PRESENTED BY

INTERFERENCE TECHNOLOGY®

2020 IoT, WIRELESS, 5G EMC GUIDE


From the Creators of *Interference Technology*
INTRODUCING
LECTRIX
THERE'S ONLY ONE SPOTLIGHT
ARE YOU IN IT?
Positioning Ambitious B2B Electronics Companies
for Aggressive Growth
www.lectrixgroup.com
PHILADELPHIA, PA | HONG KONG

TABLE OF CONTENTS


ROHDE&SCHWARZ
Make ideas real
Be ahead in 5G.
TURN VISIONS INTO REALITY
The next major step beyond LTE/LTE-Advanced (4G) sets challenging requirements. Rohde&Schwarz is a world leader in all areas of RF and microwave test and measurement equipment. As a technology expert, we have been actively involved in mobile communications since the first generation. We are committed to supporting the wireless communications industry with the solutions needed to investigate, develop and standardize 5G.
Check out our test solutions at https://bit.ly/31OQOmi

INTRODUCTION

Jennifer Arroyo
Editorial Director, *Interference Technology*

The need for communication has never been more important than in 2020. This is the year of virtual birthday parties, meetings, and graduations. The COVID-19 pandemic has forced us out of offices, schools, and daily routines, into our homes, making wireless technology a vital resource. 5G is on its way—in fact, it is already rolled out in some locations—and promises faster speeds and more bandwidth to handle all of the streaming and other applications that we are all using. However, like with most wireless technologies, 5G and IoT are not without issues, particularly concerning EMC.

This new *2020 IoT, Wireless, 5G EMC Guide* from *Interference Technology* offers content and reference materials that center around:

- Proper testing to ensure the functionality of IoT devices and connected electronics
- Mitigating EMI issues in microwave and millimeter-wave devices and systems with simulation software
- Protecting 5G technology and infrastructure

Additionally, we have a reference section with a host of useful information on wireless networks, protocols, frequencies, bands, and organizations.

I also wanted to point out the downloadable EMC guides we've produced over the year that are featured on our homepage. Some of the more popular ones include Testing, Automotive EMC, Military/Aerospace, and EMC Fundamentals.

Cheers,

Jennifer Arroyo
Editorial Director, *Interference Technology*
jennifer@lectrixgroup.com

IoT, WIRELESS, 5G 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 Product/Service							
Manufacturer	Contact Information - URL	Amplifiers	Antennas	Current Probes	Fixed 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
Alaris Antennas	www.alarisantennas.com		X						
Anritsu Company	www.anritsu.com		X					X	X
Avalon Test Equipment Corp	www.avalontest.com	X	X	X		X	X	X	X
CommsAudit	www.commsaudit.com/products/direction-finding		X		X		X		X
Doppler Systems	www.dopsys.com		X		X		X		
The EMC Shop	www.theemcshop.com	X	X	X		X		X	X
F2 Labs	www.f2labs.com							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 Product/Service							
Manufacturer	Contact Information - URL	Amplifiers	Antennas	Current Probes	Fixed DF Systems	Near Field Probes	Portable DF Systems	Pre-Compliance Test	Spectrum Analyzers / Receivers
Keysight Technologies	www.keysight.com/main/home.jspx?cc=US&lc=eng					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/narda/default_en.asp	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.rhothetaamerica.com/index.html				X		X		
Rigol Technologies	www.rigolna.com	X		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
Siglent Technologies	wwwsignlentamerica.com					X		X	X
Signal Hound	www.signalhound.com			X		X		X	X
SPX/TCI	www.spx.com/en/our-businesses/detection-and-measurement/TCI/		X		X		X		X
SteppIR Communication Systems	www.steppir.com		X						
TechComm	www.techcommdf.com		X		X		X		X
Tektronix	www.tek.com					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

ENSURING PERFORMANCE OF CONNECTED HOME ELECTRONIC PRODUCTS

Naseef Mahmud
Application Development at Rohde & Schwarz

ENSURING PERFORMANCE OF CONNECTED HOME ELECTRONIC PRODUCTS

TOWARD A CONNECTED HOME

The title of Bob Dylan's 1964 hit "The Times They Are A-Changin'" certainly holds true for home appliance products. The world of consumer electronics needs to evolve and keep pace with the growing desire of their customers, and play a part in enabling the dream of a truly connected world. The Internet of Things (IoT) trend has finally reached our homes. It has given us remote control and access to any object from any part of the world as long as it is connected to the internet. Wireless speaker systems, thermostats, home security and monitoring systems, domestic robots, smoke/CO detectors, lighting, home energy use monitors, door locks, refrigerators, laundry machines, or water detectors, nowadays come with an integrated wireless communication module supporting some form of WLAN, Zigbee, LPWAN, or Bluetooth® technology.

The additional connectivity features bring along new challenges and compliance requirements. Products failing to satisfy regulatory requirements may incur hefty fines, and, in some countries, may even be subject to a sale stop enforcement. Almost all new connected products come with a display, speaker systems, and apps support for easier user interaction. This gives rise to a new set of security, functionality, and quality assurance challenges.

The connectivity technologies (WLAN, Bluetooth®, etc.) mostly operate on the 2.4 GHz ISM band. In some cases, the frequencies overlap on one another, and create performance degradation. This is what is known in the RF industry as a wireless coexistence problem. Coexistence issues degrade the user experience and since a non-technical user may not understand the source of the problem, they easily blame the product instead. This results in brand defamation.

RESPONSIBILITY FOR TESTING

Most device manufacturers source wireless communication modules and antenna modules from different third-party suppliers, connect the two components together, and integrate them into their products in the end. The individual component suppliers certify their products according to different regulatory norms. The wireless module manufacturers perform in-device coexistence measurements using conducted test methods, but no radiated or over-the-air (OTA) testing with their DUT connected to an integrated antenna system takes place. So, the performance of the complete system is unknown. Similarly, the antenna module suppliers certify the antenna radiation performance and other antenna relevant parameters without having any integrated wireless module from the certification test. In this case, the complete system performance is also unclear.

When the device manufacturer finally connects and integrates the two individual components, a completely new product is created, which has not yet been certified. After integration, depending on mount position of the antenna and the coupling of the antenna with the body of the device, different electromagnetic interference (EMI) signals are picked up from different interference sources that come to or pass by in the vicinity of the device. An interference source of interest is any foreign device that is transmitting RF signal in the adjacent or overlapping frequency bands.

Most device bodies are made of steel or aluminium, which sometimes results in the antenna coupling with the device. Consequently, the radiation pattern also changes from the one certified by the antenna module supplier. Therefore, it is crucial that the device manufacturers test and qualify the device in its final form. This is done through radiated proximity wireless coexistence testing.

THE CHALLENGES OF TESTING CONNECTED DEVICES

To make sure that the end product meets all the described requirements, it has to go through a complex set of tests. These include coexistence and user experience tests that guarantee a high quality of service in real-world use and ensure security and product compliance. These steps are needed to minimize any potential risks before introduction to the market. This process also requires the intended use case of the device under test (DUT) to be defined in order to identify the baseline electromagnetic (EM) environment and the corresponding functional performance of the wanted communication system. As a result, it is possible to define the worst-case RF scenario in the lab in order to recreate it later on for testing purposes.

