

Internet of Things (IoT) Pocket Guide



ROHDE & SCHWARZ

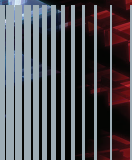


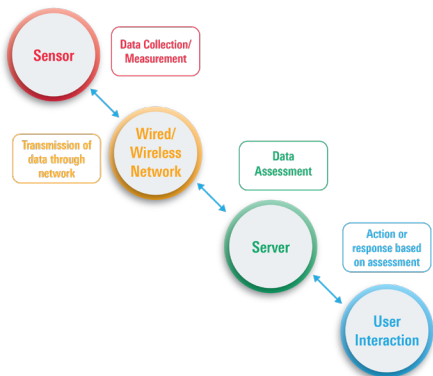
Table of Contents

Overview	3
What is the IoT Opportunity?	3
Technology Overview	9
What to Consider	13
Technologies	14
Wireless PAN/LAN - Bluetooth, WiFi	14
LR-WPAN - ZigBee, Thread,...	24
LP-WAN - SIGFox, LoRa	29
Wireless WAN - 4G, 5G, NB-IoT	34
Design and Testing	48
Testing life cycle	48
Over-the-Air (OTA)	55
Coexistence Testing	62
Power Consumption	71
Security of IoT Devices	75
Manufacturing	78
Device Certification	82
Design Strategy	82
Certification Bodies	85
Certification Process	95
Solutions	100
Testing solutions through the Life Cycle	100

What is the Internet Of Things, or IoT?

According to Wikipedia....

The Internet of things is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.

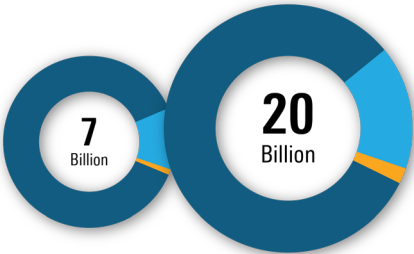


IoT will impact everyday life by connecting many things to the Internet

IoT will impact all industries and ultimately everyone's daily life. Currently, things such as containers, street lights, trash cans, trees and cows are already connected to the Internet. Many new markets are evolving, such as smart homes, connected cars, smart grids and smart healthcare; we can only imagine what will be connected in the near future.



By 2023: ~20 Billion Connected IoT Devices

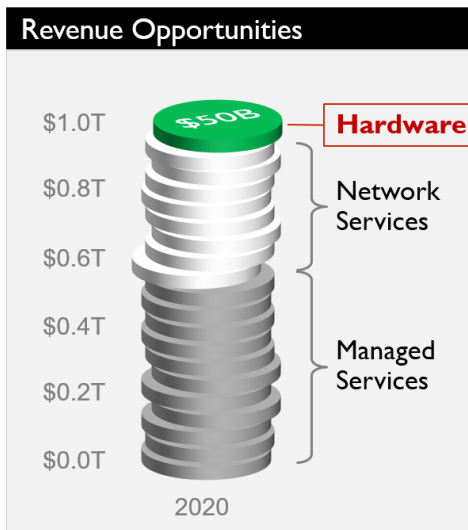


	2017	2023	CAGR
Short-range	6.2 Bn	15.7 Bn	+ 17 %
Cellular WAN	0.7 Bn	3.5 Bn	+ 30 %
Unlicensed WAN	0.1 Bn	0.6 Bn	+ 35 %

"Of the 3.5 billion cellular IoT connections forecast for 2023, North East Asia is anticipated to account for 2.2 billion. VoLTE support in Cat-M1-capable Internet of Things (IoT) chipsets, devices and network infrastructure is starting to be commercialized, and new use cases are being explored."

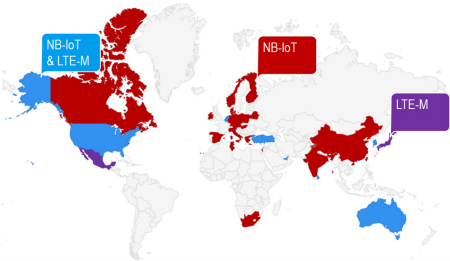
- Source: Ericsson Mobility Report June 2018

Communication Modules are just an enabler of the IoT



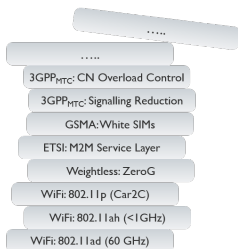
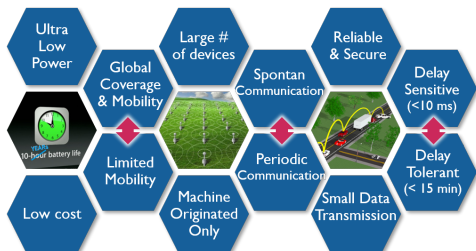
Source: Habor Research IoT market forecast
<https://s3.amazonaws.com/postscapes/loT-Habor-Postscapes-Infographic.pdf>

48 Mobile IoT Commercial Networks are launched.
Another 50 networks are under planning.

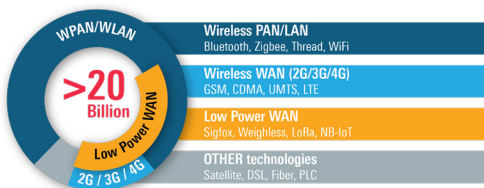


March 2018	
 AT&T	 中国移动 China Mobile
 中国电信 China Telecom	 China unicom中国联通
	 Dialog
 LG U+	 kt korea telecom
 verizon	 vodafone
 m1	 TELSTRA
 TURKCELL	 velcom

A diverse range of IoT deployment requirements

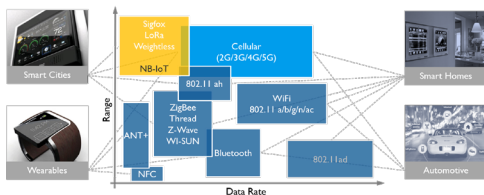


What are the key IoT communication technologies connecting billions of devices?



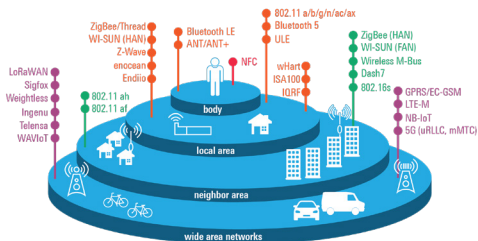
At the present time, there are already billions of devices connected to the Internet by quite, mature wireless technologies like Bluetooth, ZigBee, WiFi, or cellular technologies of the 2nd and 3rd generation. Due to the growing demand for low cost connectivity, the IoT industry is developing and deploying multiple new technologies that are optimized for this specific need.

The majority of IoT devices will use wireless technologies in un-licensed frequency bands



Some applications that require global coverage and/or mobility will use cellular technologies, but the majority of IoT devices will use non-cellular technologies' sharing frequencies in unlicensed bands to communicate with each other and with IoT applications in the cloud.

Technologies versus deployment range



The expectations on reliability, performance, quality of experience and longtime availability are extremely high and connectivity is a critical success factor. However, IoT applications have a wide variety of requirements depending on their end use. This may include data rates, range, power usage, frequency of communication and more.

