

NIST Technical Note 1885

Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure

Galen Koepke
William Young
John Ladbury
Jason Coder

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.TN.1885>

NIST Technical Note 1885

Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure

Galen Koepke
William Young
John Ladbury
Jason Coder.

*Communications Technology Laboratory
RF Technology Division*

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.TN.1885>

July 2015



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Technical Note 1885
Natl. Inst. Stand. Technol. Tech. Note 1885, 58 pages (July 2015)
CODEN: NTNOEF

This publication is available free of charge from: <http://dx.doi.org/10.6028/NIST.TN.1885>

Contents

Introduction.....	1
Background.....	2
1. Interference and Coexistence Concerns for Wireless	4
1.1 Smart Grid.....	4
1.2 Other Industries and Agencies	5
1.3 Interference Case Study	6
2. Characterizing Complex Wireless Environments and Signals	7
2.1 The Need and Value of Characterizing Complex Environments.....	7
2.2 Generic Test Waveforms vs. Actual Radiated Digital Waveforms	13
3. Interference and Coexistence Test Methods	15
3.1 Essential Criteria for Effective Test Methods.....	15
3.2 Technical Challenges to Effective Testing	17
3.2.1 Traditional EMC Testing	17
3.2.2 Choice of Measurement Facility.....	18
3.2.3 Test Signal Selection.....	21
3.2.4 In-band vs. Out-of-Band Interference.....	22
3.2.5 Choice of Bandwidth	23
3.2.6 Definition of “Failure”	25
4. Future Research	26
5. Conclusions.....	28
Acknowledgments.....	28
References	28
Appendix A. Standardization Activities for EMC and Coexistence.....	32
Appendix B. LTE Interference to Cable TV	38
Appendix C. EM Field Measurements and Antenna Characteristics	50

Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure

Galen Koepke, William Young, John Ladbury, Jason Coder.

National Institute of Standards and Technology
Communications Technology Laboratory
RF Technology Division
325 Broadway, Boulder, CO 80305

Abstract

We examine interference and coexistence testing issues, test methods, and the need to update and develop new test methodologies related to the use of wireless devices in critical infrastructure systems. A case study on interference is presented along with measurements of the ambient electromagnetic environment near banks of electricity meters in a high-rise apartment building. We discuss the challenges to characterizing complex electromagnetic environments, emulating these environments in the laboratory, and designing test methods that adequately evaluate the ability of a device to perform in that environment. We also discuss current electromagnetic compatibility and coexistence standards, and suggest future research that is needed to update or develop interference and coexistence test methods for wireless devices and systems.

Key Words:

anechoic chamber, coexistence, digital modulation, electromagnetic compatibility, electromagnetic environment, health care, interference, public safety, reverberation chamber, shared spectrum, signal bandwidth, smart grid, standards, test facility, test methods, wireless.

Introduction

Advanced wireless systems have revolutionized how people communicate with each other to the point where most of the earth's population now uses cellular mobile phones and other wireless devices [1, 2]. This explosive growth in wireless systems is also happening to machine-to-machine communications with predictions that as many as 50 billion devices will be connected by the year 2020 [3, 4], with wireless being the preferred communications technology. Many of these devices will be part of larger "smart" systems that provide computation and data communication to support critical infrastructure such as health care, emergency response, traffic management, and electric power [5]. While these systems offer great opportunities, there exist associated technical

challenges. When multiple wireless transmitters are in close proximity to each other and to other electronic systems the possibility of interference and coexistence¹ problems is increased significantly, especially when the devices attempt to share the same frequency bands. Also, the advance of communications and wireless technology is moving at a much faster pace than the development of interference and coexistence test standards and measurement metrics. In this Technical Note we will examine test methods and current standards related to electromagnetic compatibility (EMC) with applications to wireless interference and coexistence. We will also discuss possible issues with traditional test methods, and suggest new areas of research and standards development to address some of the evolving interference and coexistence issues.

Background

EMC is the ability of a device or system to operate in a manner that it both functions acceptably within the surrounding electromagnetic (EM) environment and will not cause detrimental interference to its neighbors (a more detailed definition is given in [6]). When we apply this concept to most electronic devices it implies that there is sufficient immunity to the effects of external signals or noise, and that electromagnetic emissions are well controlled. This can usually be accomplished by proper circuit design including the addition of filtering and shielding as needed. However, the trend toward lower voltage, more power efficient and densely packed electronics, along with the ever-present desire to reduce costs, can have an impact on the immunity to electromagnetic interference (EMI). The addition of a radio transceiver and antenna can further increase the possibility of interference both from internally generated signals, as well as external signals or noise detected by the antenna and coupled into the device. Maintaining EMC has also become more challenging as the density of wireless (radio) communications systems increases and these systems occupy more of the electromagnetic spectrum.

Coexistence is a natural outgrowth of interference and EMC. Coexistence concerns are driven by the increase in the use of wireless technology to connect critical equipment, the higher density of sensitive equipment (e.g., health care facilities) and the intensive use of unlicensed or shared spectrum. The combination of these factors, plus how carefully EMC and coexistence are considered, can have a direct impact on the performance and reliability of electronic systems. This is especially important in critical systems that directly affect safety, security, and the well-being of society. These include defense, transportation, communications, health care, public safety, electric power (Smart Grid), and other major infrastructure systems.

¹ Coexistence implies measuring the mutual interaction between multiple communications systems simultaneously. Interference is focused on only the impacted system and may cause both communication and basic operation disruptions.

A very necessary tool to increase the probability that systems will operate reliably in the increasingly complex electromagnetic environment is the development and application of EMC and coexistence standards. These standards and associated tests should be based on and adequately emulate actual and anticipated EM environments and use scenarios. The current arsenal of test methods should be reevaluated in the context of these more complex environments and signals.

Today's radio (wireless) systems have different EMC testing requirements compared to general electronic devices due to the characteristics of the systems, historical EM environments, and regulatory requirements. The EMC tests (immunity to radio frequency signals and noise) for wireless devices exclude testing near communications frequencies [7] (which assume these frequencies are protected and licensed), while immunity to these frequencies is a necessary test for other devices [8]. As these wireless and other electronic systems are merged into a single device or collocated in the same environment, the EMC test procedures may need to be revised, particularly if the device uses shared spectrum. The challenge is to test for compatibility when the wireless link is integral to the functionality of the device and while the communications functions are active.

Coexistence is a topic that is covered in multiple communication standards, with [9]-[13] serving as examples. These standards deal with various aspects of coexistence. For example, [9] discusses how to analyze and report on the coexistence problem in a communication network. Reference [10] provides some analysis and best practice suggestions for coexistence between two specific protocols, namely IEEE Std. 802.15.1-2002 [14] for wireless personal area networks (WPAN) and IEEE Std. 802.11b-1999 [15] for wireless local area networks (WLAN). Approaches to coexistence in the TV white space spectrum are discussed in [11] and [12] which focus on managing potential coexistence problems in industrial networks.

The coexistence solutions in [9]-[12] range from protocol design to consideration of network topology. However, as is typical in the current state of wireless standards, none of the aforementioned standards describes or recommends how to perform a coexistence test. Reference [13] provides coexistence/interference testing specifically for cellular communications and WiFi® technologies on a single device. However, other on-device RF technologies such as Bluetooth® are omitted from testing and intentionally disabled during the test. Thus, this testing approach is easily generalized to multiple devices and communication technologies. Of particular interest to this work are the impacts and testing at the physical layer (radio) which are not included as part of these standards. While the analysis and best practices put forth are useful, the crucial testing step is absent. A robust testing protocol for coexistence is necessary to provide verification that a wireless device and/or communication system can perform critical functions in the presence of multiple users with different technologies in the same spectrum. Of equal importance in coexistence testing is how much impact the device-under-test (DUT) or system-under-test (SUT) causes to other users of the spectrum.