Let us consider a smart washing machine that is connected to a WLAN network as an example. According to its intended use case, the washing machine is normally located in an area where the EM environment is mostly time invariant and stable. The worst-case scenario occurs when the washing machine is located in an area with very weak WLAN signal, while a smartphone running an active Wi-Fi hotspot and Bluetooth® application, transmitting at maximum power, is placed on top or next to it. What happens if an additional smartwatch is brought to this equation? The test challenge is to recreate this exact EM environment and test conditions inside an anechoic chamber in repeatable manner.

INTERFERENCE SIGNALS

The topic of interference signals is heavily debated among experts in the wireless coexistence testing industry. The target of testing the coexistence is to ensure satisfactory receiver performance of the DUT. This means that we need to find a repeatable test strategy and the correct type of interference signal for testing receivers supporting different type of wireless communication standards.

There are two approaches on how to select the correct type of EMI signal.

Approach 1: The first approach involves performing a complete risk assessment analysis on the DUT capability in terms of technology, frequencies, and bands supported. When this is done, a risk assessment matrix will determine the interference signals and spectral position that is required for the specific DUT.

For example, let us consider a DUT supporting WLAN, Bluetooth®, and LTE (bands 7 and 18). WLAN and Bluetooth® operate on the 2.4 GHz band, LTE band 7 on the downlink operates on the 2.6 GHz band, and LTE band 18 operates on the 860 MHz band. *Table 1* shows the risk assessment matrix for this particular DUT.

	LTE800	LTE2600	WLAN	Bluetooth
LTE800	White	Green	Green	Green
LTE2600	Green	White	Yellow	Yellow
WLAN	Green	Yellow	White	Red
Bluetooth	Green	Yellow	Red	White

Table 1: Risk assessment Matrix (green color represents no risk, yellow is moderate risk and white and red represent extremely risky)

If we consider WLAN as our wanted system, then the interference sources are other Bluetooth® and WLAN transmissions, since they overlap on the frequency spectrum and thus causing the probability of coexistence to be high. In case of the LTE 2.6 GHz transmission, the likelihood of coexistence issues is moderately low since it does not overlap on the 2.4 GHz band and would be considered as moderate risky interference source. Finally, for WLAN, the LTE 800 band transmission is of no risk and thus not considered an interference source.

Approach 2: In this case, we test an individual standard with a common interference signal strategy. The properties of an interference signal that affects the performance and reception quality of the wanted system are EMI signal bandwidth, power level, and spectral position. The modulation technique of the EMI signal does not influence the functional performance of the wanted system, but it is advised to use some kind of QPSK or QAM modulated EMI signals. As a result, the EMI signal of a different bandwidth and power level can be introduced to the wanted band on the spectral positions (center of the band, band edges) as shown in *Figure 1*. These are all in-band positions since the most influence on the wanted system is seen at the in-band EMI positions. Out-of-band EMI positions are also possible, but particle experience shows that most modern receivers have decent filtering capability to filter out the out-of-band interferences.

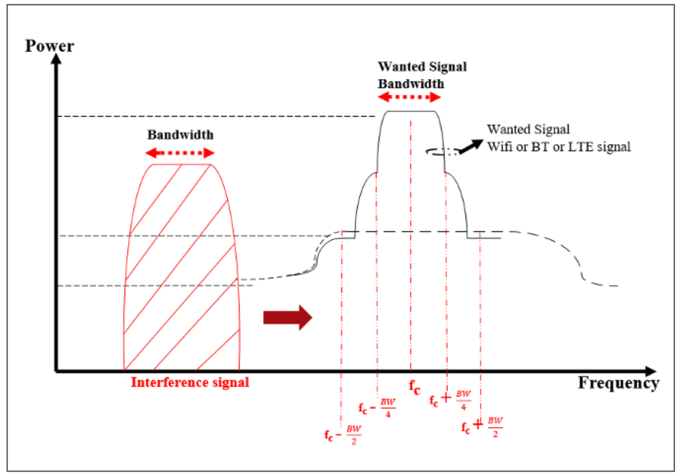


Figure 1: Spectral positions where interference signal is introduced on the wanted band.

WANTED SIGNAL

Wireless communication radios are designed to support the maximum data rate possible. If the RF environment allows, the radio will select the maximum available channel bandwidth and the maximum supported high-order modulation scheme to achieve the maximum data rate. Therefore, when performing coexistence testing, it is necessary to configure the wanted system with the maximum capability that the DUT supports for each standard.

POSSIBLE TEST SOLUTION

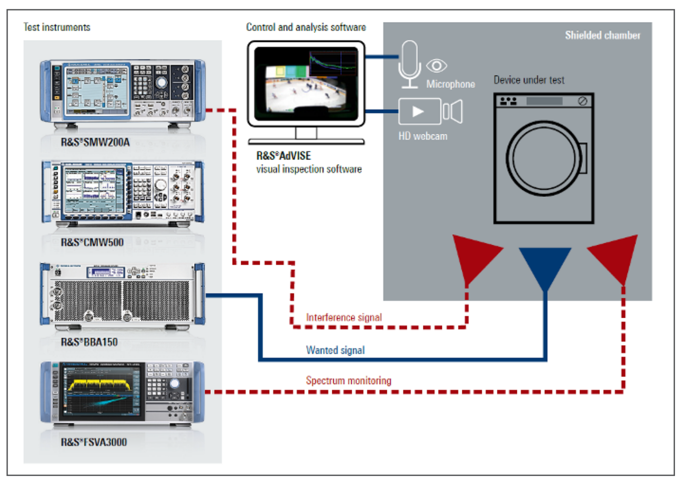


Figure 2: Setup of a possible test solution

A possible test and measurement solution as illustrated in *Figure 2* includes a radio communication tester, a vector signal generator and an optional high-power amplifier, a spectrum analyzer, and a real-time inspection software.

The DUT is placed in a large semi-anechoic chamber. The antenna of the radio communication tester is pointed directly towards the integrated antenna of the DUT. The radio communication tester is used to establish active end to end connection with the DUT by emulating a non-cellular network (such as Bluetooth® and WLAN) as well as a cellular networks (such as 3G, 4G networks) if required. The high-power amplifier is optionally used to boost the signal level in radiated testing condition. A baseline functional performance test is done, and the results for all the relevant physical and application layer KPIs (such as throughput data rate, PER, BLER, video, and audio performance) are recorded.