Many technologies are being implemented and considered for IoT applications

ANT+

Bluetooth (Multiple versions)

C-V2X (Vehicle comms)

EC-GPRS

EnOcean

HaLow (Wi-Fi version 802.11ah)

Ingenu

ISA 100.11a

LoRaWAN

LTE MTC Cat 0 (cellular)

LTE eMTC Cat M (cellular)

MiWi

NB-IoT

NFC (Near Field Comms)

Positive Train Control

Sigfox

Telensa

Thread

WAVE (802.11p or DSRC)

Weightless (N, P, W)

White Space (802.11af)

Wi-SUN

Wi-Fi (Multiple versions)

WiGig (802.11ad)

WiMAX

WirelessHART

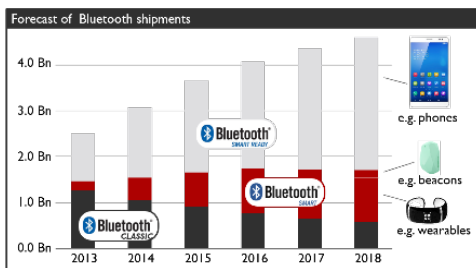
ZigBee

Z-Wave

Considerations for determining which technology best fits your application

1. What is the maximum range of a link?
2. What is the maximum data rate used in the application?
3. Is power consumption an issue?
4. What is the frequency band of operation?
5. How many nodes are to be used? Is a large network needed?
6. What other wireless services/devices are nearby that could cause interference?
7. Are licensing and certification required to use the standard?
8. Are chips and/or modules available from multiple vendors?
9. Are related connections such as cellular services needed?
10. Are reference designs, development kits, and other design support available?
11. Is your application unique? Maybe you do need to create your own standard with RF in one of the ISM bands with a protocol optimized for your use cases.
12. How big a factor is cost to develop, deploy, and maintain?

Bluetooth Smart will dominate the IoT market for wearables, while trying to address the smart home market



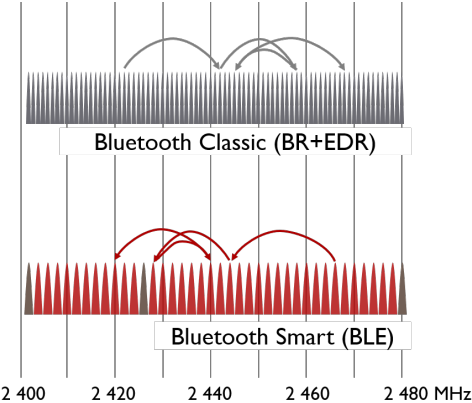
Source: ABI Research

While the power-efficiency of Bluetooth Smart makes it perfect for devices needing to run off a tiny battery for long periods, the magic of Bluetooth Smart is its ability to work with smartphones or tablets. Smart Mesh enables smart locks, lights, HVAC systems, and even appliances work together to deliver a seamless smart home.

Bluetooth SIG releases IoT enhancements

<p>Mesh</p> <p>building meshed network using relay nodes</p>		<p>Speed</p> <p>100% improvement for low latency applications</p>
	<p>Range</p>	
	<p>Gateway</p> <p>Connecting devices directly to the cloud</p>	
<p>Direction</p> <p>Extended capabilities of beacons for positioning</p>		

Bluetooth Classic and Bluetooth Smart



To avoid interference with other devices, there are 79 1 MHz channels in Classic Bluetooth, which hop at a rate of 1600 hops per second. The hopping algorithm excludes channels that have high interference. Bluetooth Smart has 40 2-MHz channels, including three fixed advertising channels.

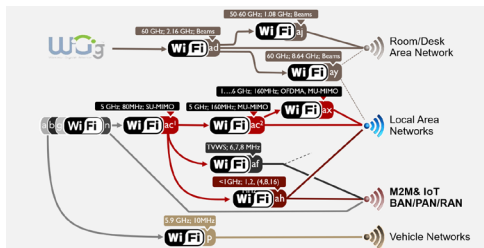
Bluetooth Classic and Bluetooth Smart

- 2.4 GHz ISM band
- 1 Msymbol/s using GFSK modulation
EDR: Data modulation $\pi/4$ -DQPSK / 8DPSK
- 79 Channels on 1 MHz spacing
- Frequency Hopping (1600 hops/s)
- Voice support
- FEC

- 2.4 GHz ISM band
- 1 Msymbol/s using GFSK modulation
- 40 Channels on 2 MHz spacing
- 3 advertising channel
- Frequency Hopping (37 channel)
- CRC



Wi-Fi adoption beyond Local Area Networks



WiFi is the leading wireless technology for local area networks. The standards body is defining new capabilities to support the demand for long range and low power operations for IoT and M2M communications markets. These new WiFi technologies offer different approaches to WiFi that could enable some entirely new device classes.

Wi-Fi is used for several IoT applications, especially in smart home and smart office environments today

	802.11a	802.11b	802.11g	802.11n	802.11ac
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5GHz	5 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20 MHz, 40 MHz	20/40/80/160 MHz,
Spatial streams	1	1	1	4	8
Max. Data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1331 Mbps
System	OFDM	DSSS	OFDM, DSSS	OFDM, OFDMA	MIMO-OFDM,

The initial launch of the 802.11 WiFi standard was in 1997. In addition to speed improvements, 802.11n introduced the first optional use of the 5GHz band, offering a less cluttered frequency band. 802.11n also introduced the first use of MIMO antennas for higher parallel throughput. The newer 802.11ac standard was designed to dramatically increase the speed of data transfers. This is the first standard to offer speeds that can reach 1 Gbit/s and it runs solely on the less cluttered 5 GHz band.

Wi-Fi HaLow

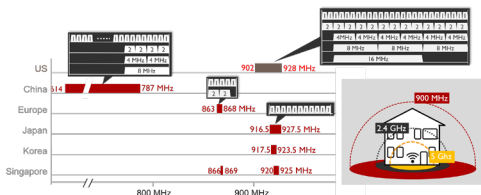
Long range operation	Low power consumption	Large number of devices per access point	High throughput compared to e.g. ZigBee	Greenfield operation
Sensor Networks	Home Security	Wearables	Range extension	Smart Metering
				

The 802.11ah standard, known as HaLow, was developed as a lower power WiFi solution and is designed to cover a range of up to 1 kilometer. HaLow will enable a variety of new power-efficient use cases in the smart home, connected car, digital healthcare, as well as industrial, retail, agriculture, and smart city environments.

Wi-Fi HaLow

Operates in sub 1 GHz license-exempt band

Support of 1 & 2 MHz channels is mandatory



HaLow achieves the greater coverage by transmitting at 900 MHz. It supports multiple channel bandwidths from 16 MHz channels, for high data throughput, down to 1 MHz, for extended coverage at lower data rate.

At these long ranges HaLow will only be able to transmit data at speeds between 100 Kbit/s and 40 Mbit/s, making it slower than most existing home networks.

Wi-Fi HaLow

802.11ah in a nutshell

scalable - long range - low power network

802.11ah PHY Layer

- Operates in sub 1 GHz license-exempt bands
- Essentially 10-times down-clocked version of 802.11ac (max. data rate 340 Mbps)
- Defines 2 MHz, 4 MHz, 8 MHz, and 16 MHz channels and a 1 MHz channel for extended coverage
- For ≥ 2 MHz modes, the PHY layer is exactly designed based on 10 times down-clocking of 802.11ac's PHY layer: techniques like OFDM, MIMO, DL MU-MIMO, MCSs have been adopted
- 1 MHz channel supports additional scheme for extend transmission range by 2x symbol repetition (MCS10)

Wi-Fi HaLow

802.11ah in a nutshell










scalable - long range - low power network

802.11ah MAC Layer

- Support large number of stations (8191) by introducing a hierarchical AID structure
- Power saving mode optimized for a large number of stations in power saving mode
- Improved channel access mechanisms by introducing Target Wakeup Times (TWT) and restricted access windows (RAW)
- Throughput enhancements by reducing protocol overhead

LR-WPAN

For smart home, smart buildings and more

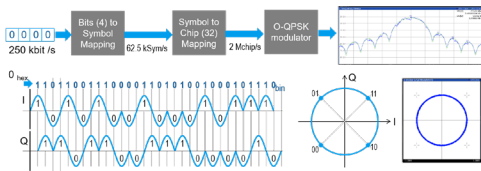
				
ZigBee - Protocol	Protocol (e.g. CoAP)	ISA Protocol	HART: Protocol	
ZigBee - Transport	UDP/TCP	UDP	HART: TCP like	
ZigBee - Networking	6LoWPAN, DTLS, Distance Vector Routing	6LoWPAN	HART Addressing/Routing	
802.15.4 MAC	802.15.4 MAC	Upper data link ISA100 802.15.4 MAC	HART TDMA - hopping	
IEEE 802.15.4 2.4 GHz + O-QPSK	IEEE 802.15.4 2.4 GHz + O-QPSK	IEEE 802.15.4 2.4 GHz + O-QPSK	IEEE 802.15.4 2.4 GHz + O-QPSK	
				

802.15.4 is one of the more successful standards for low data rate wireless personal area networks (LR-WPANs.) 802.15.4 was developed for low-cost, low-speed communications between devices at a limited range (10-30m) and a maximum data rate of 250 kbps. This physical layer technology is ideal for low data rates, low complexity and long battery life applications, such as industrial and commercial sensors and actuator devices.