A brief summary of EMC standards for radiated interference, as well as communications standards that discuss interference mitigation, and some ongoing standards work on coexistence is given in Appendix A.

1. Interference and Coexistence Concerns for Wireless

1.1 Smart Grid

A traditional concern for radio frequency (RF) communication systems is the presence of other unwanted communication or RF signals either in-band or near-band (typically categorized as adjacent bands). In a licensed frequency band, all signals other than the licensed user of the spectrum are considered interference (or RF noise). However, when the spectrum is shared, the nature of interference is not as clear. While transmitter parameters for both licensed and unlicensed spectrum are regulated by the US Federal Communications Commission (FCC), the restrictions for the unlicensed band are such that users can comply with FCC regulations *and* potentially interfere with other communication systems in the same unlicensed spectrum. An example of this is two wireless technologies that use the same Industrial, Scientific, and Medical (ISM) spectrum in the same local geographic area. While both may be able to connect to their associated user devices, the signal-to-noise-plus-interference ratio (SNIR) may degrade the performance of both systems. Thus, neither system is considered as causing “harmful” RF interference, although the applications that require the wireless connectivity may be adversely affected by the reduction in data throughput.

In the case of smart grid, both interference and coexistence are important. At first glance, the interference concerns are fairly obvious. Basically, any intended RF transmission or unintended RF emission that disrupts the communication of the wireless devices used in smart grid is a potential problem. However, in real-world deployments, the interfering signal may have a variable time dependence, and the bandwidth of the interfering signal may change over time as well. Individual devices will react differently to different waveforms, e.g., an amplitude modulated (AM), narrowband signal may cause less disruption than a wideband direct sequence spread spectrum (DSSS). Thus, realistic interference testing requires a more complex waveform than a continuous wave or simple amplitude-modulated signal. If the interference testing is to occur in or near the communication band of the device, the accurate representation of real-world interference signals becomes critical because the communication port provides a low-resistance path to the inner electronics of the device.

Coexistence becomes a concern when the smart grid communication technologies utilize shared spectrum. An example of likely spectrum sharing occurs in the use of the 900 MHz and 2.4 GHz ISM bands. This includes technologies such as wireless networking IEEE 802.11b [15] and low-rate wireless personal area networks IEEE 802.15.4 [16]. To effectively evaluate smart grid

technologies for coexistence behavior, we need to consider the emerging area of coexistence metrology. Even though most critical smart grid applications (e.g., control commands, metering information) are likely of relatively small length compared to other typical wireless user traffic, the protocol overhead and communication system architecture warrant the coexistence evaluation of wireless technologies. As vendors and municipalities seek to utilize the low-cost technologies offered for the shared, unlicensed spectrum, appropriate testing of those products should include coexistence evaluation.

Development and updates of standards, test methods, and metrics for interference/coexistence in smart grid and other critical systems is a key focus of this report. For a good discussion on the potential smart grid wireless technologies, architectural features, deployment configurations and data transactions that could lead to possible interference and coexistence problems see NIST internal report NISTIR 7761 [17].

1.2 Other Industries and Agencies

While this work centers on interference and coexistence issues related to smart grid, other industries are also facing similar challenges. Much like the smart grid initiative, smart manufacturing seeks to utilize modern information systems to optimize productivity and flexibility in production. Robots and sensor networks in a manufacturing facility are more cost effective and flexible to deploy if communications do not require traditional Ethernet or fiber optic cables. The combination of flexibility and cost benefits points to wireless communications as one of the key enabling technologies, and as a consequence, the problems of interference and coexistence surface.

Healthcare is another industry where a rapid rise in the use of wireless communication systems is leading to interference and coexistence concerns. The number of medical instruments with integrated wireless communication capabilities is driving efforts within the Association for the Advancement of Medical Instrumentation (AAMI), in concert with American National Standards Institute, Accredited Standards Committee C63 (ANSI ASC C63), to standardize coexistence test methods. A primary goal is to ensure that the sharing of the unlicensed ISM bands does not negatively impact patient care.

Finally, the emergency response community is also concerned with interference and coexistence. Many of the new products that aid emergency personnel rely on shared frequency bands, both licensed and unlicensed. Technologies such as RF personal alert safety systems (RF PASS) and wireless connectivity between components on the body, e.g., wireless microphones on face plates connecting to the land mobile radio, utilize a wireless link that is susceptible to both interference and coexistence problems. Much like smart grid, the average usage of the communication link over a period of time may be quite small, say less than 10% of the time, but the timeliness of the

messages is critical. The data must be transferred within a short time duration, on the order of seconds in many cases.

1.3 Interference Case Study

Those concerned with critical infrastructure are not the only industries looking at the problem of coexistence and EMC in a modern communications environment. Recently, Cable Television Laboratories, Inc. (CableLabs) [18], a research and development consortium within the cable television/communication industry, was also concerned with the issue of radiated networks interfering with their conducted (cable) communications. Though not strictly “critical infrastructure,” the situation of the cable industry is analogous to the situation developing in the electric power industry as it moves to a smart grid. Both industries have billions of dollars invested in an established infrastructure and are now facing a new challenge: the modern RF environment. In addition, both industries are working to take advantage of the revolution in wireless devices.

NIST worked with CableLabs to help design a series of experiments with the goal of understanding the risk of interference between a radiated network (in this case, cellular telephone 4G/LTE²) and their conducted (cable) network including distribution equipment, in-home hardware, and cabling [19]. All of the active hardware we tested had first been tested by use of IEC 61000-4-3 [8], which utilizes an 80 % modulated, 1 kHz AM signal. However, to examine the specific risk posed by LTE, the test signal was a 10 MHz wide LTE signal filled with simulated data to mimic an upstream signal from a mobile device.

The test results summarized in Appendix B show that the general risk of interference is very low and specific circumstances need to prevail in order for the interference to be observed: the equipment needs to operate in a channel that overlaps the LTE band and said LTE band must be heavily utilized by a mobile device within a few meters of the set-top box. The vast majority of cable equipment tested was only found to be susceptible to radiated signals that exceeded the legal limit for mobile phones.

As discussed in Appendix B and [19], this measurement is no longer a straight-forward radiated immunity test. Several difficulties arise from the introduction of a complex device-under-test (DUT) (e.g., a set-top box or “STB”) and a broadband radiated signal. Most notable are the definition of when the DUT “fails” and how to define and measure the radiated electric field.

The lessons learned from these experiments may benefit others interested in testing their devices’ susceptibility to radiated broadband modulated signals. Because there are so many variables in

² 4G/LTE, “Fourth Generation/Long Term Evolution”, LTE is the project name of the Third Generation Partnership Project (3GPP) and an evolution of the universal mobile telephone system (UMTS).

the test, standardization is essential to enable results from different laboratories and different products to be compared with each other.