In the next iteration, the power level of the wanted signal is reduced to the cell edge condition to replicate the worst-case scenario and the interference signal is introduced using the vector signal generator. The vector signal generator is used to generate realistic wideband modulated EM interference signals. It is an extremely powerful instrument that can generate any type of signal at any frequency on the fly. The functional performance in presence of results at this point will show the divergence from the baseline results. While performing coexistence testing, it is important to monitor the RF spectrum, which is listed as mandatory step in most standards. This is done using the spectrum analyzer. Most modern spectrum analyzers can be configured to operate in both real-time spectrum analyzer and a swept-tuned spectrum analyzer mode. Most home automation products these days come preloaded with a display screen and a built-in loudspeaker system. These two features help the users interact with the product. Therefore, it is of immense importance that the functional performance of the application level is also tested in presence of interferences.

The DUT can stream video and audio from the streaming server of the radio communication tester over the WLAN link and an inspection software will perform real-time picture and sound quality analysis. There are specialized solutions on the market that use any USB based HD webcam and microphone to collect live data in order to monitor in real-time the audio and video performance of the DUT. This enables fault events to be recorded and documented automatically on the test report.

TEST RESULTS

Figure 3 shows, the spectral plot of wireless coexistence scenario of a WLAN transmission and a 1 MHz wide EMI Bluetooth® signal in the middle of the wanted band. The WLAN module is connected to the radio communication tester access point (AP) using the IEEE 802.11g 20 MHz channel. The measurement result of WLAN communication with Bluetooth® in band EMI shows an average 15% PER over a transmission of 1,000 packets over the network. The EMI signal is introduced with a power level of -30 dBm.

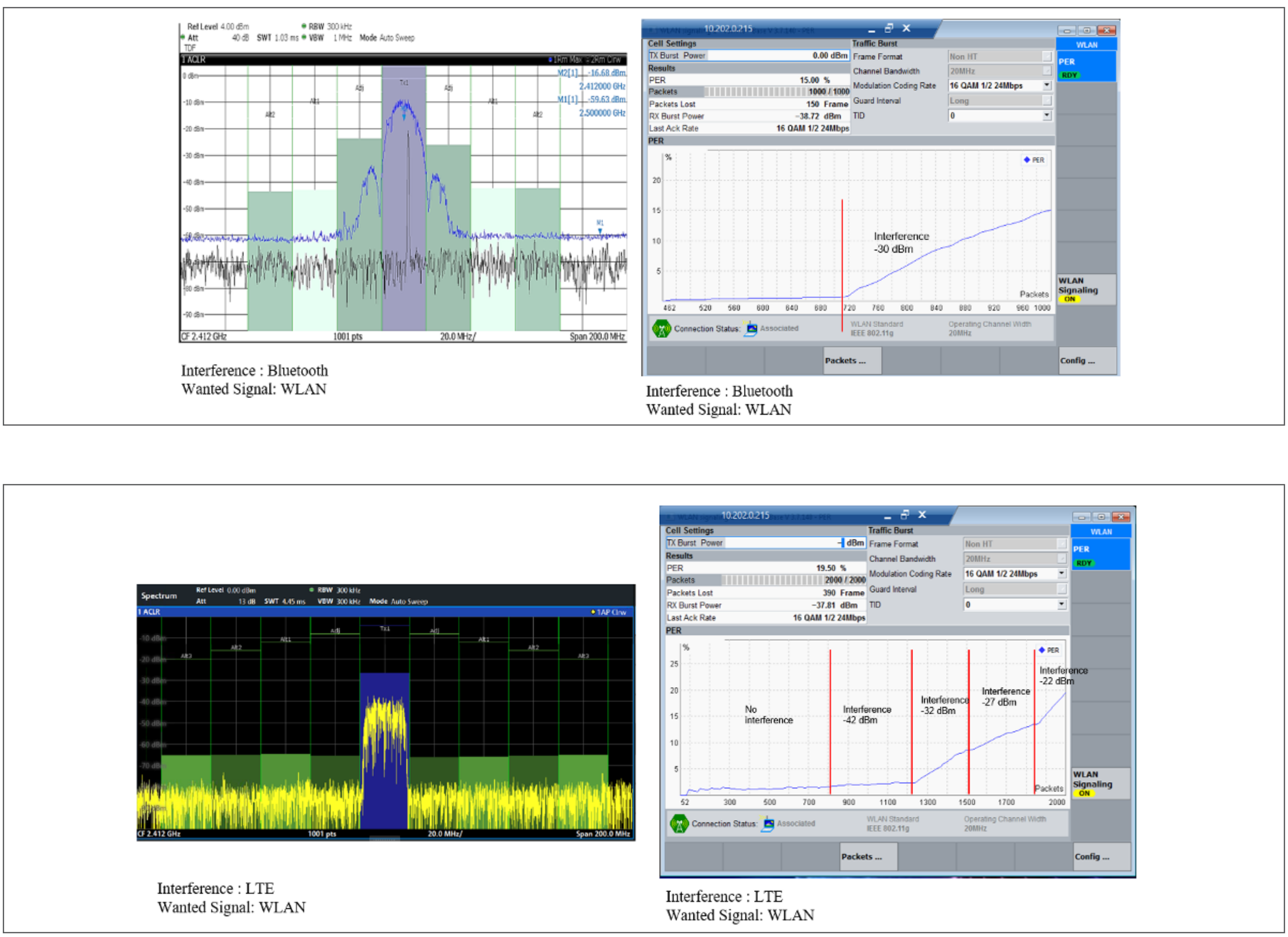


Figure 4: The spectral plot of wireless coexistence and the measurement result of WLAN communication with Bluetooth® in band EMI

Figure 4 shows, the spectral plot of wireless coexistence scenario of a WLAN transmission and a 20 MHz wide EMI LTE signal in the middle of the wanted band. The WLAN module is connected to the radio communication tester AP using the IEEE 802.11g 20 MHz channel. The measurement result of WLAN communication with LTE in band EMI shows an average 19.5% PER over a transmission of 2,000 packets over the network. The EMI signal is introduced with a gradually increasing power level with each increment resulting the PER to increase steeply.

AN INCREASING NEED FOR TESTING

This article describes a systematic approach on how to perform radiated proximity wireless coexistence testing on a product in its final form. Proximity wireless coexistence testing is a new form of testing that is slowly picking pace in popularity. This is because it not only helps manufacturers testing compliance but could also double as an end-of-line functionality test. Most products these days get the latest firmware update before they leave the factory. If there is a wireless coexistence issue hampering the last software update, they might fail to perform once sold to the customer. The call-back, troubleshooting and replacing the product is very expensive. Therefore, a final test just prior to loading it onto the truck would save enormous time and resources for the manufacturer.