802.15.4: 2.4 GHz ISM Band

◆ 16 Channels ◆ O-QPSK ◆

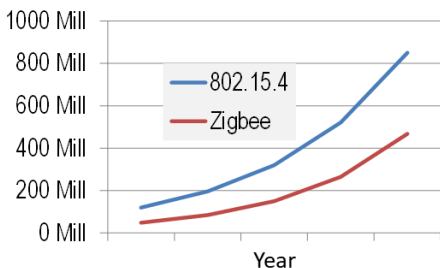
250kbps



802.15.4 operates in the unlicensed spectrum depending on the country: 1 channel in the 868MHz band for Europe, 10 channels in the 915MHz ISM band for North America and 16 channels in the 2.4 MHz ISM band worldwide. It defines the channel bandwidth at 5MHz and at the 2.4GHz ISM band, 802.15.4 specifies the use of Direct Sequence Spread Spectrum and uses the Offset Quadrature Phase Shift (O-QPSK) modulation scheme.

IEEE 802.15.4 - used in Home Area Networks (esp. Smart Metering & Home Control)

60% CAGR annual chip shipment



ZigBee

6LoWPAN

Wireless
HART

JenNet

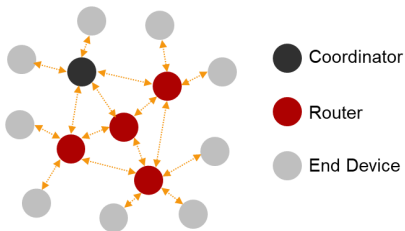
802.15.4 (L1/L2)

ZigBee Technology Facts

Reliable, Low Power, Cost
Effective

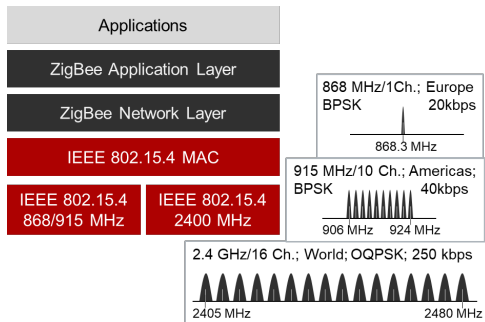


Meshed Network of thousands of devices



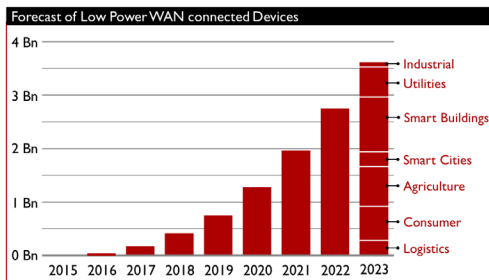
ZigBee Technology Facts

Reliable, Low Power, Cost
Effective



Low Power Wide Area Networks:

Low cost, battery powered devices and strong propagation



Source: Analysis Mason 2015



SIGFOX
One network A billion dreams



The SIX L's characterizing LP-WANs

10-dollar devices capable of 10 km range with 10-year battery lifetime



Low Power

Battery powered devices requiring 10+ years lifetime



Low Cost

Communication modules for 5 dollars and even less



Long Range

Covering large areas with low number of base stations



Large Scale

Several thousands of devices per gateway or base station



Low Throughput

From 100 bps to some few kbps: short message once per hour/day/week...



Low Responsiveness

Relaxed requirements regarding responsiveness of a device

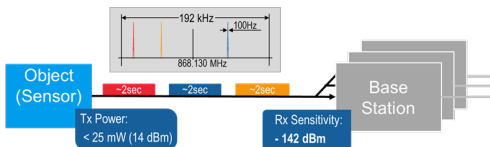
LP-WAN (unlicensed)

The new kids on the block

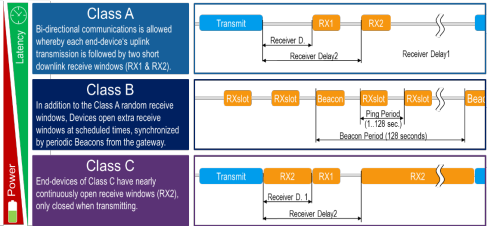


	Sigfox	LoRa	Weightless-N	RPMA
Frequency Bands	868 MHz (ETSI) 915 MHz (FCC) 2 400 MHz	868 MHz (ETSI) 915 MHz (FCC)	868 MHz (ETSI) 915 MHz (FCC)	2 400 MHz
Technology	Ultra Narrow Band DBPSK/2GSK	FM chirped spread spectrum	Ultra Narrow Band DBPSK	Random Phase Multiple Access
Single channel	100 Hz/ 600 Hz	125/250/500 kHz	200 Hz	1 MHz
Driver	Sigfox	Semtech	nWave	Ingenu
Signal Range	621 miles	12.4 miles	2KM	300 square miles
Data Rates (UL/DL)	100bps	50Kpbs	~2.5kbps – 16Mbps	624 kbit/s / 156 kbits/s

SIGFOX



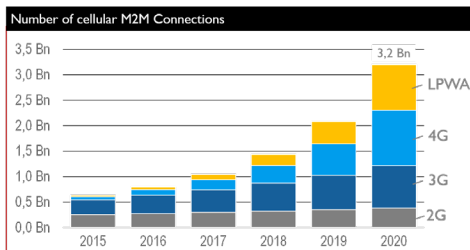
The SIGFOX technology is aimed at low cost machine-to-machine application areas, where wide area coverage is required. SIGFOX uses the 915GHz ISM band in the US, with its patented Ultra Narrow Band (UNB) technology. UNB enables very low transmitter power levels to be used while still being able to maintain a robust data connection. With the SIGFOX protocol, the device is only allowed to receive data just after a packet is transmitted, otherwise the device receiver is turned off in order to conserve battery life.



One of the major advantages of LoRa is the technology's long range capability. A single LoRa gateway or base station is capable of covering an entire city or hundreds of square kilometers, however this highly depends on the environment or obstruction in a given location. As with SIGFOX, LoRa operates in the 915 MHz ISM band in the US and also has a physical layer developed by Semtec. The physical layer uses a proprietary chirp spread spectrum modulation technique where the frequency increases or decreases over a certain amount of time to encode information.

Wireless WAN (3G/4G/5G)

Long-term availability with LTE-M & NB-IOT

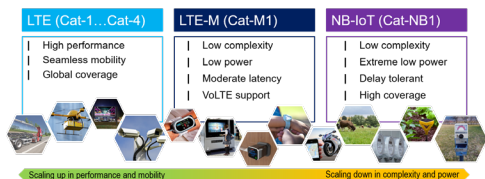


Source Cisco VNI Mobile 2016

- Cellular M2M connectivity still dominated by 2/3G technologies
- Increasing global 4G coverage makes LTE to an attractive alternative to 2G/3G especially considering the long term perspective of 2G networks.
- Availability of M2M optimized LTE only chipsets
- LTE-M and NB-IOT opens opportunities in new markets

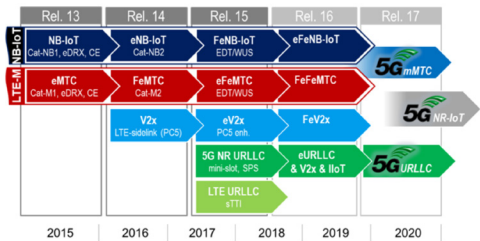
Where are we today?

3GPP Cellular IoT addresses the IoT/LPWAN market with LTE-M and NB-IoT



3GPP has been working on new requirements to support Machine Type Communications (MTC) for LTE. The goal for these new 3GPP MTC requirements is to provide cost effective connectivity to billions of IoT/M2M devices which require very low power consumption and excellent coverage.

