scotland). It covers most goods which previously required the CE marking, known as ‘new approach’ goods.

The UKCA marking came into effect on 1 January 2021. It allows businesses time to adjust to the new requirements, it is able to use the CE marking until 1 January 2023 in most cases. The standards used by UKCA still follow the CE system, and the process is also consistent. The only difference is the Conformity Assessment tasks for UKCA mark must be carried out by a UK Approved Body. The product areas listed below are covered by the UKCA marking:

- Toy safety
- Recreational craft and personal watercraft
- Simple pressure vessels
- Electromagnetic compatibility
- Non-automatic weighing instruments
- Measuring instruments
- Lifts
- ATEX
- Radio equipment
- Pressure equipment
- Personal protective equipment
- Gas appliances
- Machinery
- Equipment for use outdoors
- Ecodesign
- Aerosols
- Low voltage electrical equipment
- Restriction of hazardous substances

IoT wireless technology:

The following wireless communication technologies are commonly used in the telecommunications and IoT industry to refer to IoT devices:

Wi-Fi

- Used for local area networking of devices and Internet access
  - Technologies: IEEE 802.11b, 802.11g, 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6 /6E)
  - Frequency bands: 2402-2480MHz (802.11b,g,n,ax), 5150-5350MHz, 5470-5725MHz, 5725-5875MHz (802.11ac,ax), 5925-6425/7125MHz (802.11ax)

Bluetooth

- Used for a short-range exchanging data between fixed and mobile devices over short distances
- Technologies: Bluetooth Low Energy (BLE), Bluetooth Classic 1.0 - 5.2
- Frequency bands: 2402-2480MHz
- Channels: 40 channels with 2Mhz spacing (BLE), 79 channels with 1MHz spacing

Narrowband IoT (NB-IoT)

- Used for setting up a connection between IoT devices and services
- Technologies: 3GPP LTE (Release 13)
- Frequency bands: coexistence with both LTE and GSM
- Band number Uplink frequency range / MHz Downlink frequency range / MHz
- 1 / 1920 - 1980 / 2110 - 2170
- 2 / 1850 - 1910 / 1930 - 1990
- 3 / 1710 - 1785 / 1805 - 1880
- 5 / 824 - 849 / 869 - 894
- 8 / 880 - 915 / 925 - 960
- 12 / 699 - 716 / 729 - 746
- 13 / 777 - 787 / 746 - 756
- 17 / 704 - 716 / 734 - 746
- 18 / 815 - 830 / 860 - 875
- 19 / 830 - 845 / 875 - 890
- 20 / 832 - 862 / 791 - 821
- 26 / 814 - 849 / 859 - 894

- 28 / 703 - 748 / 758 - 803
- 66 / 1710 – 1780 / 2110 – 2200

LoRa

- Used for long range, low power and secure data transmission for M2M and IoT applications
- Technologies: IEEE 801.15.4g
- Frequency bands: 868 MHz band or 915MHz band

Near-Field Communication (NFC)

- Used for communication between two electronic devices over a distance of 4 cm or less.
- Technologies: Radio-frequency identification (RFID), ISO14443, ISO18000-3, ISO15693
- Frequency bands: 13.56MHz

Radio-frequency identification (RFID)

- Used for setting up a wireless system with the Tags and Readers to automatically identify the information from the objects attached a tag
- Technologies: Active and Passive RFID
- Frequency bands: 433MHz (Active RFID), 856-960MHz (Passive RFID)

Sigfox

- Used for providing a long range, low power and low data rate wireless connectivity for devices like remote sensors, actuators and other M2M and IoT devices
- Technologies: Ultra Narrow Band modulation
- Frequency bands: 868 MHz band or 902MHz band

Ultra-wideband (UWB)

- Used for setting up a short-range and low power network to instantaneously tracks the device's movements and positions in real-time
- Technologies: IEEE 802.15.4z
- Frequency bands: 3.1 - 10.6 GHz or 6.0 - 8.5GHz

IOT AND 5G TESTS REQUIREMENT IN EMC

Chapter 2 EMC Requirement

China:

EMC test is one of testing requirement in GB standards. GB standards are the basis for the product testing which products must undergo during the China Compulsory Certificate (CCC or 3C) certification. If there is no corresponding GB Standard, CCC is not required. All products listed in the CCC catalogue must pass the certification carried out by authorised certification bodies designated by the state and can only leave the factory, be imported, sold and used at business venues upon meeting the statutory quality standard and obtaining the relevant certificate and CCC mark. IoT devices and 5G products fall into the category of Electrical and electronic products.

EMC Standards:
Emission requirement:
GB 9254-2008 《信息技术设备的无线电骚扰限制和测量方法》
(equivalent to CISPR 22: 2006)
GB17625.1-2012《電磁相容限值諧波電流發射限值(設備每相輸入電流≤16A)》
(equivalent to IEC 61000-3-2.2009)
GB17625.2-2007 《电磁兼容 限值 对每相额定电流≤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 requirement:
GB/T 17618-2015《信息技术设备 抗扰度 限值和测量方法》
(equivalent to CISPR24: 2010)

Japan

The PSE Mark is a mandatory safety and EMC (Electro Magnetic Compatibility) approval for electrical products sold on the Japanese market. The PSE Law is the DENAN Act (Electrical Appliance and Material Safety Act) of Japan. The Japanese Ministry of Economy, Trade and Industry (METI) is the responsible authority for the PSE Certification.

EMC of low-power, DC-input products is generally not covered by the PSE Law or Radio Law. To supplement this issue, a voluntary scheme was established in Japan which is operated by the VCCI Council.

Radio Equipment in Japan is required to comply with Japan Radio Law. It divides to three types of radio equipment: Specified Radio Equipment (e.g., Bluetooth, Wi-Fi, LTE, GSM, ZigBee, Wireless mics, RFID (2.4 GHz, 920 MHz), Telemeters, UWB radio systems)

EMC Standards:
Emission requirement:
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

KC Certification (KC Mark) is a mandatory certification scheme and mark that must be applied for and appear on products for electrical appliances, toys, textile listed in the related Korean laws and ordinances. Electromagnetic Compatibility (EMC) is one of the requirements in this KC Certification, a mandatory certification scheme. It is similar to CE mark scheme.

EMC Standards:
Emission requirement:
KS C 9832: 2019 멀티미디어기기 전자파 장해방지 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

The Australian Communications and Media Authority (ACMA) incorporates the listed standards as mandatory standards under section 162 of the Radiocommunications Act 1992 as part of the ACMA's Electromagnetic Compatibility (EMC) Regulatory Arrangement. The ACMA mandates performance requirements in relation to emissions, therefore compliance to standards within this list is only required to the extent that matters within the standards that relate to the interference to Radiocommunications and any uses or functions of devices. The immunity, harmonics and flicker tests are not required by the ACMA. For EN, IEC and CISPR standards, unless stated otherwise, the expiry date of a standard is taken to be the expiry date published in the Official Journal of the European Union (OJEU).

Emission requirement:
AS/NZS CISPR 32 / EN 55032 / CISPR 32 Electromagnetic compatibility of multimedia equipment—Emission requirements

Saudi Arabia

The Communications and Information Technology Commission (CITC) is the government authority for wireless, telecom, and EMC aspects of electronic products, including limits on human exposure to radio frequencies. CITC accepts both EU Directive “CE” compliance reports and FCC grant and reports as proof of compliance. CITC is responsible to issue the technical specification for telecommunications and IT equipment. The technical specification GEN001 is applicable and mandatory to any IoT equipment.

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

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

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

United Kingdom:

The Electromagnetic Compatibility Regulations 2016 ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance. The Electromagnetic Compatibility Regulations 2016 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 Regulations 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.

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

United States:

The Federal Communications Commission, FCC in the USA imposed legal limits on the electromagnetic emissions from all digital equipment. These limits were imposed as a result of all electronic and electrical equipment that were interfering with wired and radio communications and broadcast systems. FCC Part 15 is the section of Title 47 of the Code of Federal Regulations that covers EMC and is regulated by the Federal Communications Commission (FCC). It specifies limits on the radiation from both intentional and unintentional radiation sources.

Most electronic and electrical equipment regulated by FCC Part 15, Subpart B fall into one of two categories. Class A devices are those that are marketed for use in a commercial, industrial or business environment. Class B devices are those that are marketed for use at home. Class B limits are more stringent than Class A limits as indicated in the tables below. The radiated and conducted EMI test procedures are defined in the ANSI Standard C63.4. The FCC Rules and Regulations, Part 15, only regulate electromagnetic emissions. Currently there are no FCC regulations pertaining to product immunity to electromagnetic fields.

Canada:

The Department of Innovation, Science and Economic Development Canada (ISED; formerly Industry Canada) is responsible for producing EMC standards whose requirements need to be met in order to place products on the Canadian market. This Interference-Causing Equipment Standard (ICES) ICES-003, issue 7, Information Technology Equipment (including Digital Apparatus), sets out limits and methods of measurement of radio frequency emissions, as well as administrative requirements for information technology equipment (ITE), including digital apparatus

IOT AND 5G TESTS REQUIREMENT IN CYBERSECURITY

Chapter 3 IoT and 5G Tests requirement in Cybersecurity: Adopting IoT Security Best Practices - Taking Small Steps Towards a Secure Cyberspace

1. Introduction

The Internet of Things (IoT) market continues to grow. According to Gartner, the IoT market would grow to 5.8 million endpoints in 2020[1]. More and more IoT devices will connect to the Internet. Research on the state of the IoT connections[2] indicated, "Of the 21.7 billion active connected devices worldwide, 11.7 billion (or 54%) will be IoT device connections at the end of 2020." Along with the growing trends, the number of IoT device connections will soon dominate the whole Internet cyber space.