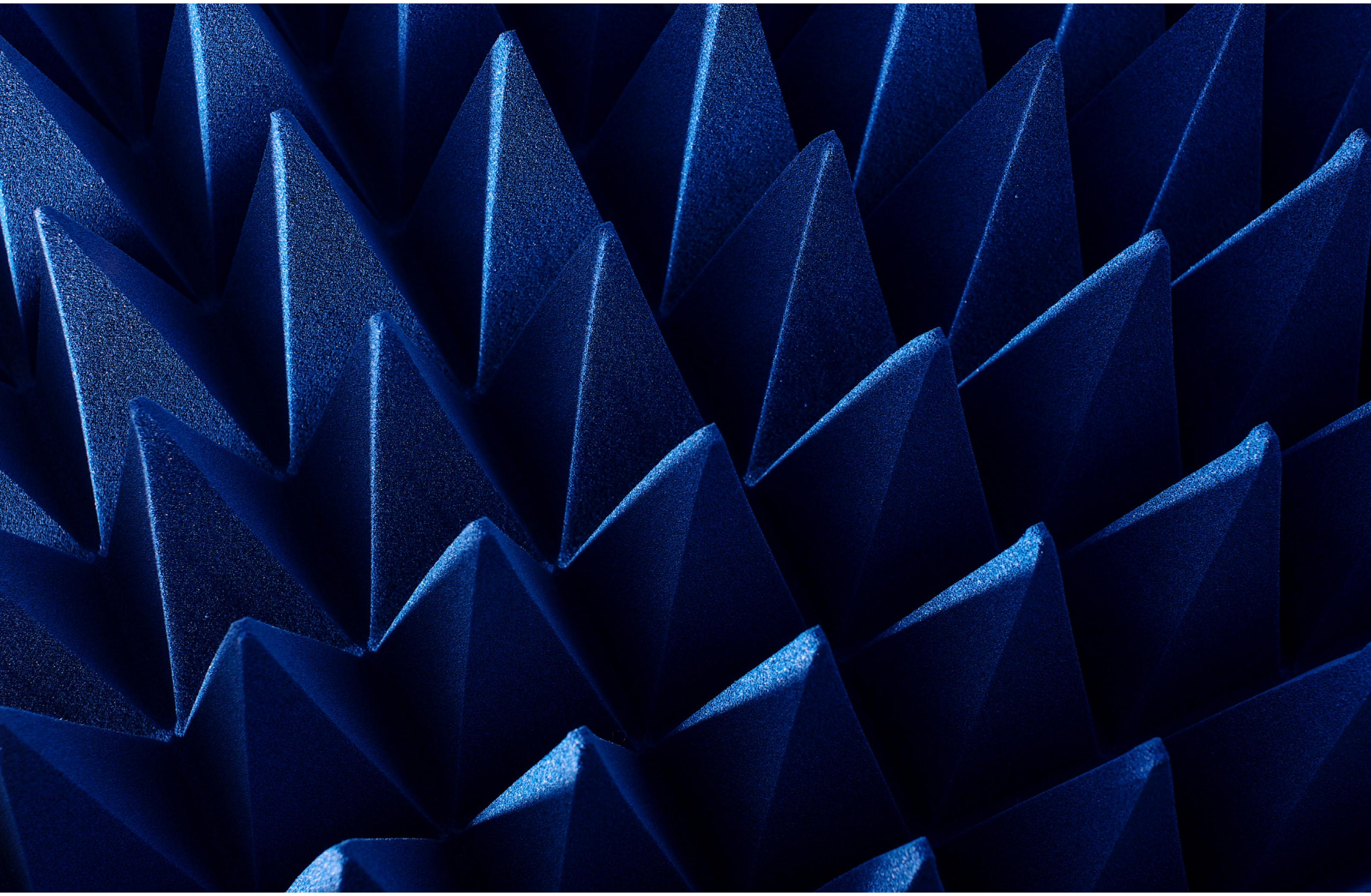
A modified and short open lab wireless coexistence test routine checks for functionality and real-world performance of the product in its intended environment. This gives the device manufacturer an added level of confidence in their product and helps to uphold the brand reputation.

BIO

Naseef Mahmud received his Master's Degree in Electrical, IT, and computer engineering with a focus on communication engineering from the RWTH Aachen University in Germany in 2014. Since then, he has been working as an application development engineer at the test and measurement company, Rohde & Schwarz. In this role, Naseef had the unique opportunity to work with and gain industry insights from some of the biggest companies in multiple industries. He holds multiple patents in the fields of satellite, IoT, and automotive testing. Over the years, Naseef has become a trusted advisor for the topic of over-the-air testing and coexistence testing for Rohde & Schwarz as well as their customers. He also represents Rohde & Schwarz at the REDCA and ANSI C63.27 wireless coexistence work group.

THE VITAL ROLE OF SIMULATION FOR VIRTUAL EMI AND EMC TEST ENVIRONMENTS

Jiyoun Munn
Technical Product Manager, Comsol, Inc.



THE VIRTUAL ROLE OF SIMULATION FOR VIRTUAL EMI AND EMC TEST ENVIRONMENTS

Before deploying microwave and millimeter-wave devices and systems within 5G, the Internet of Things (IoT), and high-speed wireless communication, it is essential to predict their performance. This need has increased the demand for virtual test platforms through simulation software.

High carrier and system bus frequencies are necessary for high-data-rate communication between multiple devices present in such systems. However, increased operational frequencies may induce undesirable and troublesome electromagnetic compatibility (EMC) and electromagnetic interference (EMI) issues, especially when communication is congested. Moreover, the impact from other physics is no longer negligible in mmWave devices. Multiphysics phenomena, such as structural deformation caused by heat expansion, need to be a part of the design consideration as well. Fortunately, a wide range of EMC and EMI scenarios can be virtually emulated and tested without having to elaborately adapt test configurations to real-world environments.

Using electromagnetics simulation software for evaluating device functionality reduces time and costs during the development and production cycle. Virtual evaluations can be performed prior to fabrication, test, and manufacture, and are an important component in reliable quality control processes.

The goal of simulation is to describe the real world as closely as possible on the computer by using proven physics equations. Ideally, the numerical model is used to mimic multiple physical phenomena representing a great variety of operational conditions, which is hard to realize in a lab environment. Accurately analyzing real-world designs and conditions comes at a cost. The more complex the analysis, the more computational resources are needed. Therefore, engineering judgment is used for excluding unnecessary parts from the analysis and for configuring the simulation settings to ensure efficient computations.

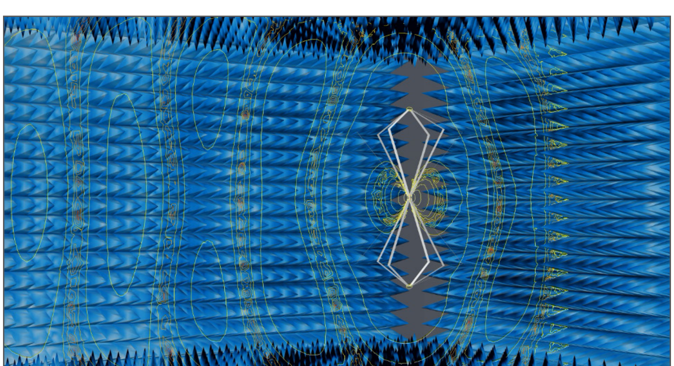


Figure 1: Contour plot of the logarithmic field distribution of a biconical antenna in a fully anechoic chamber.