Evolution of Cellular IoT (C-IoT)



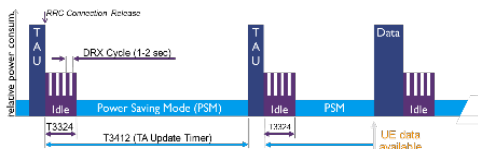
Rel. 12: New Category 0

- For low complexity UEs

	Cat 1 (Rel-8)	Cat-0 (Rel-12)
Downlink Peak Rate	10 Mbps	1 Mbps
Uplink Peak Rate	5 Mbps	1 Mbps
UE RF Chains	2	1
Duplex Mode	Full duplex	Half duplex (opt)
UE Receiver bandwidth	20 MHz	20 MHz
Max UE Transmit Power	23 dBm	23 dBm
# soft channel bits	250 368	25 344
max TBS for PMCH	10 296	4 584
MIMO Layer	1	1
Highest DL Modulation	64QAM	64QAM
Highest UL Modulation	16QAM	16QAM

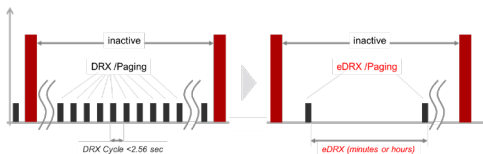
Rel. 12: Power saving mode for UE that can accept long latency for terminating data

PSM Mode: UE remains registered with the network and there is **no need to re-attach or re-establish PDN connections** – saves power, but UE isn't reachable in PSM Mode



UE request an Active Time value (T3324) during every Attach / TAU Request. Network confirms usage of PSM by allocating an Active Time value to the UE

Rel. 13: Enabling extended battery life, reduced data transmission to a minimum (I-eDRX)



For devices with infrequent uplink data transmission, energy consumption can be reduced significantly by longer cycles for discontinuous reception (DRX).

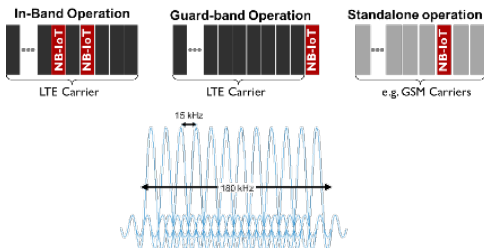
Rel. 13: NB-IoT - even more 'streamlined' than cat-M1



Objectives

- Improved indoor coverage: extended coverage of 20 dB
- Support of massive number of low throughput devices
e.g. 40 MTC devices per household
- Reduced complexity
- Things that cost less than a 2G device
- Improved power efficiency: more than 10 year battery life time
- Relaxed Delay characteristics: ~10 sec.

Rel. 13: Narrowband IoT (standardization ongoing)



MTC features like Power Save Mode (PSM), extended DRX (eDRX) cycle are valid.

Rel. 13: Narrowband IoT (standardization ongoing)

The Uplink and Downlink total transmission bandwidth is 180 kHz

Downlink: OFDM with 15 kHz sub-carrier spacing. Same subcarrier spacing, OFDM symbol duration, slot format, slot duration, and subframe duration as LTE

Uplink: SC-FDMA with 3.75 kHz and 15 kHz for single-tone transmissions and optional multi-tone transmissions with 15 kHz subcarrier spacing

Only FDD in half-duplex mode (analog to UE cat.0 half-duplex TypeB),

Only mobility in IDLE mode is supported



feMTC (Rel.14) power consumption, positioning, VoLTE and more

Data rate improvements

- Max uplink TBS of 2984 bits (M1)
- Up to 10 DL HARQ processes
- HARQ-ACK bundling in HF-FDD
- Faster frequency retuning (guard period of less than 2 symbols)

New UE Category

- New UE category (M2) with max TBS of 4008/6968 bits (UL/DL) and optionally support of 5 MHz (wideband) for PDSCH/PUSCH
- M2 device can operate as M1

VoLTE support

- Optimized parameter for VoLTE like new PUSCH repetition factors, restricted modulation schemes (QPSK) and adjusted scheduling delays (HARQ-ACK)

Device positioning

- E-CID support
- OTDOA support based on positioning reference signal (PRS) adapted for LTE-M (e.g. frequency hopping support, long cycles)

Mobility

- Mobility in connected mode
- Intra-frequency and inter-frequency measurements (RSRP/RSRQ) in CE mode

Group messaging/updates

- Adoption of Rel.13 Single Cell point-to-Multipoint (SC-PTM) feature
- Supported only in idle on 1.4 or 5 MHz



eNB-IoT (Rel.14) power consumption, positioning, VoLTE and more

Data rate improvements

- New UE category NB2 with max. UL and max. DL TBS of 2536 bits; optional support of two HARQs

1 000 000 devices per km²

- Both anchor and up to 15 non-anchor carriers can be used for paging and for random access procedure (PRACH)

New power class

- New power class of 14 dBm to support coin-cell battery operation e.g. for wearables with relaxed MCL of 155 dB

Device positioning

- E-CID support
- OTDOA support based on specific narrowband positioning reference signals (NPRS)
- Measurements in idle mode

Mobility

- Connected mode mobility realized by RRC connection re-establishment triggered by radio link failure (RLF)
- AS release assistance indication

Group messaging/updates

- Adoption of Rel.13 single cell point-to-multipoint (SC-PTM)



What's next in NB-IoT/LTE-M standardization

NB-IoT (feNB-IoT/NB-IoTenh2) in Rel. 15

- Latency and power consumption reduction:
 - Early data transmission during random access procedure
 - Wake up signal
 - Reduced system acquisition time
- NPRACH reliability and range enhancements
- Small cell support
- TDD support

What's next in NB-IoT/LTE-M standardization

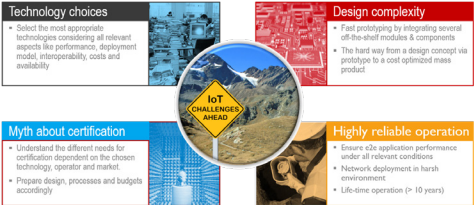
LTE-M (eFeMTC/eMTC4) in Rel. 15

- Latency and power consumption reduction:
 - Early data transmission during random access procedure
 - Wake up signal
 - Reduced system acquisition time
- Higher velocity (e.g. 200 km/h)
- Lower UE power class
- Improved spectral efficiency
- Load control improvements (CE)

5G Networks enable the IoT of the future



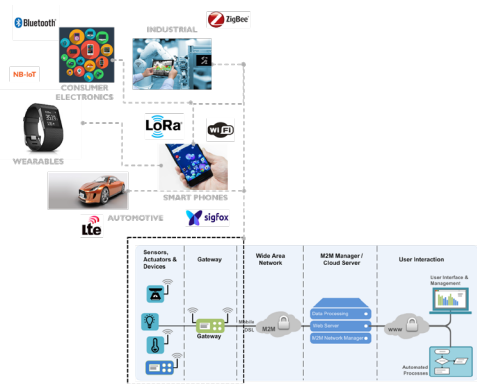
Challenges in a very dynamic and demanding market environment



Why test a very low cost IoT device?

- The main value add of the Internet of Things comes essentially from application software that relies on real-time sensor data
- Wirelessly connected devices are just the enabler, but only valuable when connected – secure, reliable and 24/7

A typical IoT System

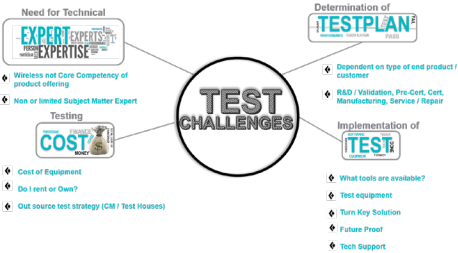


Testing in all phases of life cycle of IoT devices and networks



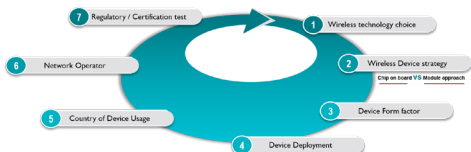
Typically, most IOT devices will go through six phases of development. Testing may seem to be very complicated, time-consuming and costly, especially for players entering the wireless communications arena for the first time. As an expert in wireless communications, Rohde & Schwarz will help you understand the critical testing requirements for your IoT device and can provide you with the proper test solutions to validate your device from the early R&D phase all the way through to manufacturing.