2. Characterizing Complex Wireless Environments and Signals

2.1 The Need and Value of Characterizing Complex Environments

One of the key aspects of interference or coexistence testing is the ability to represent accurately the electromagnetic environment where the devices or communication system will be deployed. In order to decide on quantities such as appropriate interference power levels and duty cycles, ambient background spectra should be measured in representative locations of deployment. When collecting ambient data, several factors need to be considered in the frequency, time, and spatial domains. For example, how fine a frequency resolution is needed across the captured bands, what is an appropriate time sampling interval, and where are the best locations to capture the time samples of the frequency spectrum. The characteristics and configuration of the instrumentation and the transfer functions of field monitoring antennas or sensors (see Appendix C) must also be considered. These determining factors are influenced by both the expected signals in the ambient environment and the DUT.

Measurement of these fundamental parameters requires tradeoffs such as frequency step size and range versus number of captures per minute. The goal is to obtain a detailed enough picture of the environment to create meaningful interference and coexistence tests. Research is needed to determine bounds on these tradeoffs. In addition, after the field data are collected, the subsequent process must draw out the key features that support useful interference and coexistence testing.

As an example of the type of data needed, the results for RF power level captures in an apartment building closet, containing a bank of power meters, is shown in Figure 1. These results show the RF power level associated with various percentiles as a function of frequency. The power level at the 25th percentile means that 25 % of the measured power levels were equal to or less than that level for that particular frequency. The 50th percentile level means 50 % of the measured power levels were equal to or less than that level, and so on. Results such as these can provide an estimate of realistic interference power levels as a function of time, but additional data and analysis are need to obtain a better understanding of the evolving nature of the electromagnetic environment.

The percentiles in Figure 1 are based on the aggregate or total data collected over a 24 hour period. During the data collection process, the data were collected in 2 hour bins so that results for 2 hour blocks of time could be compared to the full 24 hour data set and between each other. For example, it is useful to compare the 2 hour results with the greatest levels of activity with the 2 hour results with the least amount of activity. This will provide insight into how much (or little) the activity levels change over the course of the day. Simply looking at the 24 hour result will not provide

insight into changes during the 24 hour period. Two examples of comparison over 2 hour windows are shown in Figures 2 and 3, and discussed below in more detail.

Figure 2 shows an example of further refinement in the data processing, which focuses on the temporal aspect of the data. First, the 24 hour data are subdivided into 2 hour intervals and then the cumulative distribution value for the 50 % levels for each 2 hour interval is determined. The difference between the minimum 50 % level and maximum 50 % level per frequency is then calculated. This provides insight into how much the 50 % level changes over a 24 hour period based on 2 hour segments. For example, between 746.5 MHz to 755.5 MHz, the minimum to maximum change is 10 dB or greater. In contrast, between 755.5 MHz and 770 MHz the 50 % power level is nearly the same for any of the 2 hour blocks. Thus, an interference test covering between 746.5 MHz and 755.5 MHz will likely require a greater amount of variation with respect to time than between 755.5 MHz and 770 MHz to accurately represent the real electromagnetic environment.

These two examples of data processing start to give a clearer picture of the complexities involved with interference and coexistence testing. While we can readily assume the maximum power measured at a particular frequency to be the “worst case scenario”, as has been a common approach in interference testing, the optimal or shared usage of the spectrum requires a time-of-usage or duty cycle consideration. The example provided here based on the 2 hour time intervals needs further refinement since most data transfers take place on order of milliseconds. Thus, multiple duty cycles may be required in the interference and coexistence testing.

Similarly, the determination of the maximum power is problematic in that the measurement takes place at a particular location by use of a particular set of measurement equipment. Figure 3 shows the same 2 hour window data analysis results as in Figure 2, but for a mechanical room on the top of the building (Floor 13). While at first glance the results between 746.5 MHz to 755.5 MHz look quite similar, the difference is 3 dB to 5 dB higher in the mechanical room versus the closet with the bank of power meters (Figure 2). Clearly, data from multiple locations are required to create a general picture of the electromagnetic interference and coexistence environment.

Ideally, data are collected at many locations in a consistent manner. One way to facilitate such data collection is to deploy low-cost technologies that are calibrated with respect to more sophisticated, metrology grade equipment. Today, software-defined radio technologies allow a great amount of flexibility for spectrum analysis at relatively low cost. In addition, inexpensive modules for laptop computers also support some spectrum analysis capabilities in key shared spectrum such as the 2.4 GHz and 5 GHz ISM bands. If these devices are calibrated in a quality rf test chamber against metrology grade technology, such as a spectrum analyzer, a distributed network of such devices could be assembled to provide a much more detailed and accurate picture of the electromagnetic environment. In the case of smart grid, the extent of the environment could be an apartment building, factory, a power plant or substation, etc.