When evaluating EMI and EMC performance of radiating devices, test engineers often perform measurements in a fully anechoic chamber. Simulation tools are used to set up a numerical environment that can reproduce such tests virtually (*Figure 1*) by using, for example, the finite element method (FEM). For instance, the pyramidal absorbers that are attached to the anechoic chamber walls contain lossy conductive carbon particles. The absorbers attenuate the incident electromagnetic waves gradually with only small amounts of unwanted reflections. For efficiency, instead of modeling the full-sized wall of absorbers, the simulation uses only a single pyramidal unit cell with periodic boundary conditions (*Figure 2*). This is an efficient way of estimating the performance of the complete set of absorbers to make sure the reflectivity is at a minimum. Even if the model consists of just a single unit cell, the periodic boundary conditions make it equivalent to an infinite array of pyramidal absorbers. The effective homogeneous material properties obtained from the unit cell simulation are then used for the entire anechoic chamber wall.

To validate the virtual version of the anechoic chamber, a wideband biconical antenna is placed inside the anechoic chamber. The performance of the antenna (for example, far-field radiation patterns and S-parameters) is computed to validate that there is no degradation of performance due to the incomplete absorber characterization.

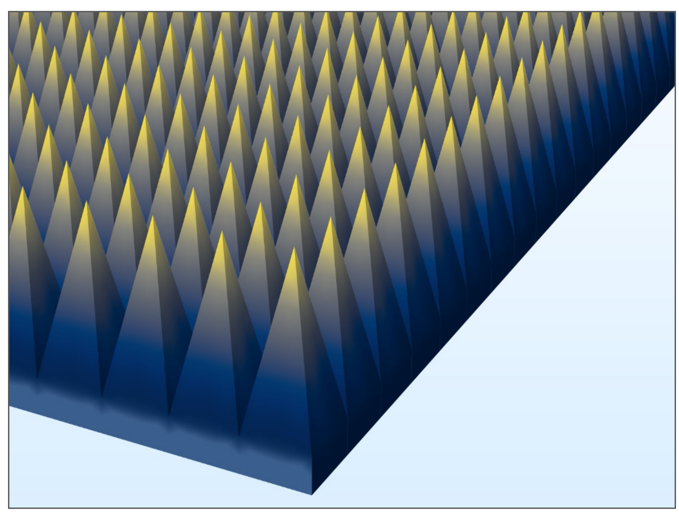


Figure 2: Microwave absorber simulation using Floquet periodic boundary conditions.

Although the real-world representation of the antenna inside the fully anechoic chamber in the simulation is visually quite appealing, as shown in *Figure 1*, its computational cost is unnecessarily high. The simulation can be made much faster and more efficient in terms of memory usage by using a numerical technique that is equivalent to the anechoic chamber walls. Such techniques involve using perfectly matched layer (PML) and absorbing boundary condition features. To efficiently study the near and far fields and other antenna parameters, it is sufficient to place the same biconical antenna in a much smaller surrounding air domain enclosed by a perfectly matched layer (*Figure 3*).

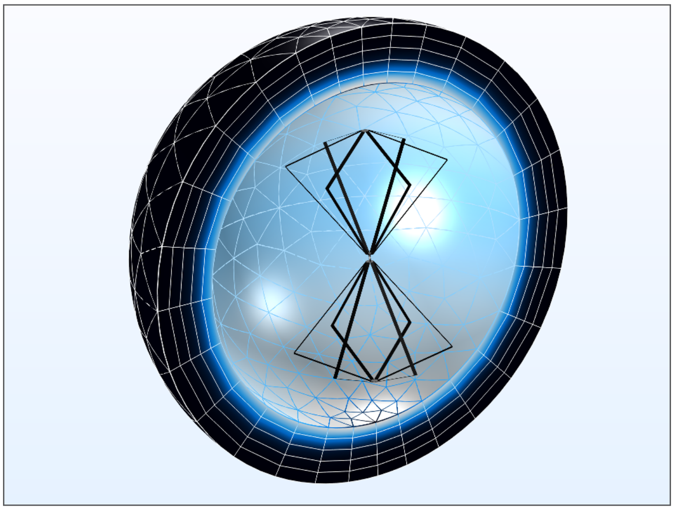


Figure 3: Biconical antenna enclosed by a PML. The PML at the front is removed from view to show the interior.

In order to simulate a large system efficiently, it is crucial to choose proper numerical boundary conditions. In addition, eliminating design details that are deemed to have negligible impact on the results, and just keeping the relevant components, can make further efficiency gains. By using PMLs, a large system can be simulated and not limited to just device-level modeling.

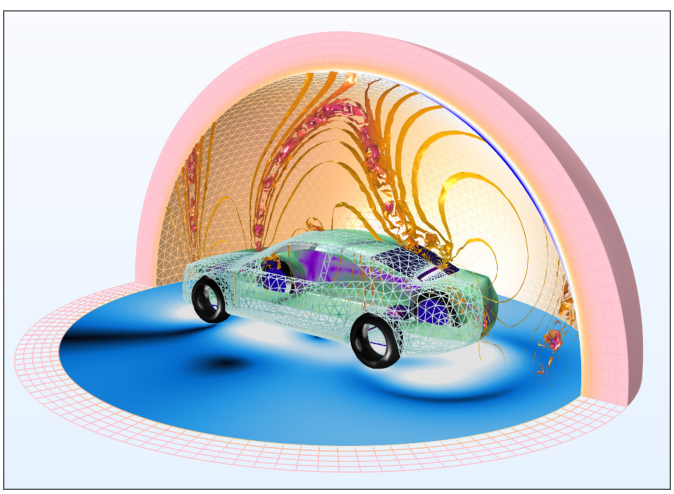


Figure 4: Impact on cable harness by the radiation from the rear windshield in the FM radio frequency band.

In *Figure 4*, the electric field transmitted from a fictitious radiating device on the rear windshield of a car is studied to see the radiated emission effect over the cable harness inside. The PML covers the upper half-space, absorbs all outgoing waves, and ensures that reflected waves do not bounce back onto the car. Meanwhile, the bottom ground and the car body generate reflection and multipath fading effects on the cable harness. The electromagnetic waves coupled to the cable are a source for unwanted conducted emission as well. In a real car system, it would be hard to access and relocate the source and victims for the EMI/EMC test. However, by using simulation, it is possible to analyze arbitrary configurations. In this way, by not being limited by physical testing, engineers can produce more robust system designs.

By using simulation, one can estimate the actual performance of devices for IoT applications when they are deployed in a real environment. IoT devices may be placed in a living room, a garage, or other spaces in a house. The electrical size of the problem in terms of the number of spanned wavelengths can easily exceed what can be addressed by so-called full-wave numerical methods. Full-wave methods include the finite element method (FEM), the finite difference time domain (FDTD) method, and the method of moments (MoM). There are alternative computational electromagnetics approaches available for approximating the performance of IoT devices without sacrificing too much accuracy. In addition, such approximate methods can produce useful results while still using limited computational resources. One such approach is the method of ray tracing. *Figure 5* shows multiscale simulation capabilities when ray tracing is employed together with FEM. The part of the simulation that uses FEM analyzes a small simulation domain surrounding the antenna of a wireless router that includes a truncated surrounding air domain. Rays are launched from the antenna location, and their initial strength is proportional to the directional intensity of the 3D far-field radiation pattern of the antenna. The antenna coverage inside a media room (*Figure 5*) can be approximated quickly without long simulation times or excessive memory usage. This multiscale electromagnetics modeling technique is a great alternative for overcoming the limitations of traditional computation methods for large EMI and EMC problems.