Cyber security has been a critical concern in information technology systems for years. Cyber-attacks are ever-changing. Threat actors keep changing their attack tactics, such as phishing attacks themed with different current affairs and trendy information. Ransomware also evolved into multiple extortions and expanding attack targets on critical infrastructure and industrial control systems. To defend against cyber-attacks, information technology (IT) systems can adopt well recognised international standards and a variety of IT security solutions are available. However, unlike IT systems, IoT technology faces a totally different picture in implementing security. Due to the hardware capability and characteristics, IoT devices are insecure by nature. Implementing IoT security has many challenges and constraints to overcome.

This paper will overview cyber security threats to IoT devices and look into the current status of the latest IoT security requirements, best practices and standards.

---

1 Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020
https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

2 State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time
https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

2. Cyber Security Threats to IoT Devices

2.1 Key Elements in IoT Ecosystems

To understand the cyber security threats to IoT devices, we first look at the key elements building up the IoT ecosystems. IoT ecosystems are built with four key elements, namely IoT devices, network connectivity, cloud platform and application.

The main difference between IT and IoT is that IoT devices have interaction with the physical world. Besides the network, computation and storage, IoT devices have sensors and actuators. IoT devices can sense the physical environmental changes and have mechanical control over an object.

IoT devices connect to backend application systems through wired or wireless connections to the Internet. With network connectivity, application systems can collect sensor data for data analytics or send out control instructions to IoT devices according to the application processing logic.

IoT application systems primarily leverage cloud platforms for its benefits like scalability and flexibility. Besides, IoT applications on cloud platforms can be easily integrated with other cloud technologies, such as big data analytics, artificial intelligence, blockchain, etc.

Mobile Apps or online web portals are common user interfaces to interact with the IoT application and IoT devices. It serves as the application frontend for device management, device control and data visualisation.

2.2 Cyber Security Threats

Threat actors always attempt to find the weakest link in cyber security. In IoT ecosystems, all four key elements are equally susceptible to cyber-attacks. We will focus on cyber security threats specific to IoT devices in the following sections.

2.2.1 IoT Malware and Botnet

IoT Malware and Botnet are the major security threats to IoT devices. Malware is a general terminology and some common types of malware are viruses, worms, Trojan horses, botnets, spyware and adware. Malware can steal confidential information, damage system data and software on the computer and disrupt or disable the computer system and network. Malware is a well-known security threat in IT systems running common operating systems, such as Microsoft Windows and Linux.

Since the development of IoT technology, it is observed that more and more malwares are targeting IoT devices. IoT malware specifically targets different types of embedded processors, such as ARM, MIPS, PowerPC, etc., common in IoT devices hardware. From security research on the history of IoT malware threats[3], a few IoT malwares were discovered since 2002. There was a significant growth of IoT malwares discovered since 2014 to 2018. According to the Kaspersky Lab IoT report[4], new IoT malwares grew three-fold in the first half of 2018.

Some sophisticated IoT malwares, known as botnet, even utilise command and control (C2) architecture to launch attacks with the infected IoT devices at scale. Once IoT devices are infected with this malware, they become part of a botnet and wait for attack instructions from C2 server. Mirai was an infamous IoT botnet, where its large-scale DDoS attack in 2016[5] brought down servers of Dyn, a company that controls much of the Internet's domain name system (DNS) infrastructure, affecting major sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US. Since this DDoS attack in 2016, the DDoS attack situation is even worse. According to an analysis from Google[6], the scale of DDoS attacks is rising exponentially. From the analysis, the DDoS attack recorded up to

3 IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks
https://blog.f-secure.com/iot-threats/

4 New IoT-malware grew three-fold in H1 2018
https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018

5 DDoS attack that disrupted internet was largest of its kind in history, experts say
https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

6 Exponential growth in DDoS attack volumes
https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks

2.54 Tbps, enough for saturating the bandwidth of twelve thousand fixed broadband users in Hong Kong[7].

The source code of the in-famous malware, Mirai, was published publicly in 2016. Based on the source code, threat actors are expected to develop different malware variants of Mirai malware to attack IoT devices. In recent years, IoT malware was discovered with enhancing features and capabilities. One of the noteworthy trends were peer to peer networking capability that increases the difficulty of being detected or taken down.

2.2.2 Software Vulnerability in IoT Products

There have been several critical vulnerabilities discovered that affect hundreds of millions of IoT devices. It is not difficult to cite a few examples in recent years. A series of vulnerabilities in a widely used low-level TCP/IP software library was discovered by JSOF research lab in Jun 2020, dubbed as 'Ripple 20'[8]. Another vulnerabilities, dubbed as 'NAME:WRECK'[9], related to TCP/IP software library, was discovered by Forescout and JOSF research lab in Apr 2021. Two dozen vulnerabilities in widely used real-time operating systems (RTOS) were discovered by Microsoft researchers in Apr 2021, dubbed as 'BadAlloc'[10]. A vulnerability in a widely used peer-to-peer software development kit (SDK) library was discovered by Nozomi Networks[11] in Jun 2021. Successful exploitation of these vulnerabilities can lead to device compromise, letting threat actors to take control of the IoT devices to implant malware or launch other attacks.

Vulnerabilities exist in all types of software. Software vulnerabilities are one of the initial attack vectors in cyber-attacks. IoT devices are essentially small computers that run the software, aka firmware, on embedded processors or microcontrollers. If a software vulnerability was identified but not yet patched, it is a security risk that threat actors can exploit the vulnerability to compromise IoT devices.

7 Internet Speeds By Country 2021
https://worldpopulationreview.com/country-rankings/internet-speeds-by-country

8 Ripple20 - https://www.jsof-tech.com/disclosures/ripple20/

9 NAME:WRECK - https://www.forescout.com/research-labs/namewreck/

10 Microsoft Finds 'BadAlloc' Flaws Affecting Wide-Range of IoT and OT Devices
https://thehackernews.com/2021/04/microsoft-finds-badalloc-flaws.html

11 New IoT Security Risk: ThroughTek P2P Supply Chain Vulnerability
https://www.nozominetworks.com/blog/new-iot-security-risk-throughtek-p2p-supply-chain-vulnerability/

However, many vulnerabilities in IoT devices are either "no patch available" or "no plan to patch". IoT product manufacturers in general have yet to establish proper vulnerability management of their IoT products. Once an IoT product releases from the product line, the ongoing software support is minimal. Manufacturers may not be able to release patches to fix security vulnerabilities timely. Due to business considerations, some manufacturers may decide not to invest in software maintenance of their IoT products further.

Even if security patch is available, pushing out software patches to IoT devices is another issue. On the consumer side, users often setup the IoT devices once and then forget. Without any display or user interface on IoT devices, users may not notice the need for software updates. On the product side, the lack of an automatic update mechanism is another issue for software updates. When IoT devices are deployed at scale or dispersed in remote locations, it is not feasible to perform manual software update without the support of over-the-air (OTA) update.

2.2.3 Risk of Safety Hazard

A recent cyber-attack caused Colonial Pipeline[12] to shut down its operation in May 2021. This incident raised the concern on critical infrastructure safety due to cyber-attacks. In the same sense, a cyber-attack on IoT applications also poses a safety hazard risk. It is because some IoT use cases involve mechanical control on machinery or having direct control on electricity or heating element.

Some vulnerabilities were identified from IoT security research and may cause a safety hazard. A vulnerability in a smart hair straightener product[13] could be exploited to set its heating power remotely. If users accidentally leave the product unattended near flammable materials, at the highest temperature (235 degrees Celsius) the product can easily catch fire. Another vulnerability, dubbed as 'BadPower'[14], was reported by Tencent Security Research Lab. It could be exploited to corrupt the fast charger's charging current and set your device on fire.

Indeed, the situation of cyber security threats on IoT devices is alarming. It is foreseeable that IoT devices will dominate the Internet cyber space as a vital portion of connected devices. If all practitioners in IoT industry

12 Hackers Breached Colonial Pipeline Using Compromised Password
https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

13 Burning down the house with IoT
https://www.pentestpartners.com/security-blog/burning-down-the-house-with-iot/

14 BadPower - https://xlab.tencent.com/en/

together act on IoT security today, it will significantly improve the overall cyber security posture in the future.

3. Status of Latest IoT Security Requirements, Best Practices and Standards

The adoption of IoT security is lagging behind the pace of IoT development. It is a common situation that IoT manufacturing optimise functionality over security and fails to put sufficient resources on IoT security. On the other hand, the lack of well-recognised international IoT security standards also hinders the adoption of IoT security.

In recent years, different countries start making a step forward in IoT security development and formulating regulations.