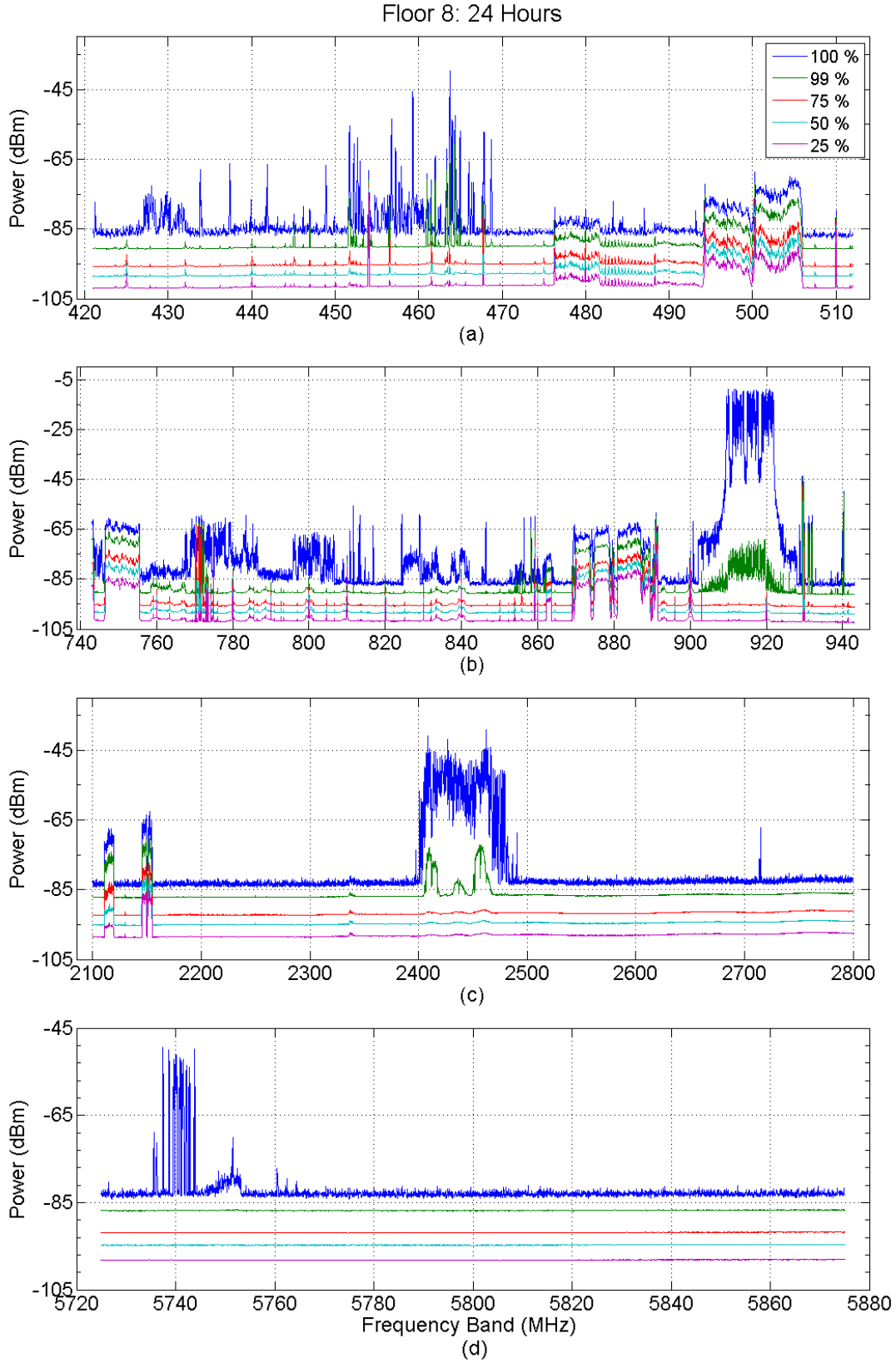


Figure 1. Cumulative distribution for five percentiles in four frequency bands. The data were collected in a utility closet containing a bank of power meters over a 24 hour period.

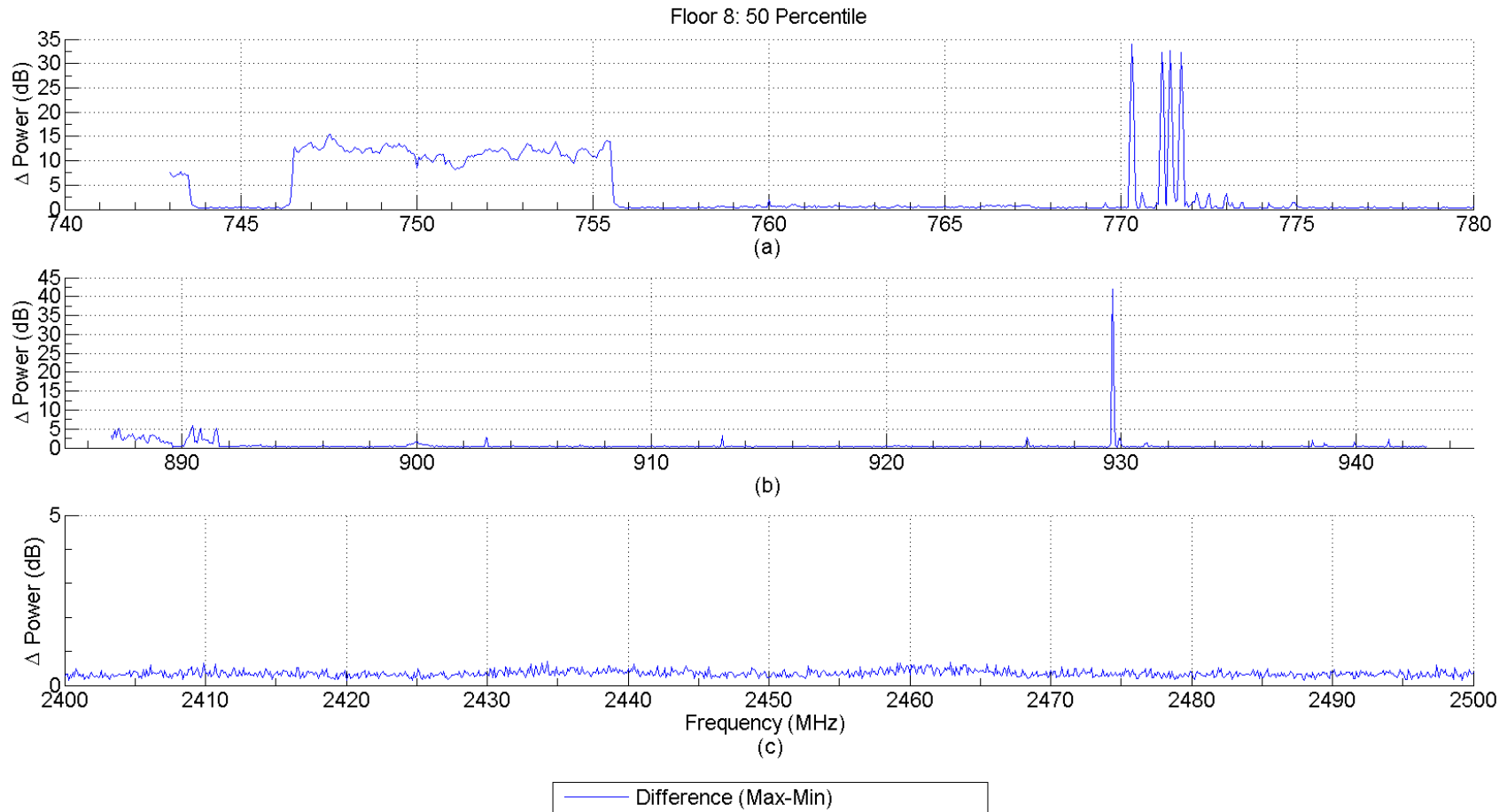


Figure 2. The difference between the maximum and the minimum 50 % level for 2 hour blocks of the 24 hour period, i.e., the 24 hours is subdivided into 2 hour sections and the 50 % power level is determined, then the difference between maximum and minimum 50 % levels are computed. The data were collected in a utility closet containing a bank of power meters over a 24 hour period.