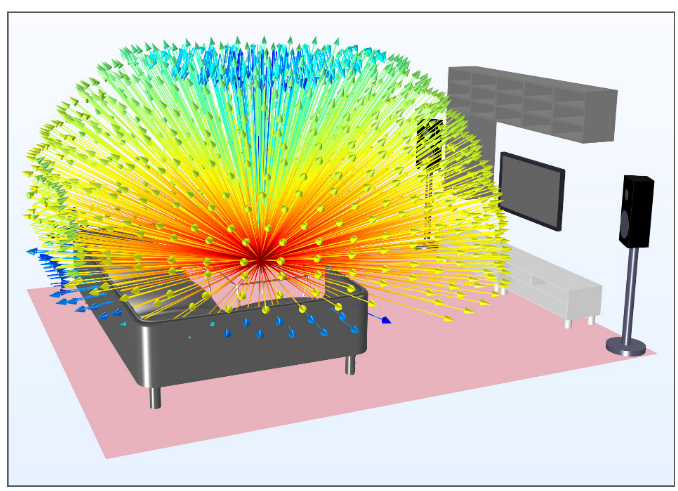


Figure 5: Multiscale electromagnetics simulation example. It combines the conventional finite element method for antenna analysis and ray tracing for describing indoor communication.

Simply combining existing computational methods can overcome the limitations of traditional numerical analysis. Two such situations are when you need to produce wideband results with high-frequency resolution, or when you need to analyze signal integrity and time-domain reflectometry (TDR) for a large device. Such simulations can be very time consuming. However, in both cases, the computational performance can be greatly boosted by conducting a fast Fourier transform (FFT), either from the time domain to the frequency domain or the other way around. For example, you can first perform a transient analysis and then run a time-to-frequency FFT to achieve a wideband S-parameter and far-field calculation in the frequency domain. Alternatively, you can first perform a frequency sweep and then run a frequency-to-time FFT for a time-domain bandpass impulse response. This is useful for time-domain reflectometry analysis, such as identifying a defective part of a transmission line, which results in impedance mismatch and signal quality degradation.

Simulation provides virtual analysis platforms for a wide range of test scenarios. However, learning how to use electromagnetics simulation software may not be the best use of time for everyone in an organization. Limited training and access to simulation software may restrict usage of electromagnetics simulation tools to a small set of expert users. Completed numerical EMI and EMC test models may frequently need new input parameters in order to adjust to a real-world test environment's variations. The need for updating boundary conditions, mesh, and postprocessing settings outside of the simulation group can cause unexpected delays in the development cycle. The good news is that simulation software has evolved to accommodate specialists who are not dedicated simulation engineers. The simulation models can be converted to easy-to-use apps (*Figure 6*). An app has a straightforward, specialized user interface (UI) and can be shared with colleagues and customers through existing web browsers or as a standalone executable file. Such standalone apps do not require purchasing extra software licenses and can run regardless of the operating system. A large number of people involved in EMI test projects can easily access the virtual test kit provided by an app and optimize the product without learning how to use the software behind the curtain.

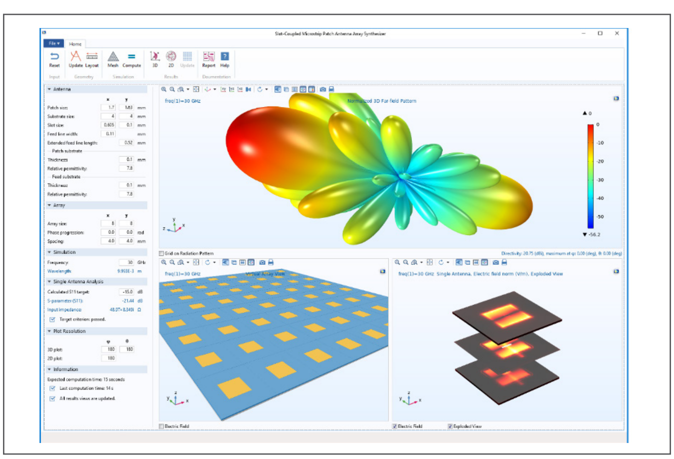
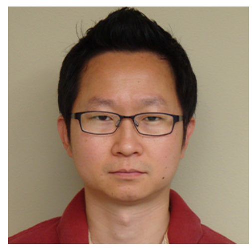


Figure 6: Simulation app for quickly estimating the far-field pattern of a phased array antenna using a full-wave single antenna simulation and array factor.

The variety of simulation tools that support multiple numerical methods within electromagnetics helps engineers and researchers not only to design conventional devices, such as filters, couplers, antennas, and waveguide structures, but also to test EMI and EMC problems in applications for 5G, IoT, and wireless communication. Conventional electromagnetics analyses can be extended to include multiple physical effects using multiphysics simulation. The simulation software industry is also evolving to meet the demands of the fast-paced market for emerging high-speed communication technologies and help more people benefit from simulation.

