PRESENTED BY

INTERFERENCE TECHNOLOGY®

2022 IoT, WIRELESS, 5G EMC GUIDE

INTERFERENCE TECHNOLOGY GUIDE SERIES | www.interferencetechnology.com

TABLE OF CONTENTS

INTRODUCTION 5
MIKE VIOLETTE, P.E.
Director, American Certification Body and Washington Labs

IoT, Wireless, 5G EMC Suppliers Matrix 7

Telecommunication Testing on Relevant RF Components 10
AR RF/Microwave Instrumentation

The Internet of Things, Wireless and Security 13
MIKE VIOLETTE, P.E.
Director, American Certification Body and Washington Labs

For Remote Patient Monitoring Systems, Wireless Coexistence Can Be Lifesaving 15
NASEEF MAHMUD
Rohde & Schwarz

REFERENCE SECTION 20

IoT, Wireless, 5G EMC Standards 20

IoT, Wireless, 5G EMC Groups & Organizations 21

Useful Wireless References 23

INDEX OF ADVERTISERS 26

INTRODUCTION

A Short Perspective on our Industry: IoT, Wireless and Security

Mike Violette, P.E.
Director, American Certification Body and Washington Labs

Progress works out to be about 20 dB/decade, a familiar slope in our trade.

The term “The Internet of Things” is a concept that went from a novel (like Bitcoin or Streaming or something similar) to a phrase that is as household as a Spying Siri or an Alert Alexa.

Way back, when I was a green engineer, the nominal upper frequency for testing of PCs and the like was 1 GHz. System clocks ticked along at a blistering 25 MHz. Jump a generation and the talk is in the THz, which is a nominal 1000-fold increase in frequency, or to the logarithmically inclined, an increase in 60dBGHz which works out, throughout my career, an increase of about 20dB/decade indicating an exponential increase in operating frequencies, which goes with a plethora of design challenges, ever higher data rates, spectrum expansion and the potential for interference, not to mention the need to making measurements of this stuff.

Staring at the green pre-LED phosphor-painted wiggles on our trusty HP 8568 spectrum analyzer, we didn’t see much “up there” as most of the mush from the early machines of the x86 family of microprocessors petered out above a few hundreds of MHz. (Historical note, initial versions of Intel’s offerings appeared as 8086 and 8088. **The 4044 being the first commercially-available 4-bit µP** As the speeds/densities increased, Intel released models numbered 80286, 80386 and 80486 and finally said “Heck with it, let’s stop at ‘5’ and call it PENTIUM.) Of course, this was about 26 dByears ago (ah, refer to previous footnote regards liberal use of the dB acronym), as many advances in processor technology have occurred. Currently, the Pentium product is nominally an entry- to mid-range processor—Intel’s “Core” offerings are the current high-end data workhorses.

Now, embedded designs, agile software-defined radios, multi-function chipsets and networked solutions are the norm.

For ***Interference Technology’s 2022 IoT, wireless, 5G EMC Guide***, this short intro covers a few topics, namely some thoughts on the Internet of Things, Wireless and Security—all things that designers, test houses/compliance professional/systems planner have to contend with. The convergence of these ideas and notions has happened amazingly quickly.

The current generation of **IoT** consists of numerous applications, from asset-tracking to inventory control, Earth sensing and geo-location. We have a client that uses low-data rate array of sensors to communicate with a Low Earth Orbit (LEO) satellite constellation. The ground-based sensors use Ground Penetrating Radar (GPR) to image the dirt underneath. These data are relayed to the satellite to provide the image data to geo-physicists for research and exploration (beats digging up the planet, I guess, and is nominally less intrusive than explosive-based seismic monitoring or brute-force prospecting). This particular application uses a very low bit rate and burst communications to the satellites, a good example of “Internet of Space” and the application of sensing to IoT.

1. [1]For the mathematically pure, this is not a correct use of the decibel. The next decade, in years, is 10X the current year or about the year 20220, but what the hey, mixing meanings here, is the author’s prerogative.

On the opposite end of the "spectrum of use" so-to-speak are the SATCOM networks used for broad-access broadband internet communications, useful in our busy e-commerce environment and appealing to Tik-Tokers the world-over (and yes, I am guilty of hours of "swiping up" to the next silly video). Various contenders use LEO and GEO orbits for data delivery.

IoT is a medium of many forms and, really, has been around for many decades. Expect more…

Wireless Applications are proliferating profusely. 5G is pretty common nowadays and rapidly spreading. 6G is next (and being adopted in various guises)—the "G" having nothing to do with frequency, but about performance metrics, data delivery and access, and marketing. The exciting part of this area of technology is the upper-push into the GHz+ space. Various stakeholders are working and competing in this arena are across the industry and government. One common link to these activities is the mmWave Coalition https://mmwavecoalition.org/ which is an advocacy group for spectrum access for industry and academia. Incumbents include government users and space-exploration advocates. Careful accommodation of the various users of the spectrum is a key goal.

The tricky part of these frequencies are the milli-meter wave measurements that need to be quantified (for performance and regulatory purposes). As a test lab, we are continuously challenged to make the most-accurate measurements possible. The real tricky part of these measurements are the very fine-beamwidths that are affiliated with the physics of the propagation of small-wavelength signals (and noise). Tiny displacements of device arrangement and measurement probes make a huge difference in performance and quantification. I think of these subtleties as the precision needed to focus a magnifying glass to a fine point to scorch a leaf or burn a piece of paper. Millimeters matter.

Layered atop these implementations of IoT and wireless application are the real concerns about security. The actions of bad-actors, state-sponsored and sophisticated bandits, lays a heavy cold blanket atop the promise of more access and functionality of our data-driven world.

For device suppliers with a European market (CE Marking, UKCA), a cyber-requirement is emerging under the Radio Equipment Directive (RED). The implementation of cyber-protections is emerging and will require compliance with Article 3.3(d), (e) and (f). A useful guide can be found here: https://ec.europa.eu/docsroom/documents/33162

EMC, in its traditional sense, has morphed to cover layers of the physical and software world. As the world becomes more complex and intertwined, the EMC engineer needs to be a "Swiss-Army" engineer with multiple tools to assist clients and maintain proficiency in our fast-changing industry

WIRELESS & IoT EMC SUPPLIERS MATRIX

INTRODUCTION

There are two main categories of equipment in this handy supplier guide: EMI troubleshooting & measurement equipment and direction finding equipment.

EMI troubleshooting and measurement equipment includes spectrum analyzers, near field probes, current probes, antennas, and other pre-compliance equipment.

Direction finding (or DFing) equipment usually includes specialized portable, mobile, or base station spectrum analyzers with custom antennas and mapping software especially designed for locating interfering sources.

Wireless & IoT EMC Supplier Matrix		Type of Equipment								
Manufacturer	Contact Information - URL	Amplifiers	Antennas	Current Probes	Fixed DF Systems	Mobile DF Systems	Near Field Probes	Portable DF Systems	Pre-Compliance Test	Spectrum Analyzers / Receivers
360Compliance	www.360compliance.co/								X	
Aaronia AG	www.aaronia.com	X	X		X	X		X	X	X
Alaris Antennas	www.alarisantennas.com		X							
Anritsu Company	www.anritsu.com		X							X
Avalon Test Equipment Corp	www.avalontest.com	X	X	X		X	X		X	X
CommsAudit	www.commsaudit.com/products/		X		X	X				X
Doppler Systems	www.dopsys.com		X		X	X		X		
The EMC Shop	www.theemcshop.com	X	X	X			X		X	X
Gauss Instruments	www.gauss-instruments.com/en/									X
Intertek	www.intertek.com								X	
Kent Electronics	www.wa5vjb.com		X							