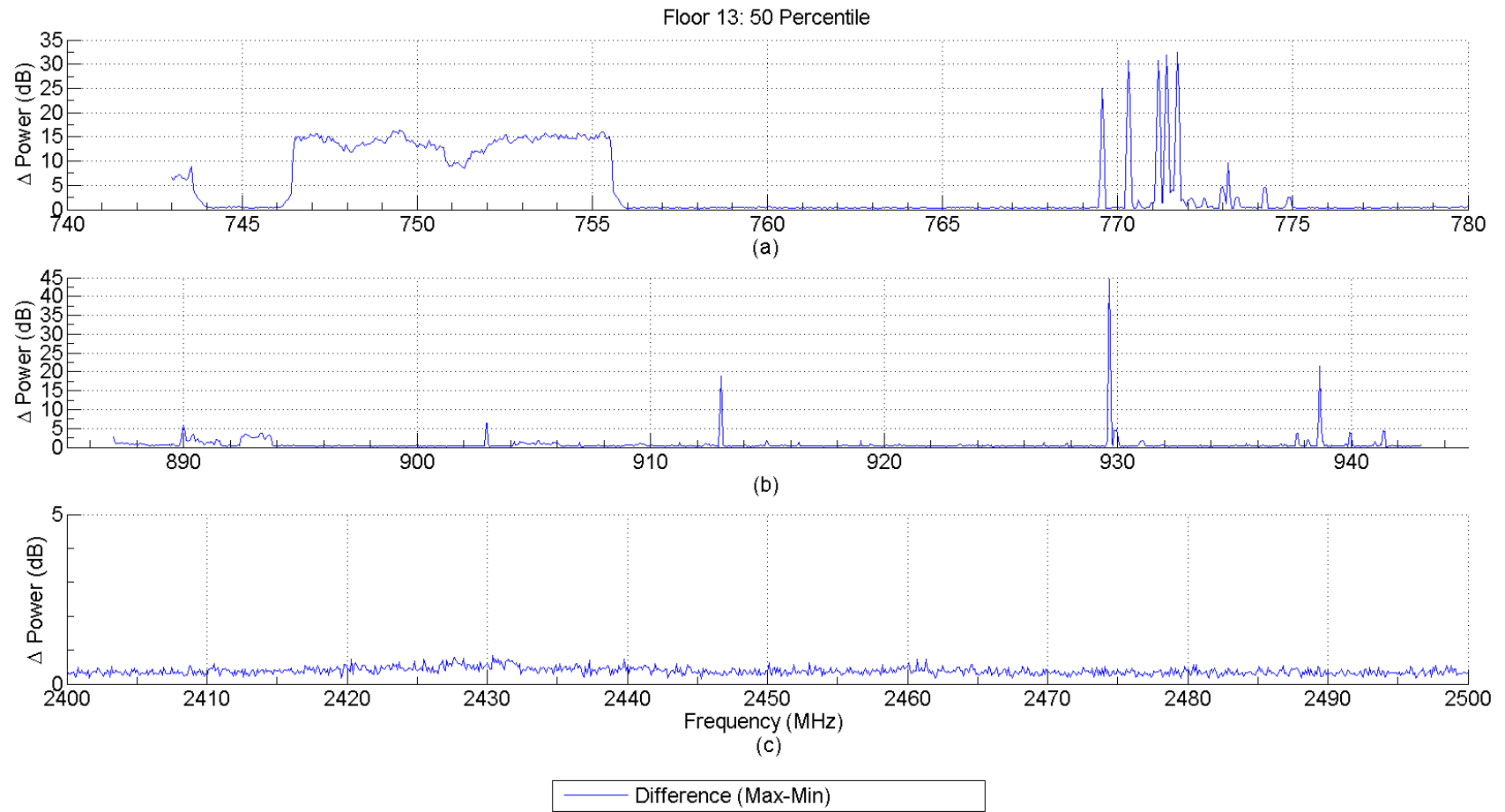


Figure 3. The difference between the maximum and the minimum 50 % level for 2 hour blocks of the 24 hour period, i.e., the 24 hours is subdivided into 2 hour sections and the 50 % power level is determined, then the difference between maximum and minimum 50 % levels are computed. These data were collected in a mechanical room that would be a likely location for smart grid technology.

2.2 Generic Test Waveforms vs. Actual Radiated Digital Waveforms

The ability to characterize and then emulate a particular electromagnetic environment in the laboratory is one important part of developing representative EMC and coexistence tests. Another component of the test method is to emulate accurately the possible interfering signal characteristics. The current paradigm is to use continuous wave (CW) amplitude-modulated (80% and 1.0 kHz) signals for general EMC immunity tests (IEC 61000-4-3 [8]). The ETSI RF immunity tests for telecommunications equipment (ETSI EN 301 489-1 V1.8.1-2008-4, Section 9.2.2 [7]) are also based on the IEC 61000-4-3 test signal but with exclusion bands (a range of frequencies including and surrounding the operating frequency excluded from the immunity test). The CW signal with 80%, 1.0 kHz amplitude modulation may be an adequate test signal if the interference source has similar narrowband characteristics, however with the introduction of complex modulations and proliferation of transmitters, this simple model may not be sufficient. The following discussion highlights some examples where choosing a different interference waveform may lead to more representative EMC or coexistence evaluations.

Figure 4 compares the spectrum of several different modulation formats. The included spectrums are a “victim” 20 MHz WLAN signal, a CW, 80% AM at 1 kHz interference waveform, and a Bluetooth® interference signal. A partial spectrum for an interfering WLAN signal is also shown. Figure 5 shows an expanded view of the 8 MHz centered on the Bluetooth® and AM CW carrier. As is obvious in these two figures, the spectrum is significantly different for each of these four waveforms.

A key question is whether or not the particular waveforms (or technology) cause a difference in the interference or coexistence behaviors as experienced by the victim node. In Figure 6, the error vector magnitude (EVM) [20] is plotted as a function of the orthogonal frequency-division multiplexing (OFDM) subcarriers of the victim WLAN signal. The EVM provides a measure of the quality of the signal constellation, that is, how far the symbol is from the correct constellation point after the receiver demodulation. Notice that the AM modulation generally exhibits the least impact in terms of the number of subcarriers affected and the resulting magnitude of the EVM. Thus, this AM signal may not adequately test a systems ability to perform in the presence of in-band interference. This topic will be discussed further in Section 3.2.3.

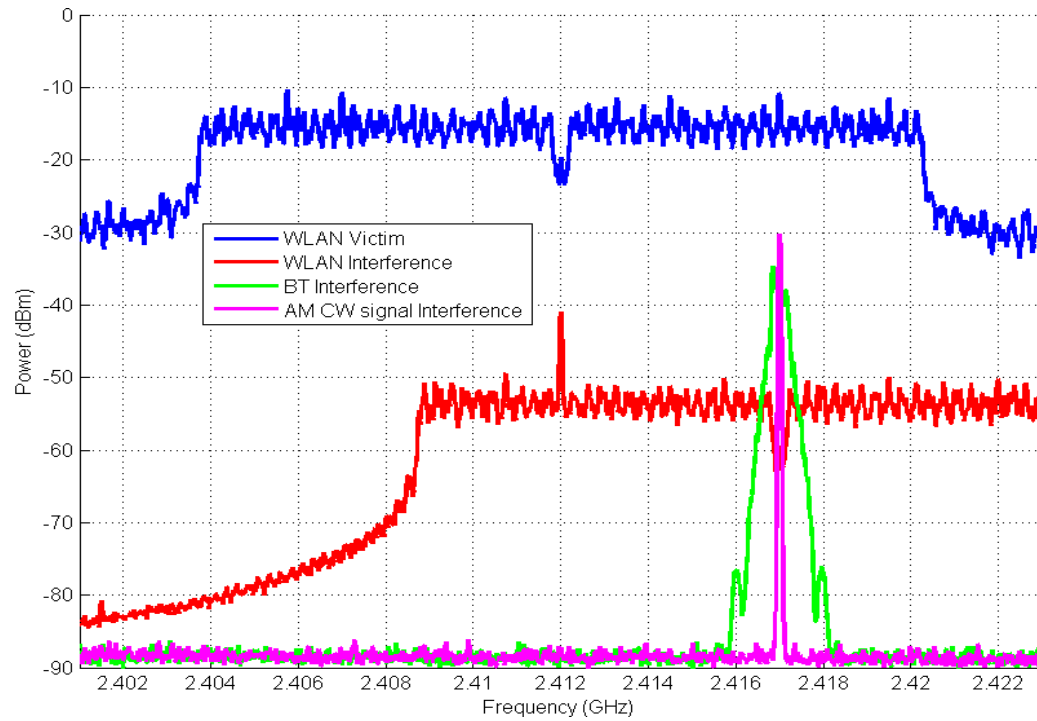


Figure 4. Spectrum created by different modulation schemes and communication technologies. BT = Bluetooth®; WLAN = Wireless Local Area Network; AM CW = Amplitude Modulated Continuous Wave



Figure 5. 8 MHz of the spectrum centered on the carrier frequency of the Bluetooth® and AM interference signals.