BIO

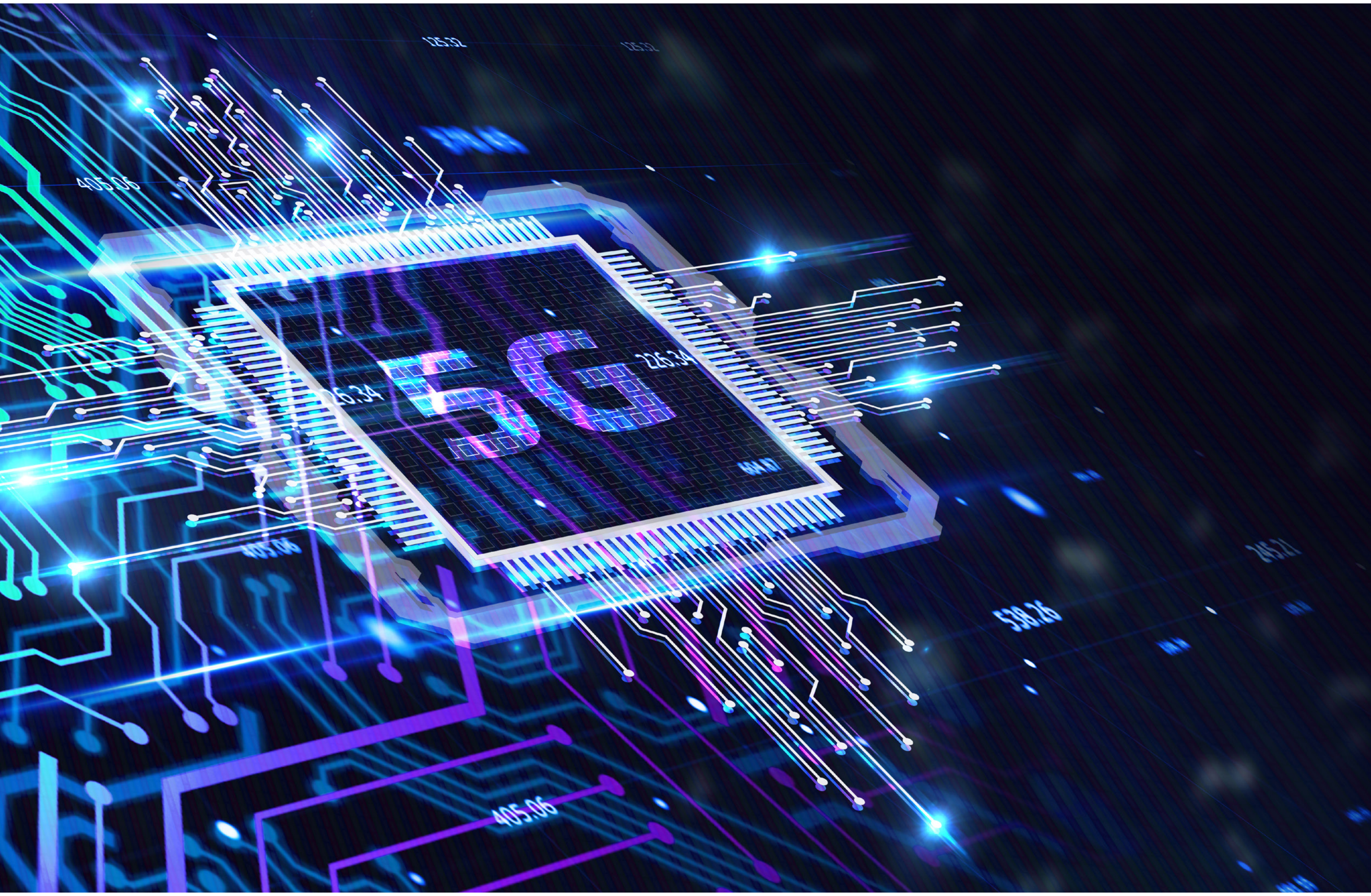


Author: Jiyoun Munn
Title: Technical Product Manager
Email: jiyoun@comsol.com
Mailing Address: COMSOL, Inc.
100 District Ave.
Burlington, MA 01803

Jiyoun Munn is the technical product manager for the RF Module at COMSOL, and a senior member of IEEE. He has two decades of experience in the RF industry, developing more than 150 antenna and microwave device prototypes. Munn also holds patents for antenna interrogation systems. He received his MS degree in electrical engineering from the University of Michigan.

SECURING NEW 5G PHYSICAL ASSETS WITH ELECTRONIC ACCESS CONTROL

Mike Fahy
Commercial Product Manager, Electronic Access Solutions, Southco, Inc.



SECURING NEW 5G PHYSICAL ASSETS WITH ELECTRONIC ACCESS CONTROL

The 5G era of mobile computing and communications is rapidly moving forward. 5G stands for the fifth generation of wireless infrastructure—a massive upscale of network technology. It will provide data transfer rates faster than the blink of an eye, reducing latency for even the most data-hungry applications, high bandwidth and greater opportunities for connectivity and reliability.

Figure 1: With the introduction of 5G, networking equipment, storage and computing hardware, other valuable infrastructure will now be located closer to the end user, increasing the need for advanced physical security.

Within the next four years, global spending on 5G infrastructure will exceed $10 billion. A majority of leading telecommunications providers have committed to launching 5G commercially by 2020. Of the 15 largest providers worldwide, nine have public plans to launch 5G by this date, including all of the major providers in the United States, China, and Japan.

This high-value, cutting-edge, digital cell technology will be woven through and added to our existing physical telecommunications environment. However, it's not just a simple upgrade of existing cellular base stations and antennas.

5G cells are generally referred to as small cell wireless facilities (SWF). They are much smaller than typical enclosures, with dimensions that enable them to attach to walls and streetlight poles—or can even be integrated into the pole itself.

With the introduction of 5G, networking equipment, storage and computing hardware, and other valuable infrastructure will now be located closer to the end user, increasing the need for advanced, physical security.

Electronic access solutions (EAS) provide versatile security for small cells and other 5G equipment, as well as offering an intelligent way to efficiently and comprehensively manage physical access to these systems.

Electronic access systems consist of integrated electromechanical locks and latches that can be used to secure enclosures in remote locations. Networked electronic access control systems provide significant benefits for physical security management, providing simplified credential management, and audit trail monitoring for small cells.

SECURING DISTRIBUTED TECHNOLOGY

Like other utilities, such as cable companies and power companies, telecommunications companies have their equipment installed throughout our urban landscape, in cities and suburban housing developments, commercial and industrial locations, along roads and highways—even the most remote locations.

The physical components of our digital world share two common attributes:

- The remote equipment they deploy is secured in enclosures designed to protect the valuable technology that enables functional wireless networks.
- This remote equipment needs to be accessed by a variety of personnel performing routine maintenance and service tasks.

These enclosures are present throughout our world—ubiquitous and utilitarian; they almost disappear from view unless you are seeking them out.

5G small cells will be adding a whole new denser layer of equipment to our world. At their core, small cells are wireless transmitters and receivers designed to provide greater network capacity in smaller areas. While current high power "macro" towers send signals across an entire city, they lack the ability to support the data running through these networks. Global mobile data traffic will increase seven-fold by 2022 due to the continuing development of Internet of Things (IoT) technology.

As the number of devices connecting to the current networks increases, so does the demand for data. Current network infrastructure might provide coverage to all of these devices, but will lack the wireless density to support fast data transfer—ultimately slowing down devices. This explains why an individual might have full signal but still experience slow connection speeds. This is where small cells come in. Small cells multiply wireless density by only servicing a limited area, reducing the likelihood that a small cell will be overwhelmed. This enables networks to meet the data demands from multiple devices at the same time.

There are two key ways our environment will be affected by the launch 5G SWFs:

- These small cells are about the size of a picnic cooler or mini-fridge, with similar sized antennas.
- To provide the bandwidth and service performance the 5G network is designed to offer, they will typically be installed much closer together, which means there will be many more 5G SWFs installed.

Many of these smaller cells have already been deployed to support 4G network service. And many more will be installed as 5G is rolled out through 2020. Until recently, most small cells secured with a basic physical lock were accessed by a key—one that is easily duplicated, thus presenting a security risk.

These SWFs will need to be routinely accessed by service technicians, sometimes from several different companies or subcontractors. Many telecom enclosures use multiple padlocks with different keys assigned to different vendors, an inefficient and vulnerable method for securing the unit.

Securing these widely dispersed systems is crucial, especially since most are located within reach of the public, are (for the most part) unattended and are at significant risk for vandalism and theft. These enclosures are often targets for thieves seeking valuable materials, such as batteries, copper wire and other electronic components.