Key Testing Challenges for Wireless Deployment in M2M/IoT



Determination of Test

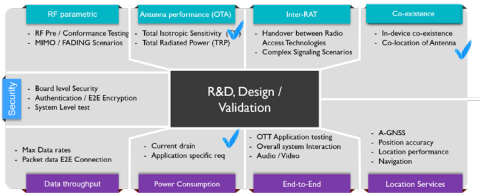
Key factors to consider



Determination of Test

- Dependent on position in Wireless food chain
 - Test requirements vary depending on chipset
 - supplier, network operator, module vendor supplier
 - and/or the high volume manufacturing
- Dependent on stage in product release life cycle
 - Early R&D / Validation
 - Pre- Certification / Conformance
 - High Volume Manufacturing
 - Service & Repair
- Testing typically centered around:
 - RF Parametric Testing (Conformance / Performance)
 - Data Testing (Conformance / Performance / Throughput)
 - Functional / User Experience Testing
 - System level testing

Typical test applications in R&D and Design Validation



The R&D and design validation testing phases are important to ensure that your product is ready, not only for the Compliance phase, but for volume manufacturing as well. Poor performing products can be expensive to recover from in later phases and may also lead to business failure.

OTA - What is Over the Air Testing?

- OTA stands for Over The Air: radiated tests
- Goal of OTA testing: to characterize the wireless performance of devices with the help of clearly defined test methodologies and performance metrics
- Complements the conducted measurements
- The CTIA organization test plan is defining the most of the OTA test requirements (GSM, CDMA, W-CDMA, LTE, A-GPS, ZigBee?)



Test Plan for Wireless Device Over-the-Air Performance

Method of Measurement for Radiated RF Power and Receiver Performance

Why perform OTA tests?

- Design of IoT devices typically use an off the shelf module + some type of enclosure + antenna
- Need to characterize the wireless performance of devices as a final product / testing of just the module is not enough

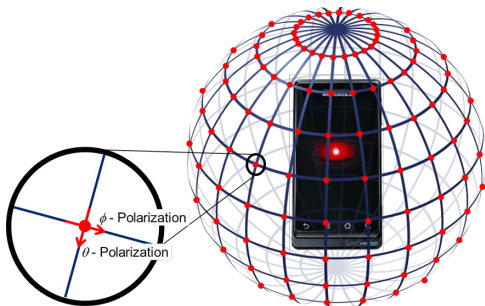


OTA Testing

Three Dimensional Evaluation

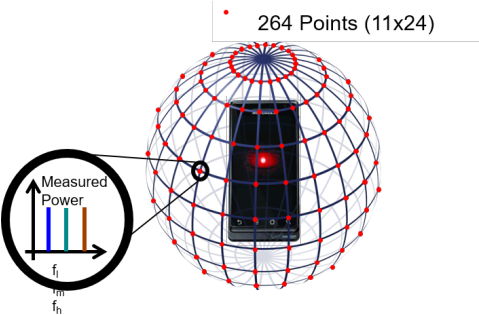
■ In order to characterize the DUT for a large variety of angles of arrival (AoA), radiation characteristics are captured in a full 3D fashion

- Elevation
- Azimuth
- Polarization



TRP: Total Radiated Power

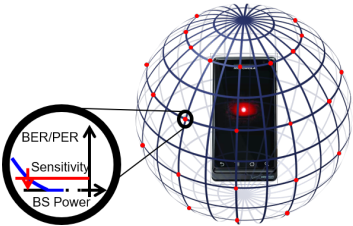
For every point on this sphere (AZ, EL, Pol) with $\Delta\phi = \Delta\theta = 15^\circ$, the radiated power (EIRP) as a function of frequency/channel is measured



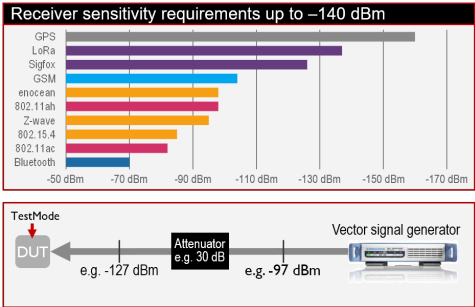
TIS: Total Isotropic Sensitivity

For every point on this sphere (AZ, EL, Pol) with $\Delta\varphi = \Delta\theta = 30^\circ$, a base station (BS) signal is generated and the received signal quality, e.g., BER, BLER, FER, PER, is measured by the DUT as a function of BS down link power (EIS)

60Points: 5x12

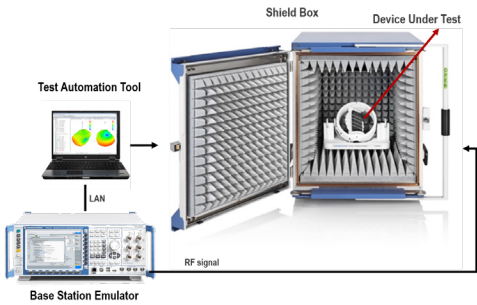


Receiver sensitivity measurements are critical

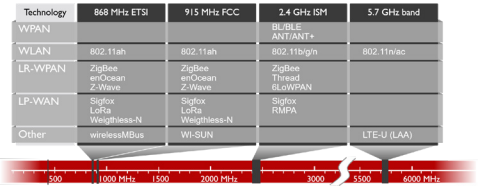


- Especially for all kinds of low power networks, the receiver sensitivity of devices and gateways is a crucial parameter
- High-quality signal generation performance is required to ensure accurate measurements
- The use of external attenuators is recommended for levels < -120 dBm
- Attenuator will lower the signal level and the noise floor level

Typical OTA Test Setup



Several devices supporting one or more wireless technologies operating in the same spectrum bands



Interference-prone Frequency Bands

LTE Band 40 2300 – 2400 MHz TDD Mode	ISM Band 2400 – 2483.5 MHz
	WLAN Channels Ch 1 : 2401 – 2423 MHz . . . Ch 13 : 2461 – 2483 MHz Ch 14 : 2473 – 2495 MHz
	Bluetooth Channels 79 Channels 2402 – 2480 MHz

Interference-prone Frequency Bands

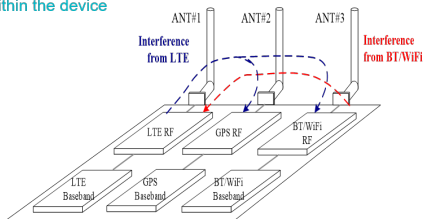
LTE Band 7 UL 2500 – 2570 MHz FDD Mode	LTE Band 38 2570 – 2620 MHz TDD Mode	LTE Band 7 DL 2620 – 2690 MHz FDD Mode
LTE Band 41 2496 – 2690 MHz TDD Mode		

Coexistence Testing

Wireless coexistence can be defined as the ability of multiple heterogeneous wireless systems to share the same or adjacent frequency spectrum without undue interaction or interference affecting performance and transmission or reception of signals and data

In-Device Co-existence

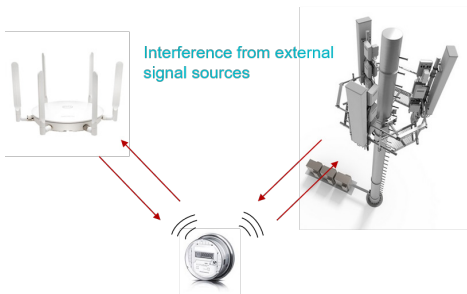
Interference internally from components / hardware within the device



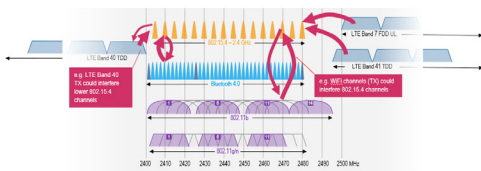
Coexistence Testing

Wireless coexistence can be defined as the ability of multiple heterogeneous wireless systems to share the same or adjacent frequency spectrum without undue interaction or interference affecting performance and transmission or reception of signals and data