Wireless & IoT EMC Supplier Matrix		Type of Equipment								
Manufacturer	Contact Information - URL	Amplifiers	Antennas	Current Probes	Fixed DF Systems	Mobile DF Systems	Near Field Probes	Portable DF Systems	Pre-Compliance Test	Spectrum Analyzers / Receivers
Keysight Technologies	www.keysight.com						X		X	X
Morcom International	www.morcom.com/direction_finding_systems.html							X		X
MPB srl	www.gruppompb.uk.com		X	X					X	X
MVG, Inc	www.mvg-world.com/en		X				X		X	
Narda/PMM	www.narda-sts.it	X	X						X	X
Pearson Electronics	www.pearsonelectronics.com			X						
RDF Antennas	www.rdfantennas.com							X		
RDF Products	www.rdfproducts.com				X	X				X
Rhotheta America	www.rhothetaint.com				X	X		X		
Rigol Technologies	www.rigolna.com			X			X		X	X
R&K Company Limited	www.rk-microwave.com	X								
Rohde & Schwarz USA, Inc.	www.rohde-schwarz.com/us/	X	X	X	X	X	X	X	X	X
Siglent Technologies	www.siglentna.com						X			X
Signal Hound	www.signalhound.com			X						X
SPX/TCI	www.spx.com		X		X	X		X		X
SteppIR Communication Systems	www.steppir.com		X							
TechComm	www.techcommdf.com		X		X	X		X		X
Tektronix	www.tek.com					X	X	X	X	X
Teseq	www.teseq.com/en/index.php	X		X					X	
Thurlby Thandar (AIM-TTi)	www.aimtti.us								X	X
TMD Technologies	www.tmd.co.uk	X								
UST	www.unmannedsystemstechnology.com/company/marshall-radio-telemetry/							X		X

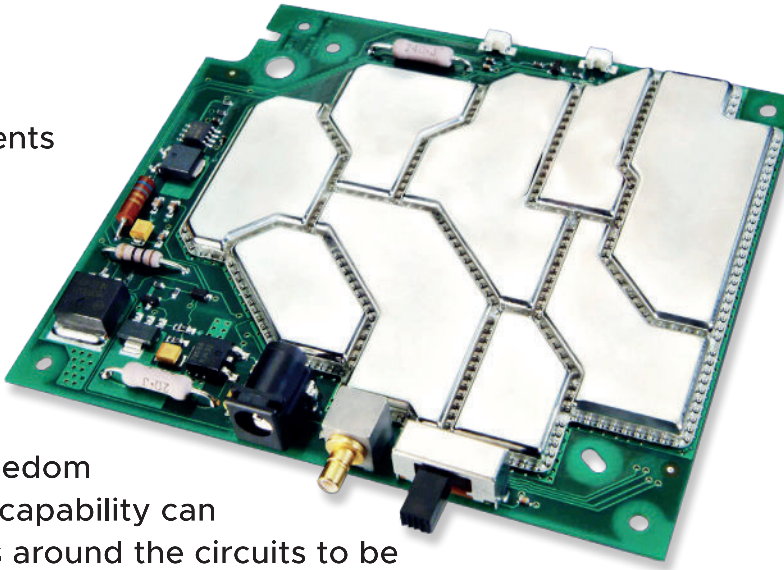
Superior Shielding & Total Customization

SnapShot®

Board Level EMI Shielding

SnapShot® Board Level EMI Shields ... celebrating 20 years of success!

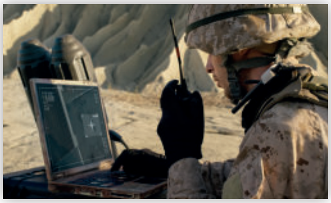
- Total Design Freedom
- Lowest Profile Shield Available
- Extremely Durable for Extreme Environments
- Installs AFTER Reflow
- Removable and Replaceable
- Ultra-Lightweight
- Space Saving Multi-Cavity Capability



SnapShot EMI shields are custom designed for every application allowing unmatched design freedom when laying out your PCB. The true multi-cavity capability can save over 50% on your trace width requirements around the circuits to be shielded. All of this is enabled by XGR's unique engineered shielding material and proprietary thermoforming process.

20 years of success in applications across industries:

- Industrial Handheld Computing
- Military Communications
- Medical Imaging Equipment
- Network Computing Equipment
- Military and Industrial Drones
- Avionics and GPS Equipment
- Consumer Wearable Electronics



xgrtec.com

TELECOMMUNICATION TESTING ON RELEVANT RF COMPONENTS

AR RF/Microwave Instrumentation

The telecom industry has undergone rapid development in the past several decades. Digital communications methods have advanced, requiring increased bandwidth and frequency coverage. This advancement has complicated an RF measurement system's capability to accurately characterize system components. The 3rd Generation Partnership Project (3GPP) provides modern broadband mobile communication guidance. This development is chronicled in the evolutionary steps known as 2G, 3G, 4G, and now to the 5G stage currently being launched. A review of how the air interface layer changed through this evolution will help explain how measurement systems often need to be upgraded to meet the new performance criteria.

1.0 2nd Generation

2G modulation was the early format to move from analog modulation to digital modulation schemes. And building off of analog bandwidth and frequency coverage, the only thing to be added within the measurement system was time domain considerations to match the modulations transmitter gating.

2.0 3rd Generation

3G represented a significant advancement in digital communication. Military developments in spread spectrum technology spun off into the commercial space leading to Code Division Multiple Access (CDMA) and the higher data rate wideband CDMA (WCDMA) shown in *Figure 1*. As shown in *Figure 2*, this scheme used a Pseudorandom number waveform (PN) and quadrature modulation that required more bandwidth than the previous 2G channels. Additionally, the orthogonal modulation used has extensive peak power excursions, seen in *Figure 3*.