3.1 Cyber Security Labelling Scheme

Finland[15], UK[16] and Singapore[17] have announced cyber security labelling schemes for IoT products in Nov 2019, Jan 2020 and Oct 2020 respectively. With the analogy to food security, the labelling scheme will give consumers a rating of the level of cyber security provisions of the products. It enables consumers to identify products with better security and make an informed decision. The labelling scheme also benefits the IoT industry by having an incentive to improve their product security for outstanding competitiveness.

For Singapore, the labelling scheme is categorised into four tiers, from the least advanced tier 1 to the most advanced tier 4. The scheme adopted a baseline security requirement from European Standard, identified as ETSI EN 303 645[18], as the tier 1 requirement. For Finland, the scheme also adopted ETSI EN 303 645 as the certification criteria. For the UK, the scheme based on the guideline within Code of Practice for consumer IoT security published by UK Government, later formulated as European Standard ETSI TS 103 645[19] with the supporting work by the European Telecommunications Standards Institute (ETSI).

It is observed that the development of IoT security regulations and IoT security standards are tightly dependent. As such, the establishment of requirements and standards is crucial to advance the regulations in different countries.

3.2 Status of IoT Security Requirements and Standards

As of 2021, there are several guidelines, best practices and standards developed and published by different international bodies and security organisations. The below sections will highlight some of the key documents worth referencing and preview some future development.

3.2.1 International Bodies

Since part of the IoT ecosystem rely on IT systems and applications, it is worth first referencing the well-recognised ISO/IEC standards from the IT perspective. ISO/IEC 27001[20] Information Security Management is the fundamental guidance and certification standard in formulating an information security management system (ISMS) within an organisation. Another standard, ISO/IEC 27017[21], focuses on cloud security with security controls for the use of cloud services. These standards cover major security areas, including company security policy, asset management, physical and environmental security, access control, communication security incident management and regulatory compliance.

For ISO/IEC standards related to IoT security, ISO/IEC 27400[22] “Cybersecurity — IoT security and privacy — Guidelines”, provides guidelines on IoT security and privacy. However, ISO/IEC 27400 is still under development and calling for comments on the draft at the moment of writing.

15 Finland becomes the first European country to certify safe smart devices new Cybersecurity label helps consumers buy safer products
https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

16 Government to strengthen security of internet-connected products
https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

17 Cybersecurity Labelling Scheme by Cyber Security Agency of Singapore
https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls

18 ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

19 ETSI TS 103 645 Cyber Security for Consumer Internet of Things
https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

20 ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT
https://www.iso.org/isoiec-27001-information-security.html

21 ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
https://www.iso.org/standard/43757.html

22 ISO/IEC DIS 27400 Cybersecurity - IoT security and privacy Guidelines
https://www.iso.org/standard/44373.html

National Institute of Standards and Technology (NIST) of US published NISTIR 8259[23] "Foundational Cybersecurity Activities for IoT Device Manufacturers" in May 2020. It recommends actions that IoT device manufacturers should perform in relation to cyber security before selling IoT devices to customers. At the time, NIST of US also published NISTIR 8259A[24] "IoT Device Cybersecurity Capability Core Baseline". It lists out the baseline security capability required in designing, integrating, and implementing IoT devices to address cyber security risks. It covers the security areas, including device identification, device configuration, data protection, logical access to interfaces, software update and cyber security state awareness.

European Telecommunications Standards Institute (ETSI) published "Cyber Security for Consumer Internet of Things: Baseline Requirements", ETSI EN 303 645[25], in Apr 2020. It provided a set of 13 recommendations of security baseline for connected consumer products. The top three recommendations are no default passwords, implement a vulnerability disclosure policy, and keep software updated.

For the IoT security related to Industrial Control Systems, ISA/IEC 62443[26] is a series of standards that provide a framework to address and mitigate security vulnerabilities in industrial automation and control systems.

3.2.2 Cyber Security Organisations

OWASP Internet of Things Project of OWASP Foundation, a globally respected source of guidance on web application security, released "OWASP IoT Top 10"[27] in 2018. It represents the top ten things to avoid when building, deploying, or managing IoT systems. The foundation has another new project, "OWASP IoT Security Verification Standard"[28] under development. As of the current development status, it provides security requirements on five components as a stack, including hardware platform, communication, software platform, user space applications and IoT ecosystem. It also divided a set of requirements into three security verification levels to suit different IoT use cases and products nature.

IoT Security Foundation updated "IoT security compliance framework"[29] in May 2020 since its first publication in 2016. For the flexibility of use, the framework is defined into four classes, from Class 0 for simple devices requiring fewer security measures to Class 3 for devices handling sensitive data. With the mapping of class and requirement applicability, the framework helps the auditor or self-assessor determine the compliance level and select the appropriate security measures from the total 233 requirements.

Hong Kong Computer Emergency Response Team (HKCERT), a centre for coordination of computer security incident response for local enterprises and internet users, published "IoT Security Best Practice Guidelines"[30] for developers to adopt IoT security at the early stage of design and development. The guidelines cover common security issues in four layers of IoT solutions, including perception layer, network layer, management layer, and application layer. The guidelines include security best practices and a simple checklist for self-verification. It aims to help developers incorporate IoT security best practices starting from the design stage and throughout the development cycles. In addition, this guideline may serve start-ups, SMEs or enterprises as a reference of security specifications in the sourcing of IoT solutions. General users can also learn more about IoT security best practices through this guideline and raise security awareness in using IoT devices.

4. Conclusion

The cyber security threats to IoT devices are threatening. We must act on IoT security today and adopt IoT security requirements, best practices and standards as fast as possible. We hope IoT developers, manufacturers, business owners and industry practitioners have a better understanding of IoT security. We hope with taking a small step to adopt IoT security all together, we can build a more secure cyber space.

23 NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers
https://csrc.nist.gov/publications/detail/nistir/8259/final

24 NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline
https://csrc.nist.gov/publications/detail/nistir/8259a/final

25 ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

26 New ISA/IEC 62443 standard specifies security capabilities for control system components
https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

27 OWASP IoT Top 10
https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

28 OWASP IoT Security Verification Standard
https://owasp.org/www-project-iot-security-verification-standard/

29 IoTSF Issues Update to Popular IoT Security Compliance Framework
https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/

30 Implementing IoT Security Best Practice
https://www.hkcert.org/security-guideline/implementing-iot-security-best-practice

IOT AND 5G TESTS REQUIREMENT IN ELECTRICAL SAFETY

Chapter 4 Electrical Safety

Electrical Safety Always Matters

Everyone could imagine how dangerous it is if an electrical appliance was not tested before putting on the market. Electrical safety always matters and has been treated as one of the key parts in product testing under market access requirements. Unarguably, electrical safety testing plays an essential role to ensure that various kinds of electrical and electronic products in the markets are safe and protect people from potential fatal electric shock.

The More Smart Products, the More Safety Concerns

Hong Kong is physically small, but its compact urban environments can be beneficial for the enterprises to get inspirations in developing more and more innovative smart products. The necessity of anti-epidemic measures and the aging population can also be seen as the factors for facilitating various kinds of technological developments. Smart technologies can almost be applied in everywhere now and are rapidly evolving into key parts of business success in industries. IoT and 5G are expected to unleash their true potential to a wider range of new applications such as gerontechnology, smart hospital, smart building, smart lighting, smart mobility, etc. in years ahead. As our city becomes smarter, the importance of product testing becomes more significant in sophisticated and connected environments. With an increase in the number of smart products in homes and working environments, the chances of electrical accidents and incidents occurring would increase.

Only Decent Testing Can Tell How Safe the Products Are

Smart products come with their own set of technical requirements as they are more complicated than conventional electrical and electronic products. Manufacturers, importers, retailers seeking to bring their products to the markets face diverse challenges, for instance, some countries and jurisdictions impose particular test requirements. All these local enterprises need to pay more attention to product testing than before. Obviously, the proliferation of smart products will not only bring innovation and business opportunities but public concerns as well. Electrical safety testing is vital part to support product development and is also the most efficient way of ensuring product safety, lowering liability risks, protecting company reputation and building customer confidence. People need to keep in mind that only decent testing can tell how safe the products are.

Typical Requirements for Electrical Safety for Overseas Markets

EUROPE

- **Low Voltage Directive (LVD) 2014/35/EU**

  Achieving electrical safety compliance with the Low Voltage Directive (LVD) 2014/35/EU is an important part of the CE marking process. Manufacturers must demonstrate compliance with the LVD to place a CE Mark on electrical products for being sold in the European Market:

  - **Scope**

    The LVD covers all electrical products with the electrical input or output, specifically in the range of 50-1000V AC or 75-1500V DC. These voltage ratings refer to the voltage of the electrical input or output, not to voltages that may appear inside the electrical product.