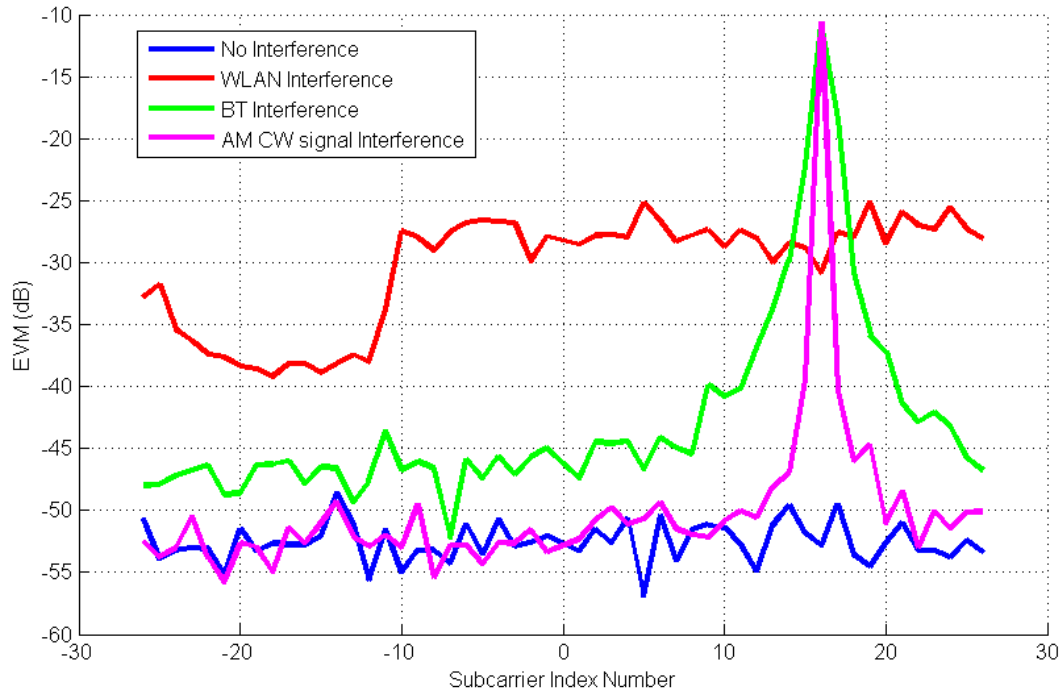


Figure 6. EVM as a function of the OFDM subcarrier index for the WLAN victim versus the interfering technologies.

3. Interference and Coexistence Test Methods

3.1 Essential Criteria for Effective Test Methods

One of the key aspects of effective test methods is how well the test reflects the intended deployment environment. With respect to EMC tests, this requires a detailed knowledge of the environment. Field measurements at targeted facilities will provide baseline power levels and spectrum activity over time that will support the development of general test waveforms.

In the laboratory setting, the impact of various waveforms can be captured over time. For example, Figure 7 shows a spectrogram of a WLAN signal with an interfering Bluetooth® signal. The Bluetooth® interference takes place in bursts; this particular case is centered on 2.41 GHz. This type of representation allows the investigation of the time evolution of the interference. Research needs to be done on the time evolution of the interfering signal that a device will experience in the field, as well as what useful waveforms can be reproduced in the laboratory. The ability to accurately replicate the field results will be a critical component in the development of relevant laboratory tests.

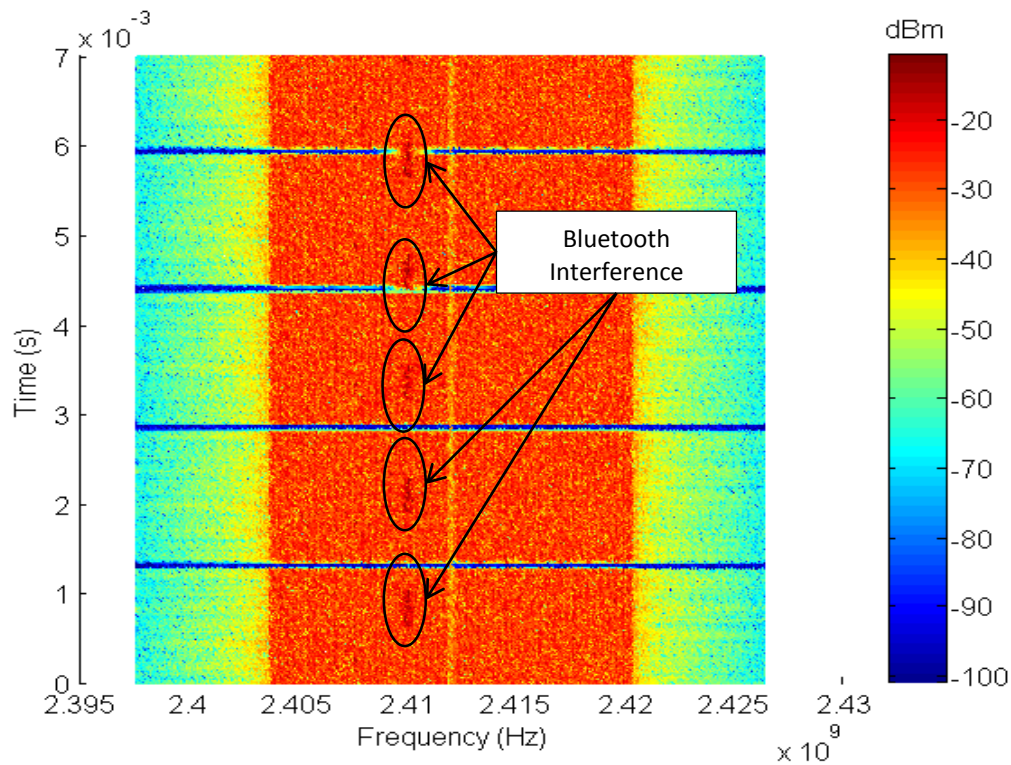


Figure 7. Spectrogram of WLAN victim signal and Bluetooth® interfering signal.

Several considerations arise when considering either new or refined tests for EM interference or coexistence.

- a) Test methods should be radiated in order to have the highest chance of correlation with real-world conditions. This will require calibration of the test environment. In the case of electromagnetic reverberation chambers, this will require calibration of dielectrically loaded chambers in order to create an environment that emulates the real-world.
- b) Testing will likely require the establishment and maintenance of a communication link as part of the test construct, which is a departure from traditional EMC tests. This also means that the testing environment will require isolation between the base station/controller and the DUT. Thus, multiple chambers may be needed as the shielding of a single chamber may not be sufficient. These setups may include any combination of reverberation and anechoic chambers. Important considerations are the accurate emulation of the real-world, and the feasibility and ease of completing tests that involve multiple chambers.
- c) The test methods will need to be correlated with current and anticipated real-world conditions. Field measurements of the RF communication activity in key locations will allow for the extraction of key RF parameters. Investigation into the most effective means

of capturing the RF communication activity is required. For example, several low-sophistication, distributed spectrum analyzers (e.g., smart phone application) may provide insight in the activity of a larger physical area, whereas a highly-sophisticated analyzer may provide in-depth and detailed results for a small subset of locations.

3.2 Technical Challenges to Effective Testing

Establishing a metrology program to evaluate interference and coexistence of wireless systems, including comprehensive test procedures, creates many challenges. These include characterizing both ambient and test fields, determining which signal parameters must be specified, selecting appropriate measurement facilities, defining pass/fail criteria, defining representative test signals, and specifying procedures for testing both in-band and out-of-band performance.