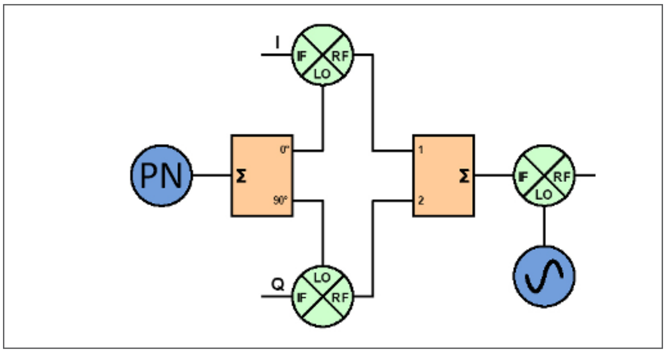


Figure 1: CDMA Transmitter Fundamentals Block Diagram

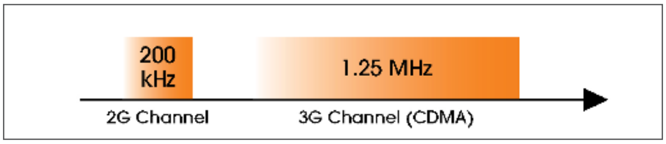


Figure 2: 2G vs. 3G Channel Bandwidth

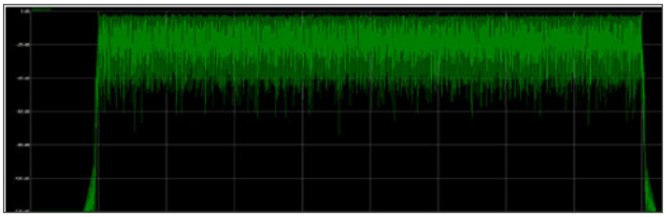
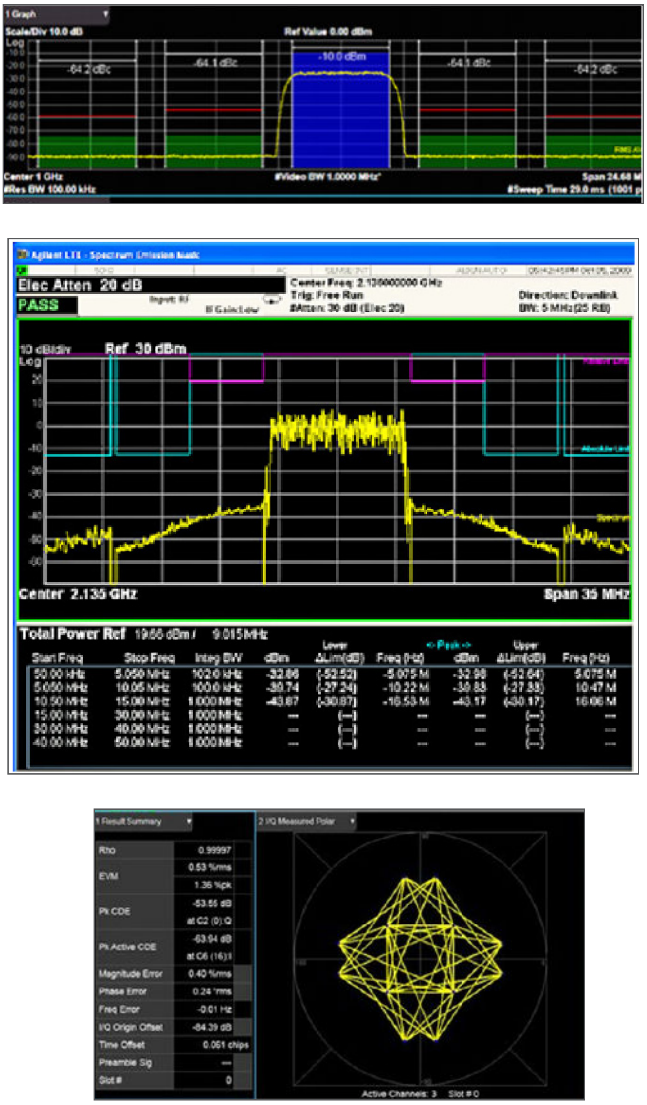


Figure 3: Power/Frequency Spectrum of an Orthogonal Modulated Carrier

3G RF measurement systems could no longer use traditional CW techniques used for many decades as these cannot accurately represent wideband orthogonal modulation. Consequently, significant investment was required in both signal generation and signal analysis. Vector signal generators are required along with signal analyzers capable of demodulation and spectral measurements such as Adjacent Channel Power (ACP), Spectral Emissions Mask (SEM), and Error Vector Magnitude (EVM), as seen in *Figure 4*. * Due to a demand for more spectrum for broadband mobile communication, moving to 3G increased the spectrum from 450 MHz to 6 GHz.



Total Power Ref 19.66 dBm / 9.015MHz

			Lower			<- Peak ->	Upper	
Start Freq	Stop Freq	Integ BW	dBm	ΔLim(dB)	Freq (Hz)	dBm	ΔLim(dB)	Freq (Hz)
50.00 kHz	5.050 MHz	102.0 kHz	-32.86	(-52.52)	-5.075 M	-32.98	(-52.64)	5.075 M
5.050 MHz	10.05 MHz	100.0 kHz	-39.74	(-27.24)	-10.22 M	-39.83	(-27.33)	10.47 M
10.50 MHz	15.00 MHz	1.000 MHz	-43.87	(-30.87)	-16.53 M	-43.17	(-30.17)	16.06 M
15.00 MHz	30.00 MHz	1.000 MHz	---	(---)	---	---	(---)	---
30.00 MHz	40.00 MHz	1.000 MHz	---	(---)	---	---	(---)	---
40.00 MHz	50.00 MHz	1.000 MHz	---	(---)	---	---	(---)	---

Rho	0.99997
EVM	0.53 %rms 1.36 %pk
Pk CDE	-53.55 dB at C2 (0):Q
Pk Active CDE	-63.94 dB at C6 (16):I
Magnitude Error	0.40 %rms
Phase Error	0.24 °rms
Freq Error	-0.01 Hz
I/Q Origin Offset	-84.39 dB
Time Offset	0.051 chips
Preamble Sig	---
Slot #	0

Figure 4: 3G Measurements

** Concurrent with 3G development were advances in fixed wireless technology commonly called WIFI/WLAN. This also uses orthogonal modulation and uses the s*

An example of a 3G RF measurement system is shown in *Figure 5*. This type of setup is used to characterize the RF components in the 3G radio head. It consists of a multichannel power supply for active devices, a signal generator capable of vector modulation, and a spectrum analyzer. Network analyzers may also be capable of 3G modulation/analysis and S-Parameter measurement.

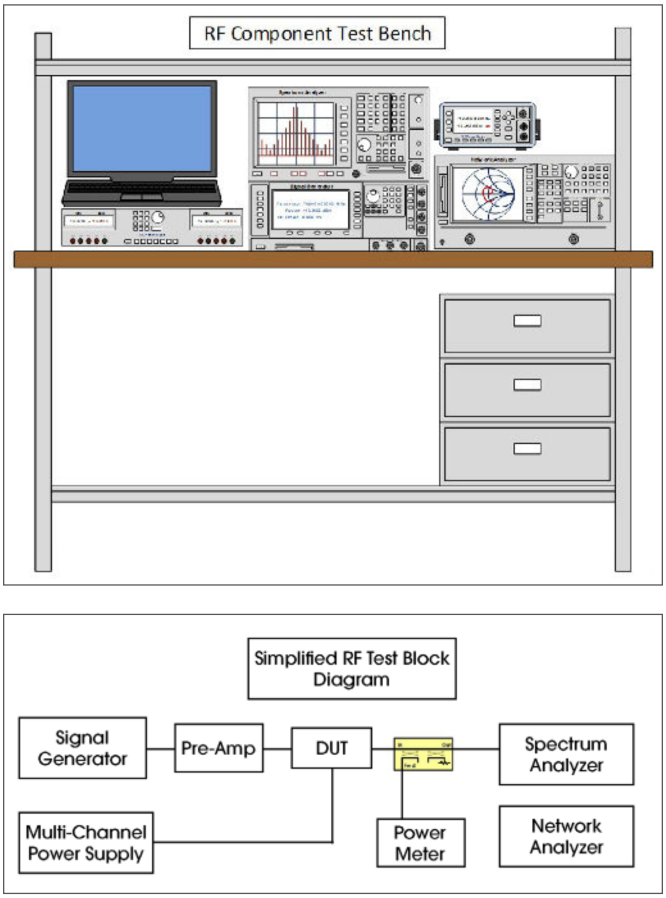


Figure 5: 3G Measurement System

The **signal generator** is a significant upgrade from 2G capable models. These Vector Signal Generators (VSG) employ arbitrary waveform generation (ARB) and I/Q modulation capability. The ARB sample rate determines the bandwidth potential, which must exceed the channel bandwidth of the desired 3G signal, which is a maximum of 5 MHz. Due to the very high peak to average power excursions of 3G modulation, the linear output power of the signal generator is often limited. A pre-amplifier is required to provide nondistorted signals to the Device Under Test (DUT).

For the **pre-amplifier**, a Class A amplifier is the best choice. Its frequency range should be broad enough to cover the entire 3G spectrum and be able to provide the additional non-distorted signal required by the DUT. Since DUT failures may present a very high mismatch, the amplifier should be ruggedized to 100% return power

The **power supply** is used for active device bias, which is a simple but vital part of the RF test bench. Current sense lines must be employed to compensate for voltage drops on high current devices. Overvoltage limiting is desired to protect the DUT from overvoltage transients.

The **DUT**, if active, should use bypass capacitance on the test circuit board, which will supply surge current energy for RF bursts and peak-to-peak power excursions. For precise efficiency calculations, a directional coupler and power meter are used to determine the exact power at the output of the DUT calculations.

In addition to covering the 3G frequency + harmonics, the **spectrum analyzer** may be configured for predefined measurements based on 3GPP specification. If EVM is measured, a vector demodulation option is required.

3.0 4th Generation

4G, otherwise known as Long Term Evolution (LTE), increases channel bandwidth to 20 MHz per channel and can include 5 contiguous channels to 100 MHz total bandwidth. *Figure 6*. The RF test bench remains much the same, with the exception that the VSG must increase ARB bandwidth to greater than 100 MHz.