    The LVD is not limited to cover electrical safety but also considers the various aspects that can harm human health. The following common hazards need to be assessed:

■ Products

◆ Examples of products within the scope of the LVD are as below:

- Audio and Video Equipment
- Electrical Cables and Wires
- Electrical Household Appliances
- Lighting Products
- Handheld Home Appliances
- Laboratory Equipment

◆ The following products are **NOT** covered by the LVD:

- Plugs and Socket Outlets for Domestic Use
- Electricity Meters
- Electrical Equipment for Radiology and Medical purposes
- Electric Fence Controllers
- Electrical Equipment for Use in an Explosive Atmosphere
- Electrical Parts for Goods and Passenger Lifts
- Specialised Electrical Equipment for Use on Ships, Aircraft or Railways
- Custom Built Evaluation Kits destined for Professionals to be Used Solely at Research and Development Facilities

■ Standards

◆ Examples of European harmonised standards for the products within the scope of the LVD:

Audio and Video Equipment	Electrical Cables and Wires	Electrical Household Appliances
EN 62368-1 Audio/video, information and Communication Technology Equipment - Safety Requirements	EN 50525-1 Electric cables - Low voltage energy cables of rated voltages up to and including 450/750 V (U0/U) - Part 1: General requirements	EN 62233 Measurement Methods for Electromagnetic Fields of Household Appliances and Similar Apparatus with Regard to Human Exposure

Handheld Home Appliances	Laboratory Equipment	Lighting Products
EN 60335-1 Household and Similar Electrical Appliances – Safety — Part 1: General Requirements	EN 61010-1 Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - General Requirements	EN 60598-1 Luminaries — Part 1: General Requirements and Tests

- Under the LVD 2014/35/EU, only the references of the harmonised standards published in the Official Journal of the European Union (OJEU) give presumption of conformity with the safety objectives. The latest summary list of titles and references of harmonised standards under the LVD can be found in the below link:

  https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/low-voltage_en

  (Last Update: 30/08/2021)

Important Notes

- Before placing electrical product on the European market, the manufacturer or the authorised representative, the manufacturer is required to ensure that:

  - the product is safe for humans, animals and properties;
  - the product carries a document with it to provide consumers with appropriate usage guidance; and
  - the product can resist environmental conditions and is not influenced by them in such a way as to make it injurious for humans and animals

- The manufacturer is required to affix CE marking and formulate a written EU declaration of conformity (DoC).

- The manufacturer must establish the technical documentation.

- The DoC must be kept in a technical file for 10 years after the product has been placed on the market.

- The technical file should, at least, contain the following:

  - General description of the product
  - Basic design and manufacturing drawings, sketches of the circuits, component, etc. with their descriptions
  - A list of the applied harmonised standards
  - Results of the calculations and tests
  - Report of the tests

- Risk Assessment:

  - The manufacturer is required to include an adequate analysis and assessment of the potential risks for the product within the technical file. The risk assessment should be undertaken as part of the conformity process.

  - The purpose of the risk assessment is to help the manufacturer identify the hazards relevant to the products and to use this information to help identify the applicable essential requirements of the LVD and any standards that can be employed to reduce or eliminate the risks. Whilst risk assessments can be subjective, CENELEC (French: Comité Européen de Normalisation Électrotechnique; English: European Committee for Electrotechnical Standardization) has issued a guidance to help manufacturers by providing key information for what these risk assessments for electrical safety should entail.

  - The CENELEC guidelines for safety related risk assessment and reduction under the LVD can be found at: ftp://ftp.cencenelec.eu/CENELEC/Guides/CLC/32_CENELEC Guide32.pdf

United States

- **Safety Certifications for the United States (US) Market**

  The Occupational Safety and Health Administration (OSHA), the US organisation ultimately responsible for ensuring safe and healthful working conditions, involves setting and enforcing safety standards for products. OSHA's Nationally Recognized Testing Laboratory (NRTL) Program is to provide evaluation, testing and certification of products. Each NRTL has its own scope of test standards and uses its own registered certification mark(s) to designate product conformance to the applicable product safety test standards, providing assurance that the products meet the safety requirements to enter the United States.

  ■ **Certification Process**

  ◆ Listing/Certification Evaluation:

  While the product itself will be evaluated and tested for conformance with the appropriate standards, the manufacturer must demonstrate a Quality Control system to assure that all future products will continue to conform. To maintain the certification mark, the manufacturer is required to conduct regular factory audits.

  ◆ Steps to Product Certification:-

  ✧ <u>Product Testing and Evaluation:</u>
  Product sample is tested, and relevant documents are evaluated pursuant to the applicable safety standard(s).

  ✧ <u>Factory Inspection:</u>
  Factory Inspection is performed prior to the issuance of the certification.

  ✧ <u>Follow-up Visit:</u>
  Follow-up visits are performed at the manufacturing site(s) for reviewing production line tests, quality procedures and relevant documents, etc.

■ **Standards**

If manufacturers are planning to sell the electrical and electronic product in the United States, there are two things they need to consider first – FCC regulations and UL standards. Although UL standards are generally voluntary, service providers such as Amazon require that many electrical and electronic products comply with UL standards. So essentially, UL standards play a key role for ensuring product safety for the US market.

◆ Here are some examples of UL standards:

✧ UL 50 - Enclosures for Electrical Equipment
✧ UL 1026 - Electric Household Cooking and Food Serving Appliances
✧ UL 60335-1- Household and Similar Electrical Appliances, Part 1: General Requirements
✧ UL 62368-1 - Audio/Video, Information, and Communication Technology equipment

◆ Product Safety Concerns Specific to Smart Appliances:

The current electrical end-product safety standards for household appliances are intended to address the anticipated risks associated with the product's design or use. However, these standards may not address the specific additional risks associated with smart appliances. For instance, Smart appliances incorporate interfaces and circuitry designed for support of effective power management on the communications functions. Such electronic communications circuits, as well as the circuits that power them, must be isolated to protect the user from electric shock. In addition, a smart appliance can receive incoming signals that could add new operating functionality or modify existing functionality that has not been thoroughly evaluated. Controls may be required to prevent the addition of new unintended functions, or the modification of existing functions.

◆ Addressing the Product Safety Gap:

UL has published a series of Certification Requirement Decisions (CRDs) which specifically address potential safety issues directly related to the communications interfaces and control circuits required to support smart functions.

CRDs for the following major appliance standards are currently available:

- ✧ UL 174 - The Standard for Safety of Household Electric Storage Tank Water Heaters
- ✧ UL 250 - The Standard for Safety of Household Refrigerators and Freezers
- ✧ UL 484 - The Standard for Safety of Room Air Conditioners
- ✧ UL 749 - The Standard for Safety of Household Dishwashers
- ✧ UL 858 - The Standard for Safety of Household Ranges/Cooktops
- ✧ UL 916 - The Standard for Safety of Energy Management Equipment
- ✧ UL 923 - The Standard for Safety of Microwave Ovens
- ✧ UL 2157 - The Standard for Safety of Electric Clothes Washers
- ✧ UL 2158 - The Standard for Safety of Electric Clothes Dryers

Other Concerns for the Requirements Related to Electrical Safety

- Difference Between an NRTL Approval and an Approval Pursuant to the IECEE CB Scheme:

  The CB Scheme, created by the IECEE (The IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components), simplifies access to numerous markets by avoiding multiple testing. Obtaining the necessary international certifications for market access can be time-consuming and expensive. The CB Scheme enables faster and easier access to global markets. It is a process for mutual recognition of test results among participating countries. As a rule, no additional tests are required. A CB test report from a CB Testing Laboratory (CBTL) and a corresponding CB certificate from a National Certification Body (NCB) will help you meet a wide range of international safety requirements and gaining access to the market in over 50 countries.

The main difference is the regional availability of the two approval systems NRTL and CB Scheme: Products tested by NRTL-approved laboratories are approved for the US and Canadian markets. The CB Scheme, on the other hand, is a multilateral agreement that has emerged from the European Commission for Conformity Testing of Electrical Equipment (CEE). Products with this approval may be traded in the markets of the member states of the IECEE. Now there are more than 50 CB Scheme member countries around the world, including European Union (EU) Member States, the U.S., China, India, Korea and Russia. Manufacturers using the CB Scheme can potentially gain access to every CB Scheme member country without the need for expensive, duplicate testing. Further, CB Scheme applicants are often given priority consideration by NCBs since no additional testing is required.

- The Concern of Battery-operated Device:

  In the IoT era, various types of equipment have got radio device built in, from small handsets, household appliances to the machinery equipment. As per Radio Equipment Directive (RED), the whole product needs to comply with the relevant Electrical Safety standard. Although the LVD only applies from a voltage of 75 V DC, there is no voltage limit as per RED. It means that the battery-operated device, which fall out of voltage limit in LVD, still needs to comply with the safety requirement, and there is no exemption. In view of this, it is recommended to test this kind of battery-operated device in accordance with the LVD anyway.

IOT AND 5G TESTS REQUIREMENT IN RADIO FREQUENCY

Chapter 5 Radio and Wireless Requirement

Right now, the regulation bodies or authorities of many countries have established a lot of regulatory frameworks for placing radio equipment on their market. All radio or wireless equipment that are placed on their market must be compliant with their standards for efficient use of the radio spectrum so as to avoid harmful interference with radio and broadcast communications service. The following radio technologies are required to conduct the testing to ensure to comply with essential requirements. The next section will introduce the global market requirements for the following radio 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. CE mark must be affixed on the Radio and wireless products sold in the European market. It indicates conformity with all applicable requirements when importing and selling in the European market. It is mandatory that the product must comply with the Radio Equipment Directive (RED). The RED has specific transmitter and receiver tests along 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. The manufacturers or suppliers must complete and sign a Declaration of Conformity (DoC) Statement, which lists all the applicable directives and harmonised standards that the product complies with.