3.2.1 Traditional EMC Testing

For high frequency (above 300 MHz) narrow-band (less than a few kHz) radiated immunity testing, there are two principal facilities and techniques available: direct-radiation/anechoic and reverberant. The anechoic procedures are described in IEC 61000-4-3 [8] (semi-anechoic) and IEC 61000-4-22:2010 [21] (fully anechoic), and reverberant techniques in IEC 61000-4-21 [22]. Direct radiation methods generally require that a DUT be placed on a turntable, and that some method is provided for changing the polarization and elevation of the source antenna. This combination allows exposure of the DUT over a wide range of incidence angles and polarizations. A CW or narrow-band signal is radiated at a fixed distance from the DUT (e.g., 3m). Large numbers of DUT orientations and source locations/polarizations result in a more thorough test at the expense of test time, so standards generally specify the required minimums. Reverberant methods avoid moving the DUT or source antenna and instead place the DUT in a highly reflective environment and change the test configuration by moving a highly reflective element (which we will refer to as a “stirrer”) that changes the boundary conditions of the chamber, which in turn changes the field conditions. Under the proper controls [22] this is equivalent to exposing the DUT from a wide range of directions and polarizations. A CW or narrow-band signal is radiated into the chamber. Distance and orientation of the antenna are not rigidly specified other than to say that the antenna should not directly illuminate the DUT and should be located a specified distance away from the DUT. Large numbers of stirrer orientations result in a more thorough test at the expense of test time, so standards generally specify the required minimums.

For both of these methods, the field strength is measured by a calibrated field probe in the working volume of the facility where the DUT will be placed. Test frequencies are selected based on known

vulnerabilities of the DUT, known signal sources that can affect the DUT, or a long list of discrete frequencies that account for unknown or future sources. However, in some cases, bands in which the DUT is designed to communicate wirelessly may be excluded from the test. Long lists of frequencies increase the chances of detecting vulnerabilities at the expense of test time. Published standards attempt to find a balance between thoroughness and test time by giving requirements on the number of required frequencies in a given band and also the number of positions of the DUT and orientations of the source antenna. Note that this discussion was prefaced with “narrow-band.” Testing devices against radiated broadband signals is a more difficult task. The existing standards that discuss testing with narrow-band signals provide a good foundation, but some revisions may be required to accommodate broad-band signals and intelligent DUTs. At present, most immunity tests are based on IEC 61000-4-3 [8]. Additional research is required to verify applicability of simple modulations to adequately predict the potential effects caused by signals with more complex modulations.

3.2.2 Choice of Measurement Facility

For simplicity, we will discuss the choice of measurement facility for this type of testing assuming that there are two options: a highly reflective environment (i.e., a reverberation chamber) Figure 8, and a free-space environment (i.e., an anechoic chamber) Figure 9. Of course, there are many variations of the two environments that lie somewhere in between the two, most notably a semi-anechoic chamber. The primary advantages in the use of a reverberation chamber are that the patterns and gains of antennas and devices used in the chamber become less important, the environment replicates high multi-path receive conditions, and high field strengths are possible with modest amounts of transmit power. The loss of directivity is also a potential disadvantage; i.e., we may want to know the arrival direction of the signal coupling into the DUT. Testing the DUT in an anechoic chamber at a variety of orientations and polarizations would be required to appropriately determine the exposure direction where the device is most susceptible. One other disadvantage of using a reverberation chamber is that to determine the exact field strength impinging on the DUT at the time of failure is difficult. The complex nature of the reverberation environment means we can determine the statistics (e.g., maximum and average field strength) throughout the test volume, but the instantaneous field strength at the position of the DUT at the time of failure is known only within the range of that statistical distribution. Radiating broadband signals inside a reverberation chamber also presents an interesting problem. At each stirrer position, a communications channel is created. As with any physical communications channel, there is some frequency dependence which could impact the radiated signal. In other words, what began as a known 4G/LTE signal at the output port of the signal generator could become a very different and unknown signal incident on the DUT. Coherence bandwidth is normally the metric used to address this aspect of a channel inside a reverberation chamber. However, definitions and implementations of coherence bandwidth can vary [23-28], and the underlying theory of which

digitally modulated signals pass through a reverberation chamber is still in its early stages of development. In traditional susceptibility tests utilizing a reverberation chamber, the radiated signal is either CW or narrow band (1 kHz AM). In these cases, there is still a channel at each stirrer position, but the coherence bandwidth is not an issue.

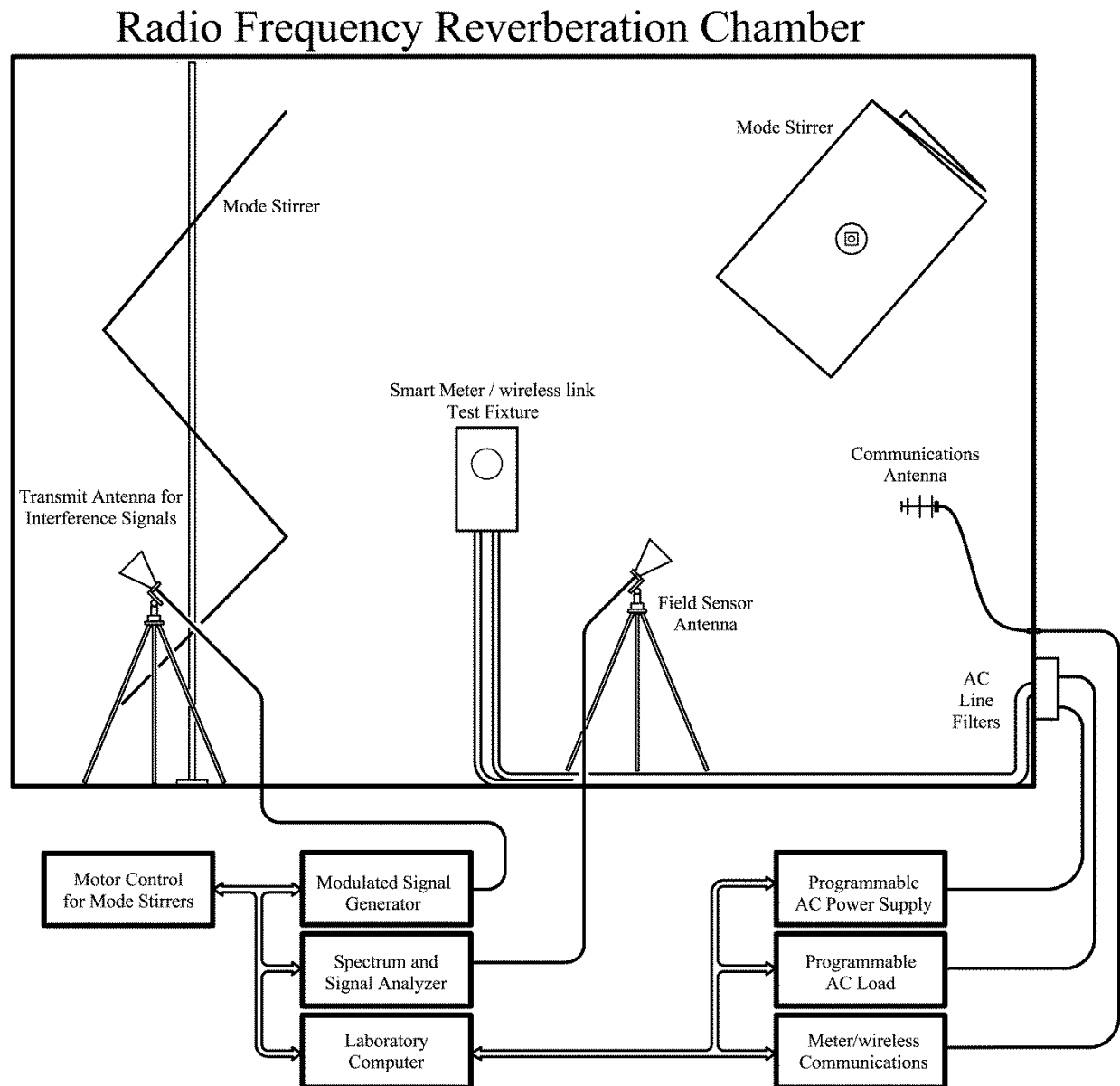


Figure 8. A reverberation chamber setup for testing radiated interference and coexistence of an example smart meter/wireless link. The equipment shown is necessary to operate the electric meter and the wireless communications link while exposing the device to interfering signals.