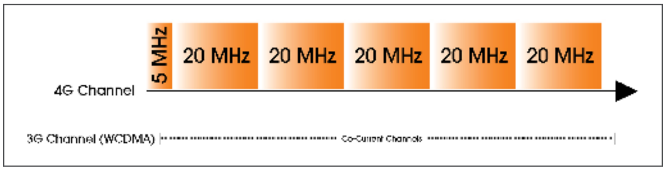
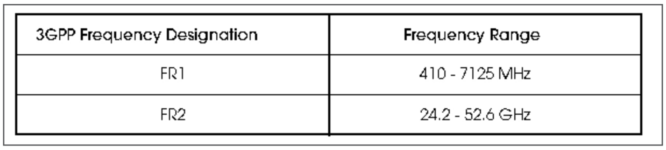


Figure 6: 3G vs. 4G Channel Bandwidth

4.0 5th Generation

5G is a paradigm in mobile communications. More than a simple evolution, this generation introduces new protocols and is called New Radio (NR). Significant increases in bandwidth and latency are keystones for this new standard. Overcrowding in the current 3GPP spectrum designated as Frequency Range 1 (FR1) and bandwidth requirements has pushed the upper-frequency range (FR2) to 24.25 – 52.600 GHz, as shown in Figure 6. FR1 measurement systems will overlap 4G system capability. However, the move to FR2 with a bandwidth up to 400 MHz will require significant investment in new measurement systems capable of those high frequencies. Test equipment manufacturers are developing test equipment and methods to alleviate the considerable cost of a new test bench. These methods may include a box solution capable of making all the RF measurements, including saturation, Intermodulation Distortion (IMD), and S-Parameters. RF cables and connectors must be low loss and length minimized. On-chip antennas will require an Over the Air (OTA) test chamber, seen in *Figure 7*.



3GPP Frequency Designation	Frequency Range
FR1	410 - 7125 MHz
FR2	24.2 - 52.6 GHz

Figure 7: 5G Frequency Spectrum

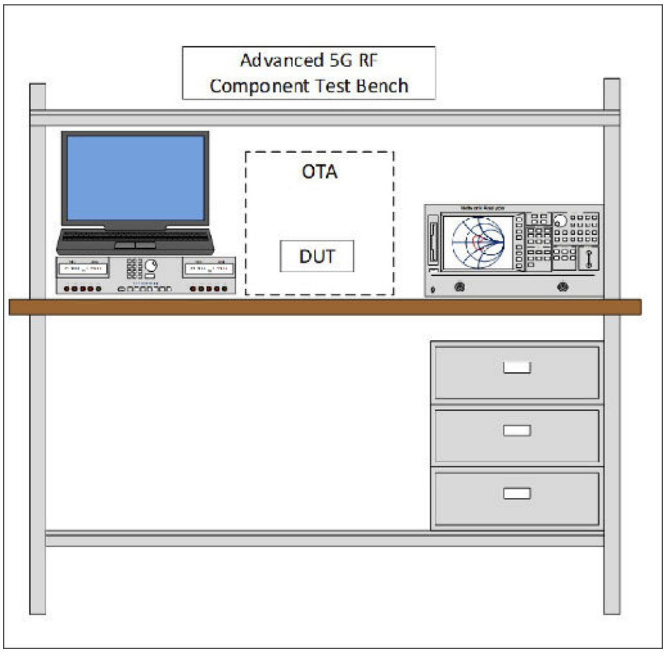


Figure 8: 5G RF Test Bench

Conclusion

The history of evolving wireless communications has shown a continuing need to upgrade measurement systems. As we continue to evolve within the telecom industry, and it is expected that this requirement will continue. The frequency spectrum and bandwidth will only increase. Test specifications will mandate additional changes to required test equipment. Capital investment in new equipment should be expected to keep up with the ever-changing demand for more data bandwidth.

THE INTERNET OF THINGS, WIRELESS AND SECURITY

Mike Violette, P.E.
Director, American Certification Body and Washington Labs

SUMMARY

This article gives an overview of international and domestic efforts to protect our connected world. These efforts will be ongoing in perpetuity as the world becomes more complex, more risky and increasing exposed to many varieties of threats.

Across the Pond

The European Union (and UK) are actively addressing the security of wireless devices, as outlined under the Radio Equipment Directive (RED). The Directive, one of many that affects electronics devices, has a specific provision that is going to be enacted in the near very near future. Manufacturers and test labs (and Notified Bodies) need to be prepared to manage an important clause in the RED.

The need is obvious: in our connected world, more Internet of Things (IoT) devices are being hooked up to networks, other devices and critical infrastructure. They are increasingly vulnerable to attacks from many corners of the internet. For instance, in our work, nearly every device has a wireless feature implementing all manner of IEEE 802.11 standards for WiFi, Bluetooth, as well as other applications for radar, sensing and other uses of the electromagnetic spectrum.

The May 10, 2021 hacking of the Colonial Pipeline by bad actors, especially during these turbulent and fraught times, made the US Federal Government to issue an emergency declaration. This, coupled with work done by others in the industry point to the fragile nature of our infrastructure where penetration into networks is nothing new.

Many other alarming examples exist across the world and across cyber-verse. In April of 2021 The New Yorker[1] published an amazing exposé of North Korea's state-sponsored hacking and blackmailing operations that squeeze billions of dollars from banks, corporations and other institutions—representing a significant contribution to the country's coffers. In an ongoing effort, the North Korean government recruits talented programmers and then gives them intense training runs targeted campaigns of extortion, often under severe duress to the programmers that include threats to families and close ones if the programmers don't deliver.

So there is much discussion in many industries of the ways to secure the networks. In the US, the National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework that provides guidance to organizations (both at the Federal and Private Industry level) with "standards, guidelines and best practices to manage cybersecurity risk.2 These are not mandated, at the present, with some exceptions for Federal Government purchasing guidelines, witness the prohibition of acquisition of products from certain companies that have been implicated in IP theft or other breaches of trust.

Add Wireless to the mix, and the cracks in the wall of security get wider.

At the present, the European Union is implementing security measures for wireless devices. There have been provisions in the RED for security.

The full legalese of the Article that addresses security is embedded here: RE Directive. Without repeating the full text of the Article, the key elements that industry is (already) considering are under the following Articles:

Article 3.1
- (a) Health and safety
- (b) EMC

Article 3.2 Radio spectrum efficiency

Article 3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(a)-(c): Inter-compatibility/functionality provisions

Until now, most of the work on radio devices looked at the above provisions as it relates to device compliance to the above Articles 3.1 and 3.2(a)-(c).

It's starting to get a little interesting with the following provisions under Article 3.3(d)(e) and (f), here:

Article 3.3 (d): *radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;*

Article 3.3 (e): *radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;*

and

Article 3.3 (f): *radio equipment supports certain features ensuring protection from fraud;*

The above clauses are commonly-viewed as the "cybersecurity clauses" and there is further guidance from the EU forthcoming.

As yet, there are no harmonized standards that have been published to guide evaluations of devices. This leaves the interpretation of these requirements with the Notified Bodies (and others).

However, on 12 January 2022, the EU Com published the Delegated Regulation implementing EU RED Art 3.3 d), e), f) covering Cyber Security.

The legal date is comes into effect is 1 August 2023 with compliance by manufacturers by 1 August 2023 with the pre-amble to the document stating:

"Whereas:

1. *Protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks.*

The regulation specifies that harmonized ENs should be published by 12 June 2023. Full implementation is specified to be before the end of 2024, with some phase-out periods of products already in the pipeline.

Not to exclude other important clauses, they must be mentioned. Notably there is much discussion about Article 3.3(g) that covers access to emergency services (911 in the US, 112 in Europe) and Article 3.3(i) which protects users with disabilities. Finally, Article 3.3(j) which mandates controls on software loaded onto devices that may otherwise compromise the compliance (this Article could be construed as to having cyber-implications as devices are increasingly connected to the Cloud for performance and functional updates and could be compromised in some way).