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 Federal Communications Commission (FCC). FCC labeling and statement must be affixed on the 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 type of product. The product must also be certified by either the FCC or a designated TCB (Telecommunication Certification Body). The accredited test report and associated technical documentation must be submitted to a FCC designated TCB. A certification will be granted for the product with associated FCC ID number. The FCC's rules and regulations are located in Title 47 of the Code of Federal Regulations (CFR). The following list of standards are applied the above radio technologies.

47 CFR Part 15 - Radio Frequency Devices
47 CFR Part 22 - Public Mobile Services
47 CFR Part 24 - Personal Communications Services

Canada

The Regulator is Innovation, Science and Economic Development (ISED). ISED logo and English/French statement must be affixed to the product. 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 type of product. The radio and wireless devices must be certified by ISED or a designated Foreign Certification Body (FCB). Then, the test report and technical documentation must be submitted to ISED or a designated FCB. A certification will be granted for the product with associated ISED ID number.

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

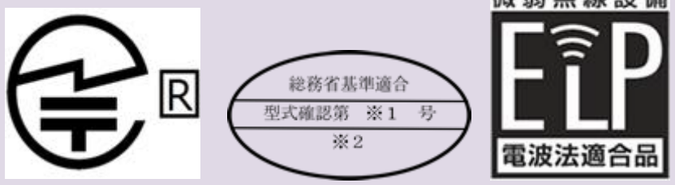
The Regulator is Australian Communications and Media Authority (ACMA). The Regulatory Compliance Mark (RCM) label is the approval scheme of Wireless Devices in Australia, or for suppliers registered under the previous C-tick/A-tick regimes, the C-tick or A-tick label must be affixed to the product. Radio and wireless products sold into the Australian market must be compliant with relevant wireless and standards such as AS/NZS, EN or FCC and must 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) Statement which lists all the applicable RCM standards which the product complies with.

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 Ministry of Internal Affairs and Communications (MIC). The MIC mark scheme is the approval of Radio and Wireless Devices in Japan. The relevant MIC compliance logo must be affixed to the radio and wireless product. Radio and wireless products sold in the Japanese market must comply with relevant MIC regulations in order to comply with JRL (Japanese Radio Law). Certification through a Registered Certification Body (RCB) is required depending on the type of product. The Radio Law's scope covers all products which emit electromagnetic waves with frequencies under 3 THz. The Radio Law requires approvals of not only 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 Registered Certification Body (RCB) such as JQA. The 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: • Bluetooth • Wi-Fi • LTE • GSM • ZigBee • Wireless mics • RFID (2.4 GHz, 920 MHz) • Telemeters • UWB radio systems
High-Frequency Devices	High-Frequency Devices: • 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 @ 3m: • <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 frequency in GHz (or 500uV/m, which is lower) for 10 GHz – 150 GHz

China

SRRC (State Radio Regulation of China) 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). 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 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 and 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 the transmitting equipment must be tested, verified and evaluated, mainly including 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 system
- Dedicated network equipment
- Microwave equipment
- Radio and TV equipment
- Satellite equipment
- 2.4GHz / 5.8GHz wireless LAN equipment
- Short-range wireless equipment
- Radar
- Other radio equipment
- Even if it is not part of the above ten products, if there are similarities with the above products, certification may be required.

5G standards:

Now, the requirements for regulatory tests for devices with 5G technology that the standards for 5G have not yet been finally harmonized. The 3rd Generation Partnership Project (3GPP) is a member-driven standards organizations to develop protocols for mobile telecommunications including 5G NR and related 5G standards. The following standards are developed by 3GGP and ETSI. Most of 5G devices adapted these standards for their compliance requirement now.

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

IOT AND 5G TESTS REQUIREMENT IN RELIABILITY TESTS

Chapter 6 Reliability Testing of IoT Devices

Performance Evaluation on Environmental Stress

Considering that IoT and 5G devices may involve the integration of electronic device(s) to managing important system and infrastructures such as home security system, traffic control system, signaling system, safety system etc., it is not difficult to imagine that the impact of unreliable IoT device will be caused on private and public services. This article is an extensive discussion on the reliability testing methodology for IoT device.

Environmental stress such as extreme temperature dwell, rapid temperature transition, humidity and vibration are the most common and major factors which cause the failure of electronic device. Artificial environments will be subjected to electronic equipment and devices to evaluate the performance of it under conditions of storage, transportation, installation and normal usage. The degree of stress, stress type and duration of the environmental testing is depending on the application of the IoT device and its product specification. There are indeed various types of testing standard which specified for a certain product and there is no existing standard which focus on IoT device in the industry, we will describe a general and widely adoption international standard for the environmental testing standard for electrical, electromechanical and electronic equipment and devices. The international standard aforementioned is “IEC 60068 Environmental Testing” which is published by the International Electrotechnical Commission and covers different aspect of environmental testing.

The following are the commonest field of testing that IoT device will be encountered during its application:

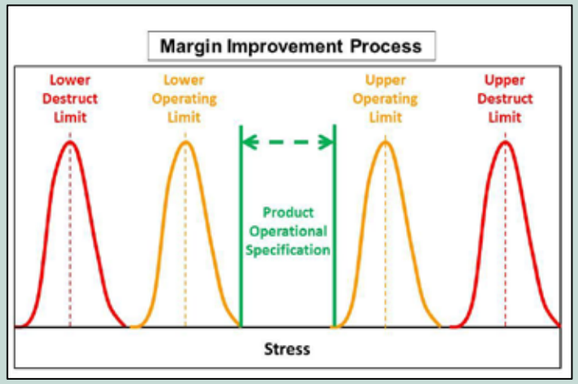
Test Items	Reference Standard	Simulated Stress
Low Temperature	60068-2-1, Part 2-1: Tests — Test A: Cold	Simulate the extreme cold condition with static low temperature stress
High Temperature	60068-2-2 Part 2-2: Tests — Test B: Dry heat	Simulate the extreme hot condition with static low temperature stress
Static Temp-Humidity	60068-2-2 Part 2-2: Tests — Test B: Dry heat	Simulate the high humidity condition with static humidity and temperature stress

Damp Heat Cyclic	60068-2-30, Part 2-30: Tests — Test Db: Damp heat, cyclic	Simulate the change of humidity and temperature condition with a 24 hours + 24 hours humidity and temperature cyclic stress
Thermal Cycling	60068-2-14, Part 2-14: Tests — Test N: Change of temperature	Simulate the change of temperature on electronics aspect (e.g., PCB and components level) with controlled temperature transition rate, e.g., 10-15 degree Celsius per minute. The test will perform using climatic chamber.
Thermal Shock	60068-2-14, Part 2-14: Tests — Test N: Change of temperature	Simulate the change of temperature on mechanical aspect (e.g., micro-crack on solder joint and component) with high temperature transition rate, e.g., <10 seconds. The test will perform using thermal shock chamber with separate heating and cooling zones.
Sine Vibration	60068-2-6, Part 2-6: Tests — Test Fc: Vibration (sinusoidal)	Simulate the vibration stress of sinusoidal wave patterning, e.g., the vibration stress during transportation
Shock Test	60068-2-6, Part 2-6: Tests — Test Fc: Vibration (sinusoidal)	Simulate the vibration stress of suddenly shocking with positive and negative pulse, e.g., the vibration stress if the product is drop down or have a sudden mechanical impact
Random Vibration	60068-2-64, Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance	Simulate the vibration stress in random magnitude and frequency with preset frequency and magnitude range, e.g., the vibration stress during normal usage

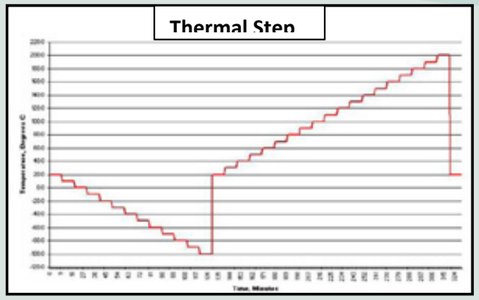
Reliability Assessment (Qualitative)

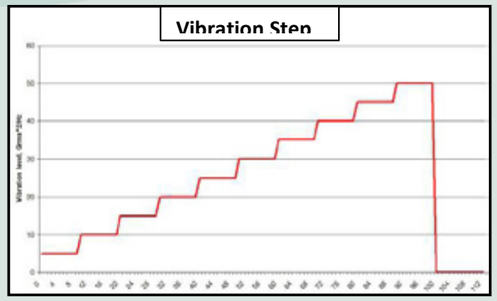
During the development stage of IoT device, product failure will normally only be revealed in months and even year and the turnaround time is too long for product improvement. Hence, we need to look up some approach to expedite the product failure cycle and reveal the product failure in a shorter turnaround time in order to improve the product. There are two major categories of reliability improvement methodology in the industry. Namely, Qualitative Accelerated Life Testing and Quantitative Accelerated Life Testing. While quantitative testing concerns mostly about the product's life time in a numerical sense, such as B10 life, qualitative testing is used to identify failures and failure modes without making any predictions as to the product's life under normal conditions.