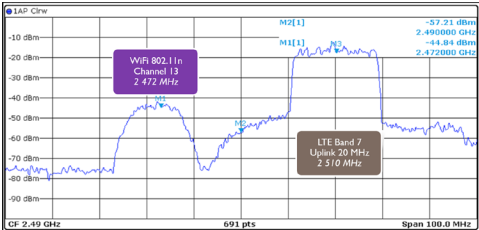
External Co-existence



(In-Device) Coexistence with Bluetooth, 802.11 and LTE

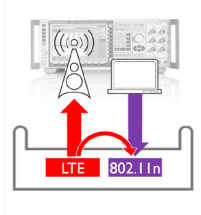
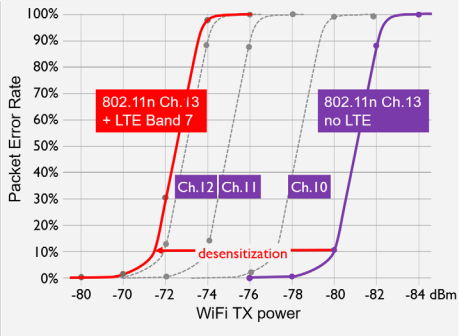


LTE/WFI In-Device Coexistence: Spectrum View



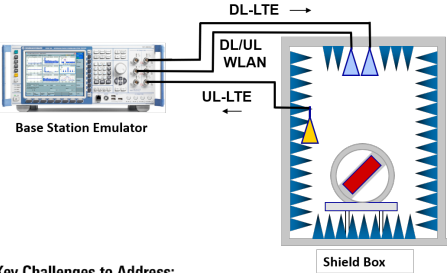
This data shows measurements on a WiFi device which is operating at 802.11n channel 13, at 2472 MHz. This device also has an LTE transmitter operating in band 7 at 2510 MHz with a 20 MHz signal bandwidth. The measured results indicate the sideband is bleeding over quite close to the WiFi channel 13.

Analyze EMI problems in development



Typical Test Setup

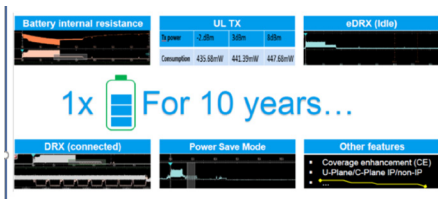
Co-existence Testing



Key Challenges to Address:

- Test Automation
- Simulation of scenarios (increase/decrease power levels, mobility etc)
- Proper shielding
- Network emulation/measurement tools

Power Considerations



Power Consumption - Why Test?

- How to deliver on the promise of the performance numbers

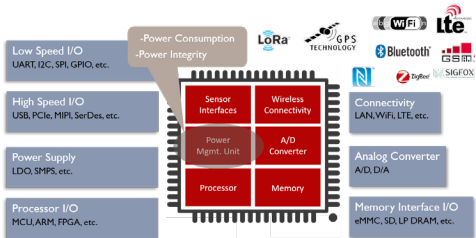


- Safety concerns
- Loss of revenue from recall



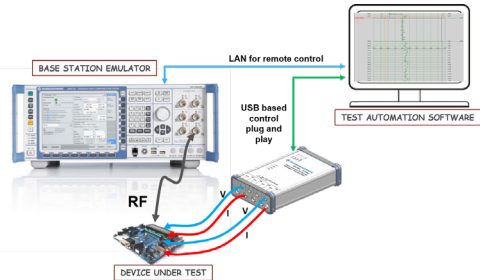
Embedded Wireless Devices

Key Components and Interfaces



For cost reasons, IoT devices often use an embedded design approach. The various functional cores are integrated on chip and module level. With the integration of wireless radios, the complexity of embedded designs increases significantly. A typical IOT device has different components. Each of components are drawing current or power from the battery, understanding how much is key.

Typical Test Setup for Power Consumption Test



Key Challenges to Address:

Ability to measure very low and transient current, voltage and power simultaneously

Simulate real life use cases with wireless network

Evaluate power consumption of each key interface for proper management independently and simultaneously

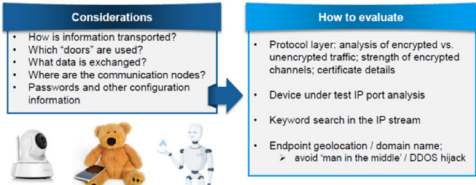
Synchronize signaling activities with power measurement

Topics for IoT Security

- What are the potential security concerns?
- Which kind of devices need to be tested?
- What are the requirements from industry and Governments?
- What solutions are being developed to test IP Security?



Identify and measure vulnerabilities in the IP connection

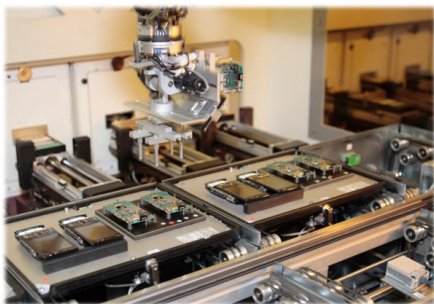


Connection Security Analysis

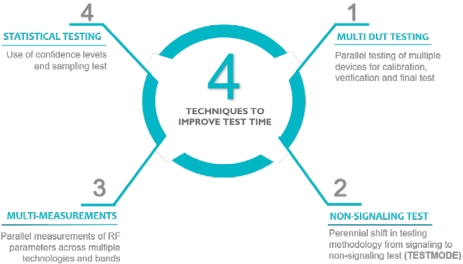


Manufacturing Test

- Main focus of testing in this phase builds on all the work done in previous phases (R&D, Validation, Compliance) verifying parts are put together properly, calibration of RF elements are done, and end of line final tests is done before product is shipped to the end user.
- Test is extremely streamlined to the bare minimum with a strong focus on cost and speed of test.
- PCB (Board test, RF Calibration, RF Verification) Final functional testing



Time = Money



Key Things to Note and Questions to Ask:

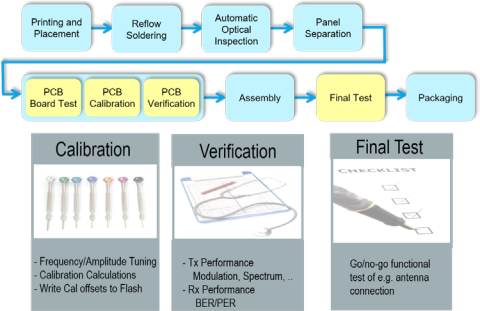
2 and 3 require support from the wireless chipset manufacturer

If using a module approach for your device, ensure module vendor has the right interface to use TESTMODE

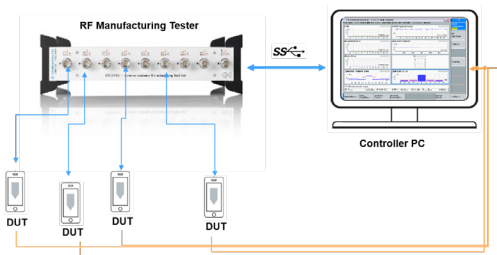
Ensure test equipment manufacturer has the right routines/APIs in place to support the Non-signaling test for the particular or family of chipset being used

Technical expertise and support

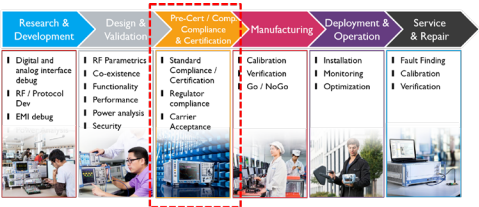
Typical Manufacturing Phases



Typical Test Setup for Manufacturing



Certification testing of IoT devices and networks



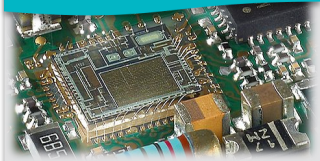
Products that communicate in the licensed frequency spectrum must abide by a set of rules that ensure they operate successfully, while also not interfering with other devices within its proximity. Even in the unlicensed spectrum there are rules and industry based governing bodies that require certifications before a product can advertise being Bluetooth, WiFi etc. certified. These rules ensure, not only compatibility between products, but also connecting the device to your home network won't disrupt the other devices in your house.