It must be noted that, like all the European Directives, there are broad performance requirements in these Articles and clauses. It is up to the standards bodies to develop criteria and procedures for these assessments and at the present time, the standards and protocols for assessment of "Cyber-resilience" are largely lacking. This should change soon as schemes get rolled out by the accreditation bodies, specifiers (such as customers and governments) and others in the industry.

The bad guys are busy. The compliance community has a large role in evaluation and helping manufacturers select effective and reasonable protections.

FOR REMOTE PATIENT MONITORING SYSTEMS, WIRELESS COEXISTENCE CAN BE LIFESAVING

Naseef Mahmud
Rohde & Schwarz

The demand for wireless medical applications such as remote patient monitoring, real-time diagnostic analysis, smart surgical systems, and implantable sensors have grown significantly over the last couple of years. Thanks to implanted medical devices, many patients live an almost normal life without having their mobility compromised. Popular implants include cardiac pacemakers, implantable defibrillators, nerve stimulators (functional electrical stimulation, FES), bladder stimulators, implantable infusion pumps, biomonitoring devices such as the capsule endoscope and implantable drug delivery systems. A patient's quality of life is vastly improved by implants using wireless communication; the risk of inflammation and infection, often caused by connecting wires and tubes, is greatly reduced, as well as being much more convenient.

The wireless medical device segment that has seen perhaps the biggest jump in demand in recent years is remote patient monitoring. One of the biggest driver of the soaring demand is a perhaps the pandemic and the due to its nature, healthcare is invariably understaffed with the largest shortages in trained nurses and doctors. Wireless remote patient monitors (WRPM) can augment conventional electrical monitoring devices to help reduce direct contact with individual patients while a doctor can still monitor the vital conditions at all times. WRPM also enable a doctor to monitor multiple patients at the same time remotely, thus freeing up valuable time to attend to the needs of the patients who need immediate attention. Not to mention, WRPM give the patient far greater freedom of mobility by removing the danger of getting entangled with wires. Moving patients between locations while continuing monitoring is also a great deal easier.

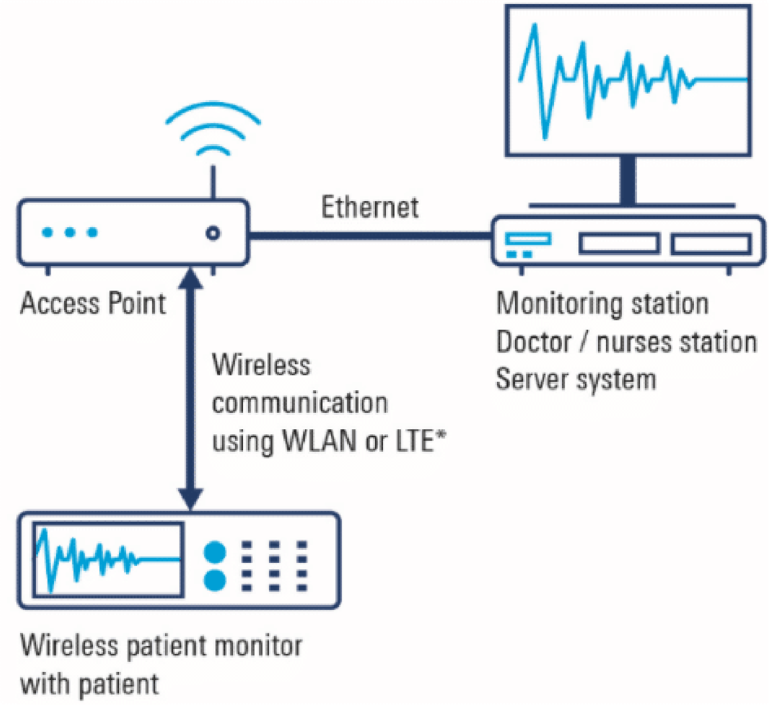
How Do Remote Patient Monitors Transmit Data?

Typically, a wireless medical device utilizes both the 400 MHz MedRadio band and the 2.4 GHz MBAN band. The sensor data and control data is sent back and forth on different frequency bands. Increasingly, state-of-the-art patient medical devices are taking advantage of commercial standardized technologies such as WLAN, Bluetooth®, Zigbee operating in the unlicensed ISM band. In certain applications, depending on the data rate requirements, where mobility is required, LTE or LPWAN (LORA & Sigfox) based implementations are also gaining popularity.

A WRPM gathers the patient's vital signs data (such as body temperature, pulse rate, respiration rate and blood pressure) from wired measurement sensors and then wirelessly transfers the data via the Wi-Fi access point to the health care facility's server system for storage at a central location. Medical personnel can then tap into the patient health status data by accessing it from the relevant server location using a networked connection. *Figure 1* shows the intended WRPM architecture in a hospital environment.

Future versions of WRPM systems will also support Bluetooth®-based vital condition data gathering, which means that the sensors will communicate with the WRPM wirelessly and allow the patient with even more mobility and comfort.

Figure 1: Hospital operating architecture for wireless patient monitoring.



RF Spectrum and Interference

A WRPM is mostly used in a hospital. Nevertheless, there is a broad range of potential use cases that includes elderly care homes, military & defense applications and in some cases even at a patient's home. This means that the devices are subjected to very different environments for Radio Frequency (RF) transmissions. In many day-to-day environments, there is an abundance of wireless electronic gadgets, most of which also operate using licensed and un-licensed technologies such as Bluetooth®, WLAN, cellular mobile radio, etc. Depending on the density of connected devices, the RF environment gets very noisy, particularly since the most data-hungry radio products operate in the ISM unlicensed bands; normally using the 2.4 GHz frequency band.

WRPM is exposed to a variety of RF environments depending not just on the application. If we consider just the hospital application use case, depending on the location of the hospital, the RF environment differs quite a bit as well. A hospital in a big city usually sees more patients, and has more staff members and visitors than one in a rural location. In the big hospital in a city, more people bring in more mobile phones, smart watches, wireless car key fobs, Bluetooth® headphones, and so on. All these devices transmit signals in the same frequency band at which the WRPM also operates. The microwave in the staff kitchen also radiates high levels of RF energy at 2.4 GHz. In addition, there is bound to be a high-powered LTE Base station tower nearby that could also act as an interference source for the WRPM and further complicate the coexistence challenge. Most hospital IT systems prefer to run regular system updates wirelessly in the night since the RF spectrum is relatively “less busy”. Nevertheless, this also acts as an interference source for the WRPM.

What happens if there is a source interfering the communication of the WRPM?

The sources of the interference signals are smartphones, smart watches, smart home appliances, IoT devices(smart tooth brush, smart lights etc), WLAN routers, car doors openers etc, which are running cellular and non-cellular services such as Bluetooth®, WiFi hotspot services etc. Not to forget, medical devices may be also be subjected to intentional jamming attacks.

When there is an interference source operating at the exact same frequency (i.e. overlapping RF interference signals) as that of the WRPM, the data transfer between the WRPM and the server will become slower (i.e the data rate of the transmission will drop). In the extreme worst case, the communication will completely break down and absolutely no data will be transferred. If the interference signal is on an adjacent frequency channel than depending on the power level of the blocker, the data rate will also be lower. A drop in data rate means the monitoring stations does not receive the patient health information instantly but with an added time delay. In the worst case, medical personnel are not informed about life-threatening changes in the vital conditions at all.

What can be done to protect WRPM from interference signals?

Even though LTE is designed with interference mitigation algorithms to identify and avoid blockers, WLAN receivers mostly suffer in the presence of one or multiple blockers. Therefore, the best approach is to design robust receivers with good filtering capabilities. In order to ensure receiver robustness for wireless medical devices in the US, the FDA recommends product compliance according to the **ANSI C63.27** and **AAMI TIR69** standards to ensure minimum performance.

However, technology evolves much faster than standards. It is therefore important in the product development phase to select test methods that future-proof a product for its lifetime. A failing product even a few years after market placement can still hurt the brand reputation and can be subjected to heavy fines and penalties.