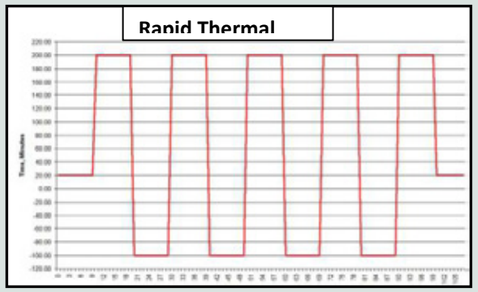
For the qualitative approach, we would like to introduce the Highly Accelerated Life Test (HALT), which could refer to IPC 9592A or Qualmark HALT Testing Guidelines Rev.04, document: 933-0336. In HALT analysis, a product is subjected to certain stimuli well beyond its expected operating conditions to determine its operating and destruction limits. The failure modes found from these exaggerated conditions could often reflect precisely the actual failure when it is subjected to normal operating environment. With the failure modes found, product development engineers could review the selection of components, design of circuit and mechanical structures and make improvements. After a reconfirmation testing process, the engineers could then find solid proof that the reliability performance or the product is soundly improved. This results in a reduced number of field returns and realizing long-term savings.

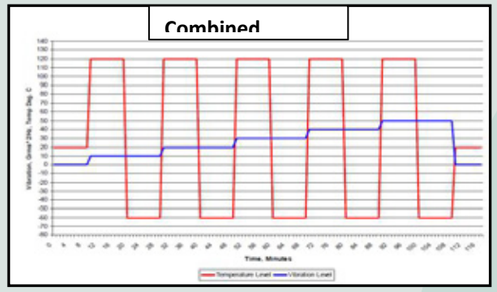


The test procedure of HALT analysis includes (i) Cold Step Stress (ii) Hot Step Stress (iii) Rapid Thermal Transition (iv) Vibration Step Stress (v) Combined Environment. During the test, functional test is required to perform after each step completed the dwell period in order to check the condition of the product. The operating limit is the last stress level that the product still fully functions and will resume normally after the stress removed. The destruct limit is the stress level that the product could not resume its normal function after the stress removed. The engineer could get back the product for offline investigation after reach the destruct limit.









Reliability Assessment (Quantitative)

For the quantitative approach, it involved testing with elevated stress (e.g., temperature and humidity) over time and estimate the product life in a numerical approach with suitable accelerated model (e.g., Arrhenius model).

Before conducting the life time assessment, we should define the failure criteria of the product and determine the best approach to check its functionality. Normally, there should be various failure mode that could descript the functionality of the product (which could reveal through performing HALT test as mentioned in the above paragraph) and we need to identity the most critical failure of the product and setup a measurable passing criterion (e.g. voltage output with acceptable range). During the life test, the IoT device is suggested to be in full functioning to simulate its normal usage in order to obtain a more trustable life time estimation. At least three different sets of data are suggested to perform in different elevated stress and at least 3 to 5 individual products are suggested to be involved in each set of experiment in order to get enough data for the life assessment. With enough data on describing the distribution of the product life cycle (e.g., Weibull Distribution) in different stress level, we could project the product life cycle at the normal usage condition of the product and estimate the life of the product, which usually in terms of Mean Time between Failure (MTBF), Mean Time to Failure (MTTF) and Reliability at time R(t) etc.

The following are some steps recommended for life assessment:

1. *Life test design and planning*
2. *Elevated stress, e.g. temperature, humidity etc.*
3. *Tailor-made functional checking on the performance of the sample*
4. *Apply Accelerated Life Model to estimate the life*

PRACTICAL INTERPRETATIONS AND CASES SHARING FOR 5G/ IOT PRODUCTS

Chapter 7 - Practical interpretations and cases sharing for 5G/IoT products

In this chapter, the practical interpretations for 5G & IoT products about test objectives, test set-ups, test parameters, test methods, performance criteria and test results will be introduced.

Three typical types of 5G and IoT products i.e., Smart Living & IoT, Smart Mobility and Smart Wearable are selected to provide 10 individual cases sharing for 5G / IoT devices from product markets (i.e., Router, Smart Plug, Lighting control device, Wireless IP camera, Wireless sensor, Drone, Scooter, Mobile phone, Smart watch and Tablet) for practical interpretations. Before providing the recommendation, advice and precaution to enhance the 5G & IoT product design solutions on the basis of testing requirement in this chapter, the introduction of Electromagnetic Compatibility (EMC) Test and Radio Frequency Test are briefed to understand the recommendation, advice and precaution easily.

Part A - Electromagnetic Compatibility (EMC) Test

In general, EMC test can be grouped into two types: Emission test and Immunity test.

- Emission test – 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 test is to ensure that any disturbance from the electronic device is below the relevant limits defined for that type of device. It provides a reasonable assurance that the device will not cause harmful interference to other devices operating within its expected operating environment.
- Immunity test – To measure how an electronic device will react and withstand when they are under the exposure of electromagnetic and other disturbances. The purpose of these tests is to gain a reasonable assurance that the device will operate as intended when used within its expected operating environment.

Emission test

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

Measuring equipment:

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

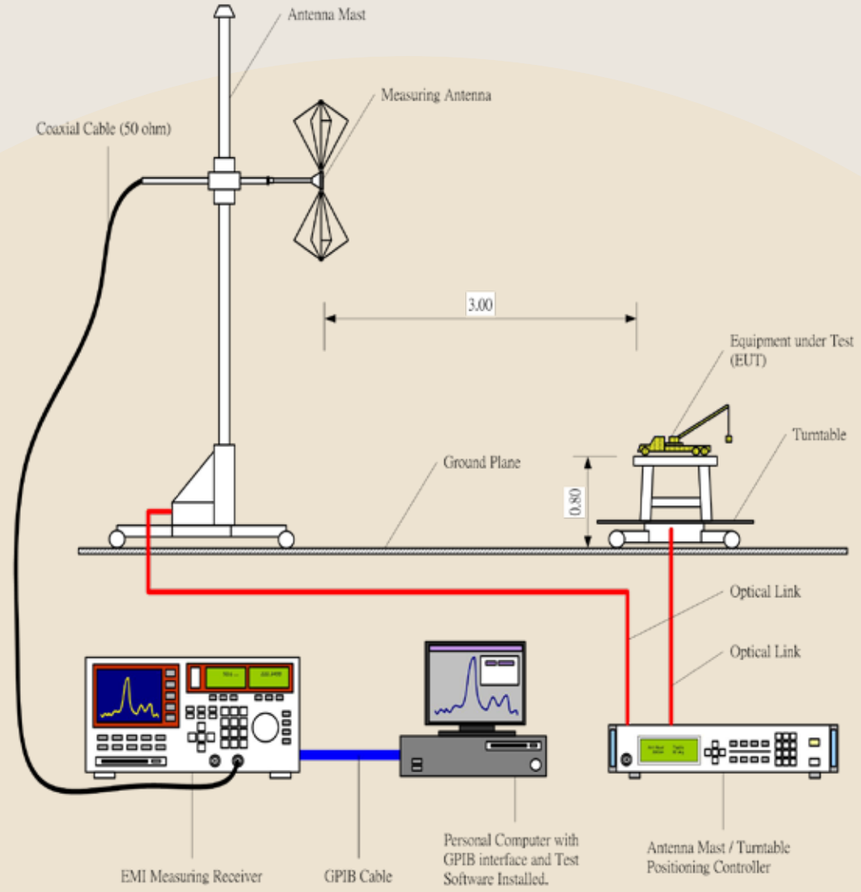
Antennas:

- 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., 10m 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. Like radiated emissions, the allowable conducted emissions from electronic devices are controlled by different regulatory agencies and testing is performed to ensure emission levels are below the applicable limits.

Test environment:

- Reference ground plane or sufficient large area
- Artificial mains networks (AMN) and / or impedance stabilization 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

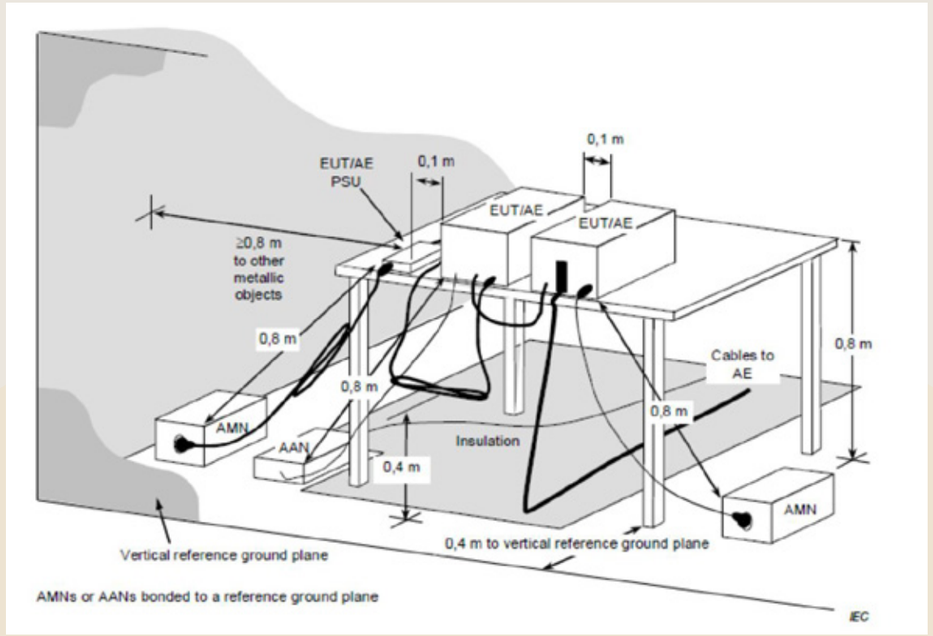
Transducers:

- (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 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 the neutral current overload that affecting transmission capacity. In addition, the phase control of the power supply causes changes in the current of the power grid that causes the voltage on the load side to fluctuate, as a result of causing the lights to flicker.