Wireless device strategy

Two key approaches

1

Chip on board



UPSIDE

Provides design flexibility

Ability to control overall cost IF skilled RF, testing, certification resource available

DOWNSIDE

Very costly Compliance / Certification process due to longer array of testing

Requires top notch Design and RF / Certification expertise

Design complexity could lead to VERY expensive \$\$\$ delays

Wireless device strategy

Two key approaches

Certified Module

2



Less RF, design and testing expertise required due to reduced complexity

Improves time to market due to reduced number of certification / compliance testing required

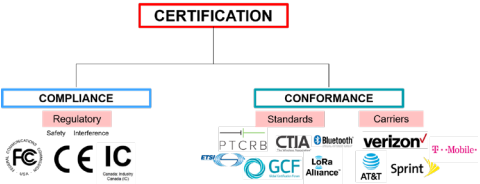
UPSIDE

Reduces design flexibility while adding form factor constraints

In certain instances adds another layer of technical support

DOWNSIDE

Certification vs Compliance vs Conformance



Certification is the act of certifying something via a recognized third-party such as a government regulatory agency or industry standard.

Compliance is the act or process of complying to the rules of a regulatory body. When you are designing and manufacturing your product, you test that it complies to the regulations.

Conformance is the act or process of conforming to the rules developed for an industry standard such as Bluetooth or LTE. In the wireless space, there are numerous agencies and network operators who work across the industry to define wireless standards.

Different Certification Bodies

1. **Regulatory Certifications** FCC (USA) ■ PTCRB (USA) ■ CE (Europe) ■ IC (Canada) ■ GCF (Europe) ■ RCM (Australia / New Zealand) ■ E-Mark (Europe) ■ TRA (UAE) • iDA (Singapore) ■ RoHS ■ NBTC (Thailand) ■ SIRIM (Malaysia) ■ SDPPI (Indonesia) ■ SRRC/CCC/NAL (China) ■ ICASA (South Africa) ■ MIC (Vietnam) etc
2. **Ruggedized Certifications** IP Certifications (Ingress Protection or International Protection)— IP65, IP66, IP67, MIL-STD-810
3. **Carrier Certifications** AT&T, Verizon, Vodafone, Telstra etc.
4. **Specialized certifications** Food, Pharma, Medical, Oil & Gas

Federal Communications Commission (FCC)

Mandate: regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. Its an independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation.

Objective: “Do no harm”

Rules: Published in the Code of Federal Regulation (CFR) Part 47 (Telecommunications) www.ecfr.gov

Mandatory Required Certifications:

- SAR under 47 CFR Part 2, section 2.1093, 1.1310 (For devices used within 20cm of the human body)
- FCC Part 15 Subpart C for intentional Radiators
- FCC Part 15.1b, unintentional radiator requirements
- FCC Part 22/24/27 for Cellular, PCS, Broadband transmission Certification

Testing must be done in accredited FCC labs

Specific Absorption Rate Testing (SAR)

Specific Absorption Rate (SAR) testing measures the amount of electromagnetic energy absorbed by biological tissue when using a wireless device over a period of time. It allows you to demonstrate that your product complies with international established RF exposure SAR limits.

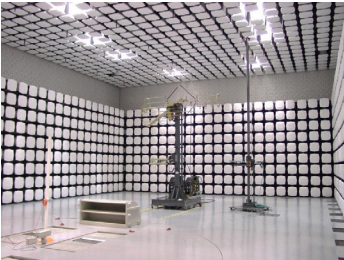
Most mobile devices will be used within 20cm of the body, head, ankle or wrist. At this proximity the user is exposed to electromagnetic fields (EMF – the wireless technology – a form of non-ionising radiation). This is how wireless devices communicate.

SAR testing involves the use of a “phantom” which simulates the human head. A liquid which is designed to be the electromagnetic equivalent of human tissue (brain) is placed in this phantom. The device under test is put into a “call” at maximum power and a robotic arm then moves a measurement antenna through the liquids and makes Electric field measurements.

FCC Unintentional/Intentional Radiators

Part 15b – Unintentional Radiator: Unintentional emissions are the undesired signals from the radio or other parts of the device including the IoT radio receiver, clock generator, power supplies and digital circuits.

- For most rule sections, the unintentional emissions must be measured to the 10th harmonic of the transmitting signal which requires a relatively high frequency spectrum analyzer or similar device.
- Testing usually done radiated



FCC Unintentional/Intentional Radiators

Part 15C – Intentional Radiator: Deals with devices that are deliberately designed to produce radio waves in the unlicensed frequency. Radio transmitters of all kinds, including the garage door opener, cordless telephone, cellular phone, wireless video sender, wireless microphone, and many others fall into this category.

3 main radio communication schemes:

- Digital Modulation: WiFi, Zigbee, Lora
- Frequency Hopping Modulation: Bluetooth
- Low power Narrow band transmission: Garage Door openers, Keyless entry for automobiles

Part 22, 24, 27 – Intentional Radiator: Deals with devices that are deliberately designed to produce radio waves in the licensed bands (Cellular, PCS, Broadband transmission Certification). 850MHz, 1900MHz and 700MHz respectively

Leveraging a Module Certification (avoiding Part 22, 24, 27 testing)

- NO Co-location: Another radio within 20cm that can transmit at the same time
- Not portable: Portable means used within 20cm of human body

PTCRB

PTCRB is a certification organization established in 1997 by leading wireless North American operators to define test specifications and methods to ensure device interoperability on global wireless networks.

Required by North American cellular carriers with the exception of Verizon Wireless

Testing covers Conformance (3GPP / OMA Specs) and OTA performance



CTIA is the current administrator of the PTCRB Certification process

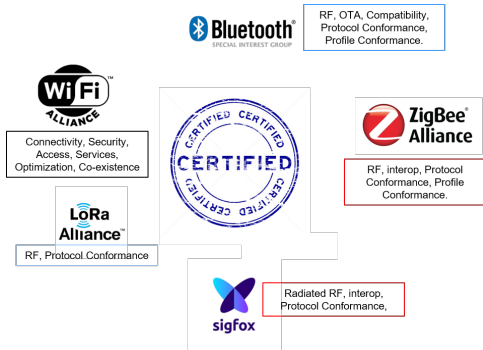


Unlicensed - WiFi, Bluetooth, Zigbee, Lora, Sigfox

Each of these technologies have their own dedicated certification test needed to be run. They must also all pass FCC certification.

While standard certification is not compulsory, its required in order to use the branding and proper interoperability

WiFi, Bluetooth and Zigbee administered by CTIA in North America

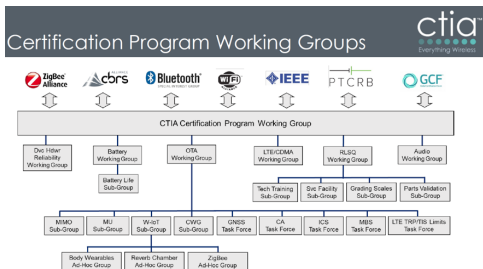


CTIA

CTIA represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem.