Regulatory Requirements for Wireless Remote Patient Monitoring Devices

The ANSI C63.27 specification is the only standard focused towards wireless coexistence testing. It is a mandatory requirement in the US, relevant devices must be complaint according to the guidelines provided in the standard. Canada, the EU and APAC countries do not have any special requirements for medical devices to be specifically wireless coexistence compliant. By the end of 2020, there will be 20 Billion wireless connected products. This means that, with the growing number of wireless products crowding the RF spectrum, hospital authorities have more confidence in products that can demonstrate interference robustness due to compliance to a certified and recognized standard (i.e. the ANSI C63.27 guidelines). All hospital administrators are interested in conformance to guidelines as a way of reducing legal liability in case of product failure that can be traced back to a wireless coexistence issue.

Thorough Testing Will Save Lives

The ANSI C63.27 standard describes wireless coexistence test using four different types of test setup. The most reproducible and realistic way of testing any wireless receiver is by performing radiated over-the-air (OTA) testing inside fully anechoic chambers.

A test plan needs to be generated that takes into consideration the risk assessment analysis for the product based on the intended use case. A product that is categorized as high risk (i.e. in the case of malfunctioning due to a coexistence-related issue, resulting in bodily harm to the patient) needs to be tested using a more sophisticated interference strategy that better simulates real world worst-case conditions. The risk assessment should take into account the wireless technology supported by the device, including the frequency and the exact bands supported as well as channels available on the radio module. The worst-case operating condition needs to be defined for the product itself and a method of evaluating the functional wireless performance (FWP) in both ideal and worst-case operating environment. The risk assessment outcome dictates how stringent the test for compliance needs to be.

The T&M challenges include, firstly, recreating the electro-magnetic environment applicable for the product's intended use while performing coexistence tests to monitor the defined functional wireless performance (FWP) in a controlled measurement area. Secondly, receiver robustness and application level testing for intentional and unintentional frequency jamming using realistic interference signals in a repeatable manner.

Test & Measurement Solution

The ideal solution includes a radio communication tester, which can emulate all the wireless network technologies present in the typical working environment for the device (such as 3G, 4G, 5G, Bluetooth®, WLAN, ZigBee). Such a radio communication tester is an extremely powerful instrument since it can be used to replicate the hospital network, and it gives the user full control over the RF parameter configuration of the intended network. Additionally, it also includes the ability to monitor various functional wireless performance parameters such as data throughput, PER, BLER, as well as track IP packet data flowing through the network. Additionally, it is possible to measure IP security with this device. *Figure 2* shows how a radio communication tester can simulate a commercial access point and replicate a real world network in a controlled testing environment. The baseline FWP is determined in ideal conditions without any interference signals present using this setup.

Depending on the risk categorization of the medical device being tested, the number of interference signals need to be adjusted. For ANSI C63.27 compliance testing, up to three interference signal sources are recommended. However, given the vast number of technologies and the quantity of interference sources (smartphones, smart watches, etc.) around us, it is recommended for R&D labs to test using an even higher number of interference sources, in order to fully characterize the WRPM device performance when the receiver is in a "fully stressed" RF

Figure 2: Replicating the hospital operating environment in the lab

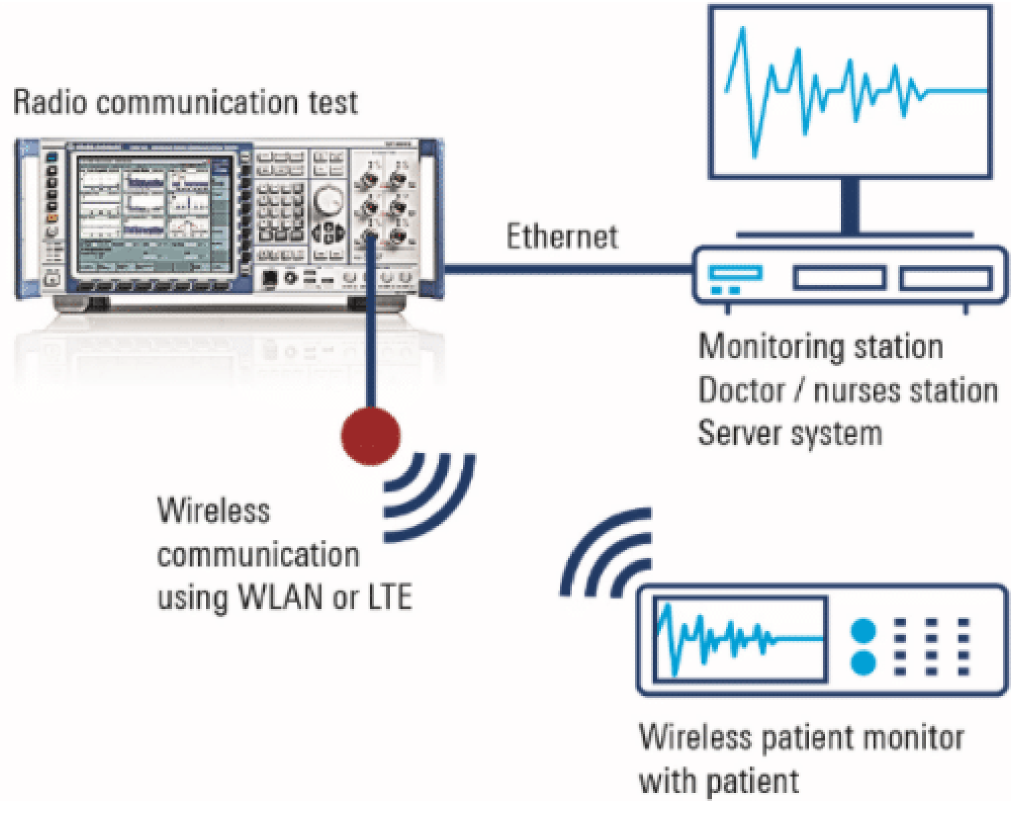
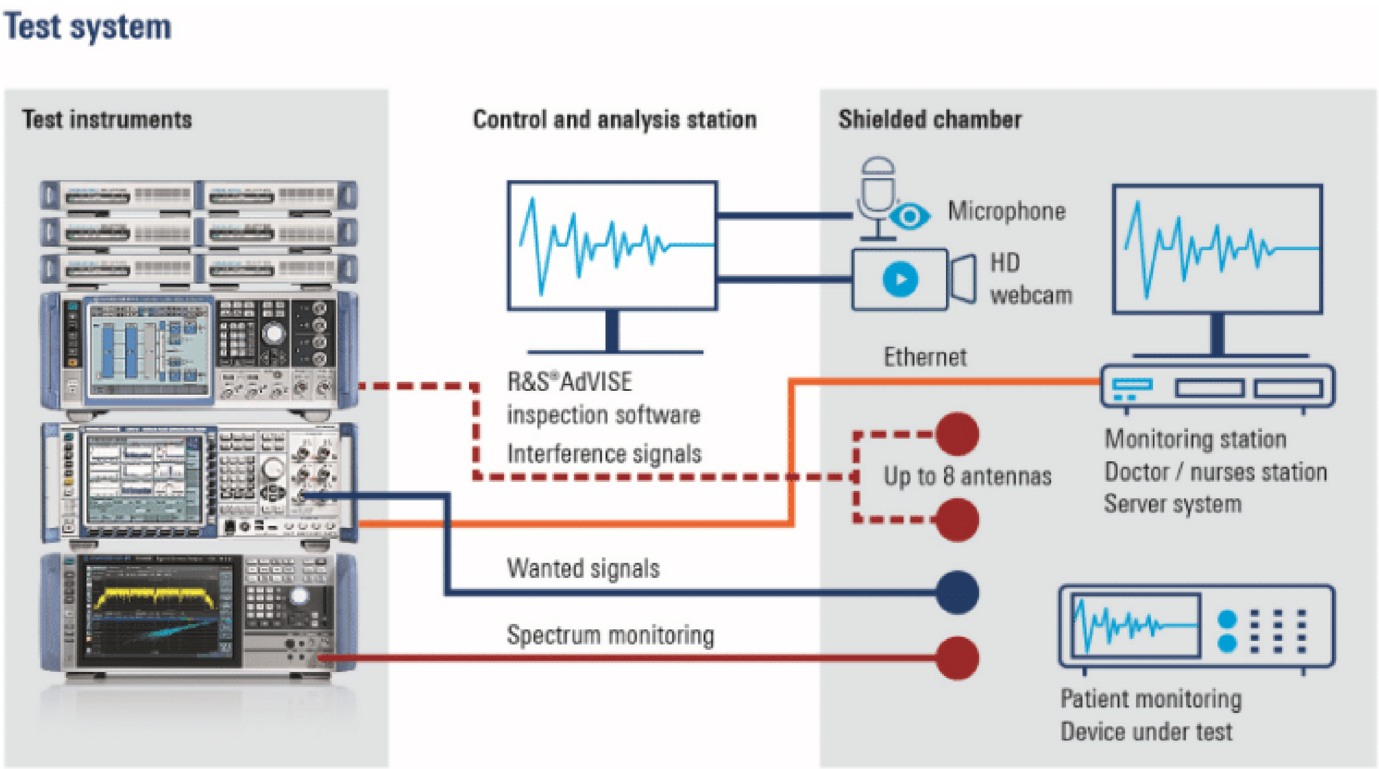