Therefore, it needs to measure harmonic distortion current and voltage fluctuations and flicker generated by the electronic device assess compliance of the product's EMC standards

Measuring equipment:

- Harmonics analysing system and test software

Measurands:

- Voltage and current changes through the analysing system

Immunity test

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.

Port under test:

- Public network or ports vulnerable to picking up RF signals

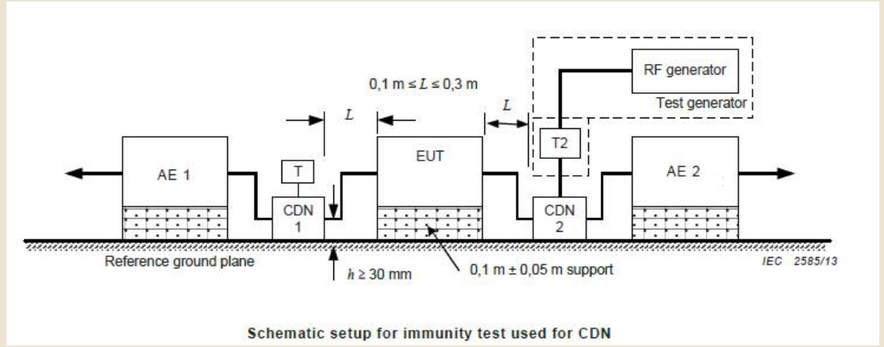
Test equipment:

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:



Schematic setup for immunity test used for CDN

Radiated RF immunity (IEC 61000-4-3)

Objective:

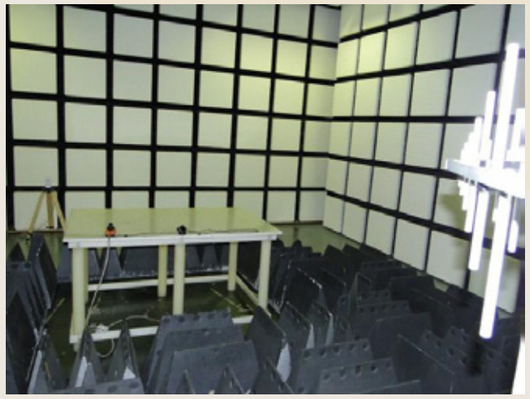
To evaluate the immunity of electrical and electronic equipment exposed to radiated, RF electromagnetic fields.

Port under test:

- Enclosure port

Test environment:

- Absorber lined shielded enclosure (ALSE), Fully-Anechoic Chamber (FAC) or its alternative sites



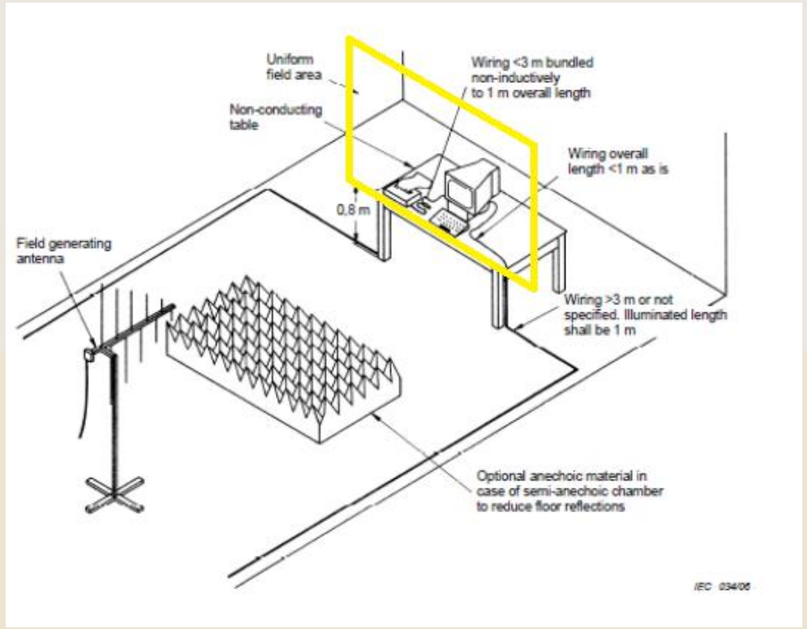
Test equipment:

RF Immunity test systems (signal generator, amplifier, antenna, field sensor, power meter)

Test Method:

- Coupled with linearly polarized antennas (Vertical and Horizontal polarization)
- 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:



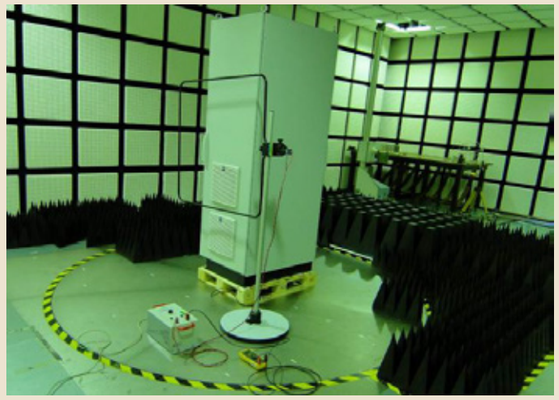
Power frequency magnetic field (IEC 61000-4-8)

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:

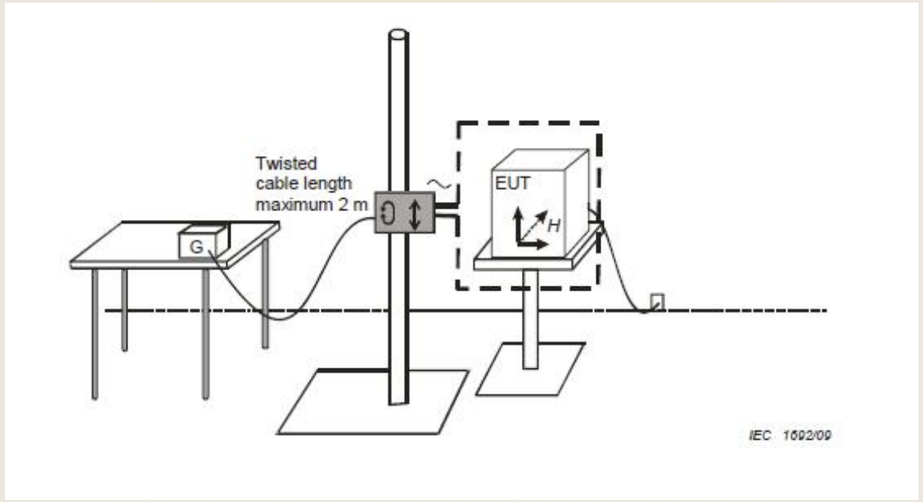
- Enclosure port



Test level:

- 3 A/m or 30 A/m: Continuous filed
- 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. In addition, it includes electrostatic discharges which may occur from personnel to objects near vital equipment.

Port under test:

- Enclosure port

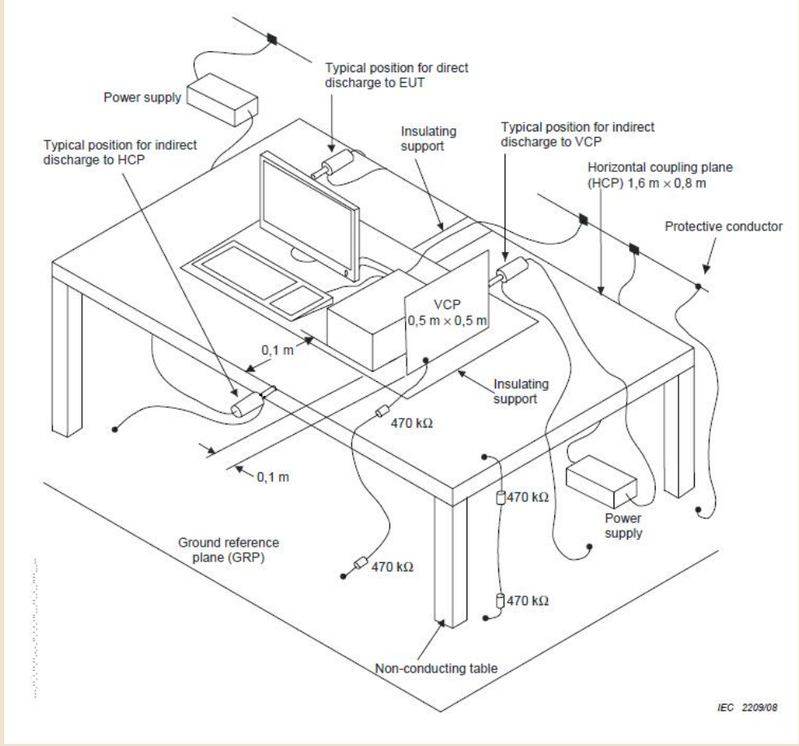
Phenomena:

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

Test method

- 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 generated by switching of small inductive loads, relay contacts bouncing (conducted interference) and switching of HV-switchgear (radiated interferences).