Manages / administers a number of certification programs and testplans

<https://www.ctia.org/initiatives/certification/certification-test-plans>



Examples of Network Operator Certification

In addition to certification by the standard bodies, each operator has their own requirements IoT devices must meet to be allowed onto their network

■ ATT

- PTCRB
- TRP: Total Radiated Power (test limits in dBm, protected by NDA)
- TIS: Total Isotropic Sensitivity (test limits in dBm, protected by NDA)
- AT&T Compatibility Testing

■ Verizon: (ODI process can be found online)

- No PTCRB
- TRP and TIS for LTE;
- LTE: Conducted RF testing; antenna ECC; SAR if tablet, CAT-M1, NB-IoT etc
- Conformance testing, field testing

■ Sprint

- No PTCRB
- GCF, TRP and TIS (they will test first attempt for free at their lab)

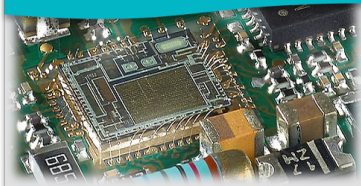
■ T-Mobile

- PTCRB, but no TRP or TIS for M2M

Certification Cost Estimates (Cellular 2G, 3G, LTE)

1

Chip on board



Lowest cost per unit

**Highest Non-reoccurring Engineering
(over \$1Million)**

Certification can approach \$1M or more

Certification Cost Estimates (Cellular 2G, 3G, LTE)

Certified Module

2



Cost of module higher than chipset

Lower Non- reoccurring engineering

\$30K - \$100K

95%

Cost reduction when cellular module is used as opposed to chip on board approach

Common Certification Issues

- Manufacturers focus a lot of effort on product design, with not a lot of compliance, so the product works, but fails certification.
- Failing Operator OTA requirements
- Failing PTCRB requirements
- Misrepresentation / understanding of new certification rules
- Lack of Product Certification support (resource and interfaces)
- Data testing especially Retry Failback
- Lack of OTA provisioning and firmware support

How to mitigate certification failures

- Design your product to work, but with an eye on\ certification test requirements
- Pretest! Pretest! Pretest!
 - Invest in validation and pre-compliance setups
 - Prevent costly design change and delay late in the development process. Testing should be an iterative process right from R&D to launch
- Pay close attention to the Antenna design
 - Space is key, make room.
 - Keep away from metal such as PCB, display, cables enclosure
- Start EMI testing early in the process
- Build support interfaces
 - Pass through mode to access the module
 - SW update capability and back off periods

Summary: Key Facts about Certification

All devices require FCC Certification

- Even for new devices using a previously FCC approved module, FCC certification is mandatory
- Exceptions: If a device is a simple evolved mobile solution that complies with the module FCC Grant Notes, typically FCC ID of the module can be leveraged.

The OEM/ODM has to research, discuss with the module supplier, and know what privileges the FCC granted the module in its certificate (e.g. limited to a very specific antenna design/config)

For products to be used outside the country, familiarize yourself with the regulatory, standards and operator certification requirements

SAR testing required for **portable** devices

Beyond FCC testing, Bluetooth, Zigbee, WiFi, Lora all require their own certification to allow use of brand and logo, interop and sale.

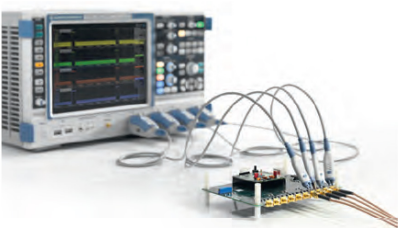
With a certified module, you drastically reduce the amount of testing needed for certification.

Testing in all phases of the lifecycle of IoT devices and networks



Test and measurement solutions from Rohde & Schwarz cover all major cellular and non-cellular technologies. Our comprehensive product portfolio offers the right T&M solution for your IoT device – from the first product idea through the full device lifecycle.

Smart debugging of embedded designs



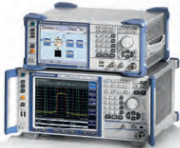
Troubleshoot your IoT device at the system level through time-correlated analysis of analog components, digital interfaces, protocol-based buses, power supplies and RF signals with a digital oscilloscope.

Single-box wireless communications tester



Test RF parametric performance of cellular and noncellular standards such as LTE, Bluetooth® and Wi-Fi (incl. IEEE 802.11p) as well as cellular protocols, including support of 3GPP MTC features like LTE Cat 0, with one box.

Wireless test setups for R&D



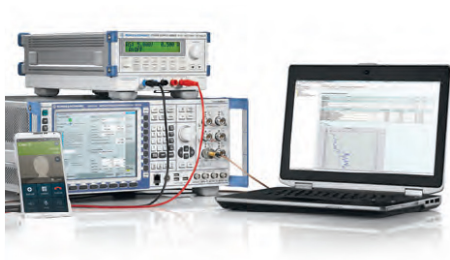
Test the radio interface of various wireless standards over the air with a compact test system consisting of a signal generator, spectrum analyzer and RF shielded box.

Automated functional tests for the essentials



Measure fundamental RF characteristics of cellular and non-cellular standards and perform functional tests under reproducible network conditions especially for integration of RF modules as well as in service and repair.

End-to-end application testing



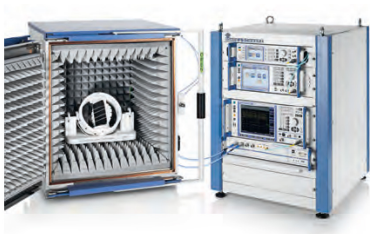
Explore the functionality and performance of your IoT device from the end-to-end perspective by analyzing data and signaling traffic, quality of service and battery consumption under realistic network conditions.

Highly efficient and automated manufacturing tests



Choose a wireless communications tester optimized for high-volume manufacturing to perform non-signaling tests on IoT devices that support cellular and non-cellular standards such as LTE, Wi-Fi, Bluetooth® and ZigBee.

Conformance testing



Test the EMC conformance of your IoT devices operating in the 2.4 GHz and 5 GHz ISM bands such as Bluetooth® and Wi-Fi.

Network installation and maintenance



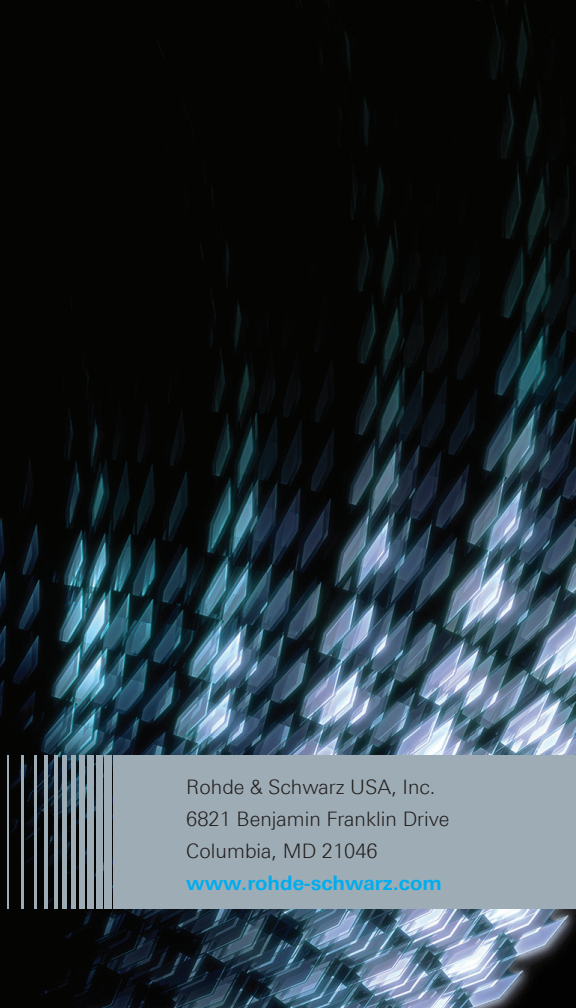
Use a handheld spectrum analyzer to maintain and install networks, assess signal quality and measure electric field strength to ensure quality of experience (QoE).

For More Information:

https://www.rohde-schwarz.com/us/solutions/test-and-measurement/wireless-communication/iot-m2m/iot-m2m-overview_230314.html

https://www.rohde-schwarz.com/us/solutions/test-and-measurement/wireless-communication/wireless-5g-and-cellular/5g-test-and-measurement/5g-overview_229437.html

https://www.rohde-schwarz.com/us/solutions/test-and-measurement/wireless-communication/wireless-connectivity/overview/wireless-connectivity_233828.html



Rohde & Schwarz USA, Inc.
6821 Benjamin Franklin Drive
Columbia, MD 21046

www.rohde-schwarz.com