One further danger associated with vandalism and theft is downtime. When equipment in these enclosures is damaged due to theft or vandalism, that node on the network goes down. Bringing it back online requires emergency repair dispatch and new components, combined with the costs associated with downtime of any network segment. Investing in more secure locking systems, such as electromechanical locks and latches can save on these significant downtime costs.

Figure 2: Concealed electronic access solutions, like Southco's AC-EM-10 series provide an effective physical security solution for small cell enclosures. The sealed AC-EM-10 features a compact design that takes up minimal application space and facilitates the electronic actuation of mechanical latches.

UPGRADING ENCLOSURE SECURITY

Electronic access solutions provide an effective physical security solution for these new enclosures. Compared to mechanical locks, which must be accessed by a physical key, EAS provides a digital credential that can be easily issued, traced, and even revoked from anywhere in the world.

An electronic access solution is composed of three primary components: an access control reader or input device, an electromechanical lock and a controller for monitoring the status of the access point. When designing an EAS, choosing the appropriate electronic lock for the specific enclosure will provide the intelligence, flexibility, and security needed for the small cell.

The most basic type of electronic access credential is an RFID card, which is widely used in many building management and technician management operations today. Many telecom service providers and the contractor vendors who service them already use RFID cards for accessing central and local offices, data centers, and other operational locations.

Figure 3: Telecom providers are encouraging enclosure manufacturers to incorporate hardware that complements the industrial design of SWFs, like Southco's E6 Constant Torque Positioning Hinge series, which provides superior durability in harsh outdoor environments and improves aesthetics.

Another form of access credential is an electronic PIN code which can be changed on a recurring basis, with different codes assigned to each individual. This makes the credential more personal. The downside is that PINs are easily shared and lost or forgotten, which can complicate maintenance activities and add security risks.

The most secure access credential is one with more than one layer, and is unique to the individual and easily modified through cloud-based systems. For example, an EAS platform that supplies an electronic, time-based key via a mobile app on a technician's smartphone has the following layers of personalization:

- The phone and phone number are unique to the technician. Some smartphones today actually have biometric-type security that uses a thumbprint or facial recognition scans to unlock the phone.
- The smartphone app the technician uses to download the key from the cloud platform is secure and password protected.
- The electronic key loaded to the app is site- and event-specific. It can only be used to open a specific enclosure, and only for a scheduled period of time.

When combined with a robust, secure intelligent electronic lock, these cloud-based access controllers can provide simple solutions for providing time-based access control to 5G small cells.

Audit trails generated by electronic access solutions provide telecom management with an additional resource: They can track when a 5G small cell door is opened in order to monitor maintenance and service activity. If a 5G cell is scheduled for activity that should take an hour, but the audit trail shows the enclosure access panel was open for far longer, management can find out why the delay occurred and exercise better management of service personnel and costs for service.

EAS is a scalable solution that is applicable when needing to add electronic access to a large number of distributed enclosures. Some enclosure manufacturers and end users have a perception that these electronic access solutions require significant hardware, IT investment, and ongoing support. However, there are EAS platforms that can provide secure access and control without having to wire into a network or install additional hardware or software. As a result, electronic access solutions can be used to elevate the physical security of 5G enclosures with minimal cost and complexity.

ON THE POLE—OR IN THE POLE

Many new 5G SWFs will be attached to streetlights and utility poles, as they are already pre-equipped to meet the needs of 5G small cells. They have the proper height (no more than 50 feet), already have power and are often close to telecom fiber-optic lines, which is the backhaul network connectivity for the 5G cells.

At this juncture, most 5G SWFs are boxes attached to the light poles at sufficient height to provide line-of-sight connectivity to the surrounding cells. However, there is a growing trend to adapt the poles themselves as the enclosure. In some cases, this is done by building the enclosure into an ornamental base; in others, the solution is to install equipment up through the length of the pole.

For enclosure manufacturers, this presents an engineering and aesthetic challenge. Many municipalities have zoning regulations defining physical and visual characteristics of street fixtures like poles. These codes (particularly in historic locations, city centers, and commercial locations) set equipment design criteria to minimize the “intrusion” of network equipment into established settings.

The telecom providers seeking to install 5G networks are encouraging enclosure manufactures to design external elements, like access panels, hinges, and latches, to be more attractive by using hardware that’s flush-mounted, concealed, and inconspicuous.

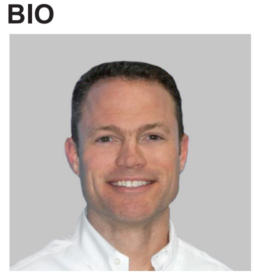
With equipment that is installed within the length of the pole, there may be a need to have two or more access panels tied to different pieces of cell equipment. Enclosure manufacturers can benefit from working with component suppliers who can supply or custom-modify hinges and electromechanical locks to have form factors that satisfy these requirements.

CONCLUSION

5G technology promises a major transformation in the way our networked, mobile computing world operates. Newly emerging concepts such as autonomous vehicles and smart cities will need the bandwidth and millisecond response time 5G offers to move from vision to reality. The IoT will also demand more bandwidth: It’s estimated that there were 8.4 billion connected “things” in 2016, which is expected to grow to 20.4 billion connected elements by 2020.

As 5G equipment is deployed, it needs to be both fully secured and easily accessed on an ongoing basis. Electronic access solutions provide significant benefits for physical security management, providing simplified credential management and audit trail monitoring. By using EAS platforms to better secure these enclosures, valuable, and sensitive equipment can be better protected, and maintaining and servicing the equipment protected by these enclosures can be managed with efficiency, flexibility, and maximum security.

BIO



Mike Fahy is Commercial Product Manager for Southco’s Electronic Access Solutions (EAS) division. He has over 27 years of experience working in various roles supporting Southco around the world. Fahy focuses on solutions for data center rack level security, from self-contained to fully-networked access control systems. He holds a Bachelors in Mechanical Engineering from Drexel University and is a member of AFCOM.

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
- Wireless and Telecom Industry Network
- 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) 2020
An exhaustive 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-2020/

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

Compliance Worldwide
357 Main Street
Sandown, NH 03873

t: (603) 887-3903
e: sales@complianceworldwide.com
w: www.complianceworldwide.com

EMC LIVE™ 2020
IoT, Wireless, 5G EMC
Online Event
September 1, 2020

t: (484) 688-0300
e: graham@lectrixgroup.com
w: www.emc.live
page: 29

F2 Labs
16740 Peters Rd
Middlefield, OH 44062

t: (440) 632-5541
e: sales@f2labs.com
w: www.f2labs.com
page: 8

Interference Technology
Call For Authors & Contributors

t: (484) 688-0300
e: graham@lectrixgroup.com
w: www.interferencetechnology.com
page: 18

LECTRIX
1000 Germantown Pike
Plymouth Meeting, PA 19462

t: (484) 688-0300
e: graham@lectrixgroup.com
w: www.lectrixgroup.com
page: 2

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

t: (888) 837-8772
w: www.rohde-schwarz.com
page: 4