Port under test:

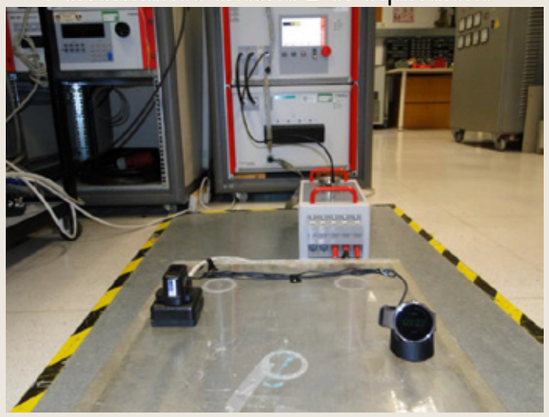
- Power supply, signal, control and earth ports

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 energies of several joules by switching (of capacitor bank) in the power network, Faults in the power network and lightning strokes (direct or indirect)

Port under test:

- AC mains and public telecom networks

Test signal:

- 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 & interrupts are caused by faults in the power network, the installation or by sudden large change of load, while voltage variations are caused by continuous varying loads connected to the power network.

Port under test:

- AC mains

Special requirement of test equipment:

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

Part B – Radio Frequency Test

In general, Radio Frequency Test can be grouped into two types: Transmitter test and Receiver test.

- Transmitter test – To measure the parameters of transmitter. In most standards, the test of the RF output power and unwanted emissions in the spurious domain are the popular test items for the transmitter. Other test items such as permitted range of operating frequencies, occupied channel bandwidth, power spectral density and so on are not available to apply for all type of wireless technologies and operating frequency ranges. The purpose of transmitter test is to ensure that output RF power, spurious emission and other essential parameters are under control by the law and regulations and fulfil the requirements of the stated measurements. No disturbance from the wireless device are below the relevant limits defined for that type of device. It provides a reasonable assurance that the device will not cause harmful interference to other devices operating within its expected operating environment.

- Receiver test – To measure the parameter of receiver. The test of the receiver spurious emissions is the popular test items for the receiver. Besides, how the receiver will react and withstand when they are under the exposure of transmitter interferences and low receive sensitivity are also essential test items for the receiver. The purpose of these tests is to gain a reasonable assurance that the wireless device will operate normally and receive the RF signal as intended when used within its expected operating environment.

Standards:

Right now, two institutes are responsible to develop the measurement methods of RF measurement in the world. One is ETSI (European Telecommunications Standards Institute) and the other is ANSI (American National Standards Institute).

General speaking, ETSI is a European Standards Organization (ESO). We are the recognized 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

recognized as European Standards (ENs). Therefore, ETSI standards are used for wireless and RF measurement in Europe.

ANSI (American National Standards Institute) is a private, non-profit organization 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 America.

In Chapter 3, we introduced many standards for RF and wireless measurements. The measurement procedures of most of them are followed the standards ETSI and ANSI. For example, the measurement procedures of the standards for Europe are used ETSI and US and Canada are used ANSI. The main difference between ETSI and ANSI is that the ETSI have more test requirements and test items for the transmitter and receiver and ANSI is more focus on the transmitter, only few test requirements and test items for the receiver. Besides, the measurement unit is the difference between ETSI and ANSI in some test items.

Transmitter test:

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 meter or spectrum analyser

Test method:

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

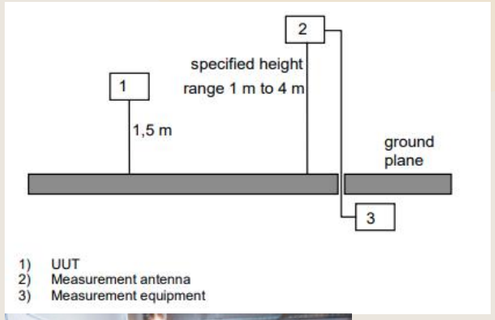
Measurement unit:

- Conducted measurement: dBm in ETSI and ANSI
- Radiated measurement: dBμV/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 are 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 Antenna port
- Radiated measurement for integral antenna equipment (without antenna connectors)

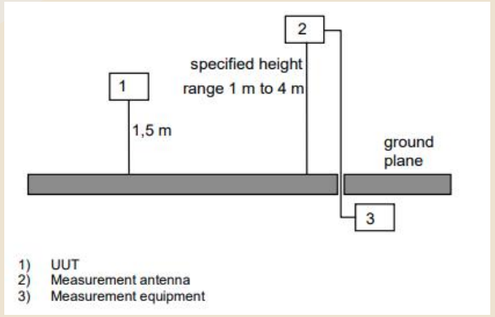
Measurement unit:

- Conducted measurement: dBm in ANSI and ETSI
- Radiated measurement: dBµV/m in ANSI and dBm in ETSI

Test setup:

- Conducted measurement:

- Radiated measurement:



Receiver test

Receiver spurious emissions (ETSI)

Objective:

To measure Receiver spurious emissions are emissions at any frequency when the equipment is in receive mode.

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 Antenna port
- Radiated measurement for integral antenna equipment (without antenna connectors)

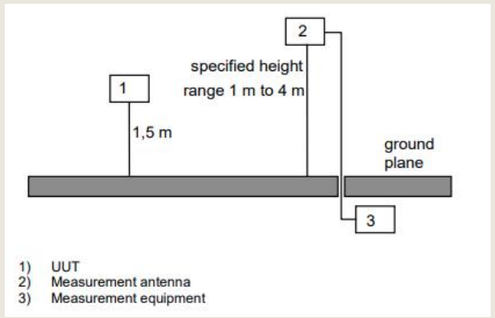
Measurement unit:

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

Test setup:

- Conducted measurement:

- Radiated measurement:



Part C - Cases Sharing

Cases sharing for 10 individual 5G / IoT devices (i.e. Router, Smart Plug, Lighting control device, Wireless IP camera, Wireless sensor, Drone, Scooter, Mobile phone, Smart watch and Tablet) will be briefed in this section.

Router

- Typically, most of electromagnetic radiation are leaking from the long cables from the LAN or WLAN router as an antenna. For example, a high data rate (i.e., above 1Gb/s) on the long-wired Ethernet cables connected to router will generate higher radiated emission of the fundamental frequency of the Ethernet data rate and plus harmonics. The twisted pairs and shielded cables with ferrite chokes can reduce the radiated emission of the differential mode noise and common mode noise.

Smart Plug and Lighting control device

- Most of the smart plugs and lighting control devices now not only have LAN connection but also wireless connections such as WIFI or Bluetooth to let us easily to control our electrical and electronic products through the internet. The smart plug always needs to connect to AC main power and wireless network. Many EMC problems occurred during immunity test and surge test. For example, the network of Smart Plug and Lighting control device is interrupted and reset suddenly. Therefore, it is common that an EMI filter and surge arrester are added in the devices to suppress EM noise high-energy pulse and prevent the damage of the device from high-energy surge pulse.

Wireless IP camera and sensor

- The main challenge for the wireless IP camera and sensor is Radio Frequency Test. In order to have a stable networking, high video quality and strong receiving sensitivity, the engineer may tune higher of RF output of the devices and the bias of pre-amplifier to ensure the transmitted and received signal strength is strong enough. Consequently, it may cause the saturation of front-end low noise amplifier circuit and cause even order harmonic distortion. The transmitter and receiver unwanted emissions in the spurious domain will happen and the spurious level may exceed the limit of the standards. A filter may add before the low noise amplifier or reduce the level of RF output to optimise the RF performance of IP camera is one of solution to improve this problem.

Drone and Scooter

- The main issue of the drone and scooter is EMC problem. It is common to fail the radiated emission and immunity test due to EM noise from DC motors and high sensitivity of its driver circuits of the drone and scooter. Therefore, a special concern is needed to select brushless DC motors, which fulfil EMC emission and immunity standards. Also, it should be more careful when considering designs of the driver circuits such as electronic speed control circuit, DC to DC circuit and data transmission circuit. A suitable EMI shielding is a possible solution to improve the EMC issue. It can prevent electromagnetic interference or radio frequency interference from impacting high sensitivity of its driver circuits of the drone and scooter. The metallic screen can absorb the electromagnetic interference that is being transmitted through the air.

Mobile phone, Smart watch and Tablet

- The main challenge for the Mobile phone, Smart watch and Tablet is Radio Frequency Test and Reliability Test. In order to have a good user experience and good product's performance, the R&D engineer may face challenges to ensure a stable wireless performance and higher reliability on environmental stress. As a result, a stable wireless performance may cause the saturation of front-end low noise amplifier circuit or cause weak receiver sensitivity. A pre-amplifier may be added after the receiving antenna is one of solution to improve this problem. Besides, the environmental testing can enhance the performance of the IoT devices and its associate accessories. The test can evaluate the performance of it under conditions of storage, transportation, installation and normal usage.