Figure 3: Test setup for performing radiated wireless coexistence testing for wireless remote patient monitoring devices



operating environment. *Figure 3* shows a test setup with an interference station with up to eight fully calibrated interference sources. Vector signal generators are used for generating interference signals, and should be capable of generating wideband-modulated signals, and able to flexibly adjust to the center frequency and the output power level of the unintended signals.

While performing coexistence testing, it is important to monitor the RF spectrum, as is listed as a mandatory step in the standard. A swept-tuned spectrum analyzer is adequate, but in some cases a real-time spectrum analyzer may also be required if very fast digital signals need to be captured. Almost all WRPM come with a display screen and a built-in loudspeaker system as an integral part of the functionality. An inspection software can be used to detect and monitor video and audio related parameters. The inspection software automates the detection process and also removes human errors completely from the display monitoring. *Figure 3* shows the R&S®AdVISE inspection software, a powerful T&M tool that uses any USB based HD webcam and microphone to collect live data in order to monitor audio and video performance.

It needs to be mentioned that additional power amplifiers and high gain directional horn antennas are required in order of boost up the signal level from the device under test as required; for the inspection software to work properly, illumination may also be required. The entire test is performed inside a fully anechoic chamber in order to block out all electromagnetic signals from the surrounding environment and make the coexistence measurement fully controlled and re-reproducible.

A fully compliant product gives its users more confidence. In this modern connected world and with more and more connected products joining the ecosystem every day, we should test medical products today using the RF spectral reality of tomorrow, in order to future proof the wireless performance of a device throughout its life time.

IoT, WIRELESS, 5G EMC STANDARDS

ETSI STANDARDS

https://www.etsi.org

Document Number	Title
ETSI EN 300 220	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1,000 MHz frequency range with power levels ranging up to 500 mW
ETSI EN 300 328	Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
ETSI EN 300 330	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 9 kHz to 25 MHz frequency range and inductive loop systems in the 9 kHz to 30 MHz frequency range
ETSI EN 300 440	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range
ETSI EN 301 489-3	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz
ETSI EN 301 489-17	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for Wideband data and HIPERLAN equipment
ETSI EN 301 893	Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
ETSI EN 303 413	GPS receivers
ETSI EN 303 417	Wireless Power Transfer

IoT, WIRELESS, 5G EMC GROUPS & ORGANIZATIONS

MAJOR WIRELESS/5G/IoT LINKEDIN GROUPS

- Wireless Telecommunications Worldwide
- Cellular, Wireless & Mobile Professionals
- Wireless Communications & Mobile Networks
- 802.11 Wireless Professionals
- Wireless Consultant
- Telecom & Wireless World

MAJOR IoT, WIRELESS, 5G EMC ASSOCIATIONS AND ORGANIZATIONS

APCO International
https://www.apcointl.org
APCO International is the world's oldest and largest organization of public safety communications professionals and supports the largest U.S. membership base of any public safety association. It serves the needs of public safety communications practitioners worldwide–and the welfare of the general public as a whole–by providing complete expertise, professional development, technical assistance, advocacy and outreach.

ATIS
http://www.atis.org
In a rapidly changing industry, innovation needs a home. ATIS is a forum where the information and communications technology (ICT) companies convene to find solutions to their most pressing shared challenges.

Bluetooth Special Interest Group
https://www.bluetooth.com
Join thousands of the world's most innovative companies already developing and influencing Bluetooth technology.

CTIA - The Wireless Association
http://www.ctia.org
CTIA is an international nonprofit membership organization that has represented the wireless communications industry since 1984. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies.

ETSI - European Telecommunications Standards Institute
http://www.etsi.org
We produce globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical, and other areas.

NAB - National Association of Broadcasters
http://nab.org
The National Association of Broadcasters is the voice for the nation's radio and television broadcasters. As the premier trade association for broadcasters, NAB advances the interests of our members in federal government, industry and public affairs; improves the quality and profitability of broadcasting; encourages content and technology innovation; and spotlights the important and unique ways stations serve their communities.

Satellite Industry Association
http://www.sia.org
The Satellite Industry Association (SIA) is a Washington D.C. based trade association representing the leading global satellite operators, service providers, manufacturers, launch services providers, and ground equipment suppliers.

Telecommunications Industry Association
http://www.tiaonline.org
The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industry through standards development, policy initiatives, business opportunities, market intelligence and networking events. With support from hundreds of members, TIA enhances the business environment for companies involved in telecom, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications, and the greening of technology.

IoT, WIRELESS, 5G EMC GROUPS & ORGANIZATIONS (CONTINUED)

Wireless Infrastructure Association (WIA)
http://wia.org
The Wireless Infrastructure Association represents the businesses that develop, build, own, and operate the nation's wireless infrastructure.

Wireless Innovation Forum
http://www.wirelessinnovation.org
WInnForum members are dedicated to advocating for the innovative use of spectrum and advancing radio technologies that support essential or critical communications worldwide. Through events, committee projects, and initiatives the Forum acts as the premier venue for its members to collaborate to achieve these objectives, providing opportunities to network with customers, partners and competitors, educate decision makers, develop, and expand markets, and advance relevant technologies.

WiMax Forum
http://wimaxforum.org
The WiMAX Forum® is an industry-led, not-for-profit organization that certifies and promotes the compatibility and interoperability of broadband wireless products based upon IEEE Standard 802.16. The WiMAX Forum's primary goal is to accelerate the adoption, deployment, and expansion of WiMAX, AeroMACS, and WiGRID technologies across the globe, while facilitating roaming agreements, sharing best practices within our membership and certifying products.

ZigBee Alliance
http://www.zigbee.org
Our innovative standards are custom-designed by industry experts to meet the specific market needs of businesses and consumers. These market leading standards give product manufacturers a straightforward way to help their customers gain greater control of, and even improve, everyday activities.

USEFUL WIRELESS REFERENCES

WIRELESS WORKING GROUPS

802.11 Working Group
The 802.11 Working Group is responsible for developing wireless LAN standards that provide the basis for Wi-Fi.
http://grouper.ieee.org/groups/802/11/

802.15 Working Group
The 802.15 Working Group is responsible for developing wireless PAN standards that provide the basis for Bluetooth and ZigBee.
http://www.ieee802.org/15/

802.16 Working Group
The 802.16 Working Group is responsible for developing wireless MAN standards that provide the basis for WiMAX.
http://grouper.ieee.org/groups/802/16/

Bluetooth SIG
The Bluetooth SIG is responsible for developing wireless PAN specifications.
https://www.bluetooth.com

Cellular Telecommunications and Internet Association (CTIA)
The CTIA represents cellular, personal communication services, mobile radio, and mobile satellite services over wireless WANs for service providers and manufacturers.
http://www.ctia.org

Federal Communications Commission (FCC)
The FCC provides regulatory for RF systems in the U.S.
https://www.fcc.gov

GSM Association
The GSM Association participates in the development of development of the GSM platform–holds the annual 3GSM World Congress.
http://www.gsmworld.com

Wi-Fi Alliance
The Wi-Fi Alliance develops wireless LAN ("Wi-Fi") specifications based on IEEE 802.11 standards and provides compliance testing of Wi-Fi products.
http://www.wi-fi.org

WiMAX Forum
The WiMAX Forum develops wireless MAN standards based on IEEE 802.16 standards and provides compliance testing of WiMAX products.
http://wimaxforum.org

ZigBee Alliance
The ZigBee Alliance develops standards for low-power wireless monitoring and control products.
http://www.zigbee.org

USEFUL WEBSITES

ARRL RFI Information
http://www.arrl.org/radio-frequency-interference-rfi

Jim Brown has several very good articles on RFI, including: A Ham's Guide to RFI, Ferrites, Baluns, and Audio Interfacing.
www.audiosystemsgroup.com

FCC
http://www.fcc.gov

FCC, Interference with Radio, TV and Telephone Signals
http://www.fcc.gov/guides/interference-defining-source

IWCE Urgent Communications
http://urgentcomm.com has multiple articles on RFI

Jackman, Robin, Measure Interference in Crowded Spectrum, Microwaves & RF Magazine, Sept. 2014.
https://www.mwrf.com/technologies/test-measurement-analyzers/article/21845885/measure-interference-in-crowded-spectrum

RFI Services (Marv Loftness) has some good information on RFI hunting techniques
www.rfiservices.com

TJ Nelson, Identifying Source of Radio Interference Around the Home, 10/2007
http://randombio.com/interference.html

USEFUL BOOKS

Interference Technology Engineer's Master (ITEM) 2022
A complete guide full of invaluable EMC directories, standards, formulas, calculators, lists, and "how-to" articles, compiled in easy-to-find formats.
https://learn.interferencetechnology.com/item-2022/

The ARRL RFI Book (3rd edition)
Gruber, Michael
ARRL, 2010.

USEFUL WIRELESS REFERENCES

USEFUL BOOKS (CONTINUED)

AC Power Interference Handbook (2nd edition)
Loftness, Marv
Percival Publishing, 2001.

Transmitter Hunting: Radio Direction Finding Simplified
Moell, Joseph and Curlee, Thomas
TAB Books, 1987.

Interference Handbook
Nelson, William
Radio Publications, 1981.

Electromagnetic Compatibility Engineering
Ott, Henry W.
John Wiley & Sons, 2009.

Platform Interference in Wireless Systems - Models, Measurement, and Mitigation
Slattery, Kevin, and Skinner, Harry
Newnes, 2008.

Spectrum and Network Measurements, (2nd Edition)
Witte, Robert
SciTech Publishing, 2014.

Radio Frequency Interference (RFI) Pocket Guide
Wyatt and Gruber
SciTech Publishing, 2015.

USEFUL FORMULAS AND REFERENCE TABLES

E-Field Levels versus Transmitter Pout			
Pout (W)	**V/m at 1m**	**V/m at 3m**	**V/m at 10m**
1	5.5	1.8	0.6
5	12.3	4.1	1.2
10	17.4	5.8	1.7
25	27.5	9.2	2.8
50	38.9	13.0	3.9
100	55.0	18.3	5.5
1,000	173.9	58.0	17.4

Assuming the antenna gain is numerically 1, or isotropic, and the measurement is in the far field and greater than 100 MHz.

Using Decibels (dB)
The decibel is always a ratio…

- Gain = P_{out}/P_{in}, where P = power
- Gain(dB) = $10\log(P_{out} / P_{in})$, where P = power
- Gain(dB) = $20\log(V_{out}/V_{in})$, where V = voltage
- Gain(dB) = $20\log(I_{out}/I_{in})$, where I = current

Power Ratios
3 dB = double (or half) the power
10 dB = 10X (or /10) the power

Voltage/Current Ratios
6 dB = double (or half) the voltage/current
20 dB - 10X (or /10) the voltage/current
Multiplying power by a factor of 2 corresponds to a 3 dB increase in power. This also corresponds to a 6 dB increase in voltage or current.

Commonly Used Power Ratios (dB)		
Ratio	**Power**	**Voltage or Current**
0.1	-10 dB	-20 dB
0.2	-7.0 dB	-14.0 dB
0.3	-5.2 dB	-10.5 dB
0.5	-3.0 dB	-6.0 dB
1	0 dB	0 dB
2	3.0 dB	6.0 dB
3	4.8 dB	9.5 dB
5	7.0 dB	14.0 dB
7	8.5 dB	16.9 dB
8	9.0 dB	18.1 dB
9	9.5 dB	19.1 dB
10	10 dB	20 dB
20	13.0 dB	26.0 dB
30	14.8 dB	29.5 dB
50	17.0 dB	34.0 dB
100	20 dB	40 dB
1,000	30 dB	60 dB
1,000,000	60 dB	120 dB

Multiplying power by a factor of 10 corresponds to a 10 dB increase in power. Multiplying a voltage or current by 10 is a 20 dB increase. Dividing by a factor of 10 corresponds to a 10 dB reduction in power, or 20 dB for voltage and current.

USEFUL WIRELESS REFERENCES

COMMON WIRELESS FREQUENCY BANDS (LINKS)

GSM Bands:
https://en.wikipedia.org/wiki/GSM_frequency_bands

UMTS Bands:
https://en.wikipedia.org/wiki/UMTS_frequency_bands

LTE Bands:
https://en.wikipedia.org/wiki/LTE_frequency_bands

MMDS:
https://en.wikipedia.org/wiki/Multichannel_Multipoint_Distribution_Service

V Band (40 to 75 GHz):
https://en.wikipedia.org/wiki/V_band

DECT and DECT 6.0
(wireless phones and baby monitors):
https://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications

Comparison of wireless internet standards:
https://en.wikipedia.org/wiki/Comparison_of_mobile_phone_standards

Wi-Fi Protocols (From Intel):
http://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000005725.html

LINKS TO MANUFACTURER'S WHITE PAPERS

VIDEO / Handheld Interference Hunting for Network Operators (Rohde & Schwarz):
https://www.rohde-schwarz.com/us/solutions/wireless-communications/gsm_gprs_edge_evo_vamos/webinars-videos/video-handheld-interference-hunting_229255.html

Interference Hunting With The R&S FSH (Rohde & Schwarz):
https://www.rohde-schwarz.com/us/applications/interference-hunting-with-r-s-fsh-application-note_56280-77764.html

Interference Hunting / Part 1 (Tektronix):
http://www.tek.com/blog/interference-hunting-part-1-4-get-insight-you-need-see-interference-crowded-spectrum

Interference Hunting / Part 2 (Tektronix):
https://in.tek.com/blog/interference-hunting-part-2-4-how-often-interference-happening

Interference Hunting / Part 3 (Tektronix):
http://www.tek.com/blog/interference-hunting-part-3-4-use-mask-search-automatically-discover-when-interference-happenin

Interference Hunting / Part 4 (Tektronix):
https://www.tek.com/blog/interference-hunting-part-4-4-storing-and-sharing-captures-interference-hunter%E2%80%99s-safety-net

INDEX OF ADVERTISERS

Coilcraft Inc.
t: +1-800-322-2645
e: sales@coilcraft.com
w: www.coilcraft.com
pages: 4

LECTRIX
t: (484) 688-0300
e: info@lectrixgroup.com
w: www.lectrixgroup.com
page: 27

Würth Elektronik
t: +49 7942 945 - 0
e: eiSos@we-online.de
w: www.we-online.com
page: 2

XGR Technologies
t: (302) 669-9554
e: sales@xgrtec.com
w: www.xgrtec.com
page: 9

Break the same old pattern.