The use of an anechoic chamber presents a different set of challenges for this testing. First, in order to thoroughly expose the DUT, it (or the radiating antenna) must be physically moved to many different positions. Second, some knowledge of the antenna's gain and pattern is required in order to accurately calculate the field level of the incident signal impinging on the DUT at the time of failure. Testing in an anechoic chamber could yield additional information about the way in which the DUT fails. Assuming the pattern of the radiating antenna is known, we can determine what part of the DUT was susceptible, thus allowing its design to be revised and the interference risk to be mitigated.

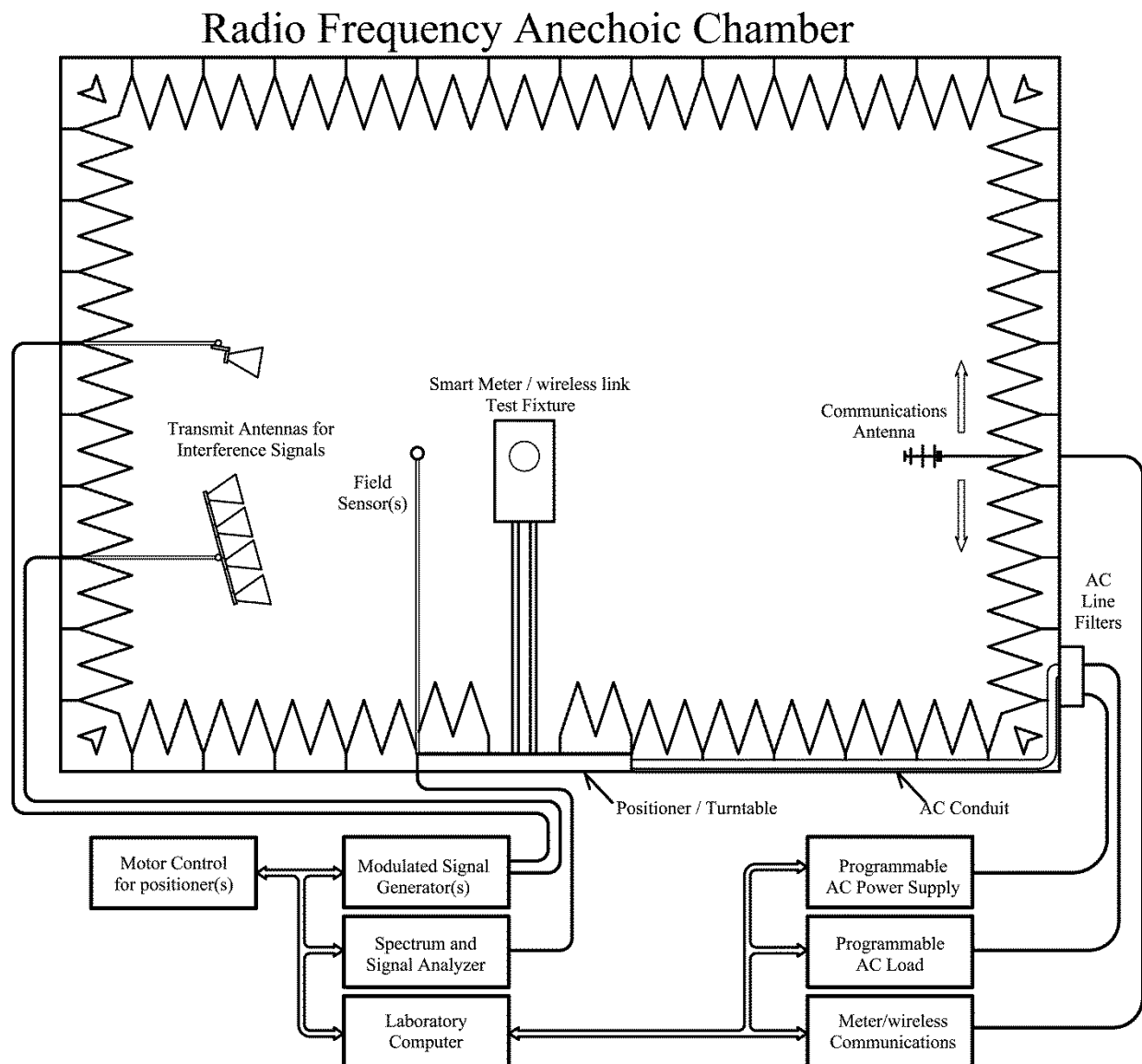


Figure 9. A fully anechoic chamber setup for testing radiated interference and coexistence of an example smart meter/wireless link. The equipment shown is necessary to operate the electric meter and the wireless communications link while exposing the device to interfering signals.

As discussed above, Figure 8 (reverberation chamber) and Figure 9 (anechoic chamber) illustrate two possible facilities for RF radiated testing of interference, coexistence, and spectrum access techniques. The two enable over-the-air (OTA) tests on complete units and systems in their native configurations; e.g., with the associated antennas (including MIMO configurations) and limited (or no) self-reporting capabilities. The example DUT illustrated in these figures is a smart meter with a wireless link but this general setup would be similar for other systems. These testing facilities allow development and validation of interference and coexistence metrics and test methods specific to the smart grid infrastructure. These facilities also enable evaluation more closely correlated to real-world deployments than conducted approaches.

3.2.3 Test Signal Selection

As described in Section 2.2, the current practice of using amplitude modulated CW signals to test for interference may not adequately predict the performance of the device when exposed to broadband modulated signals or be used to study the effects on communications systems by an interfering signal. If true, is there an optimum set of one or more complex broadband waveforms that would result in a more thorough or accurate EMC or coexistence test? One possibility is to use the specific modulation(s) that will likely exist in the area where the device will be deployed. This may be the course to follow when designing a coexistence test where the technologies that are expected to coexist in a given location are specified. The authors in [29] analyzed coexistence issues related to IEEE 802.15.4g (smart metering utility networks) and local installations of ZigBee® and WLAN networks using specific characteristics of each technology, and [30] did a similar analysis and included Bluetooth® in the mix of technologies. The coexistence studies in [29] and [30] were motivated by spectrum sharing issues in the unlicensed 2.4 GHz frequency band. However, no OTA measurement or testing methodologies were proposed by either research group.

While the use of signals specific to the technologies involved in the coexistence measurements may be appropriate, if not necessary, this may not be a long-term practical solution for a generic standardized interference test. In this case, predicting the “best” choice would be difficult because the technology is steadily changing and there exist almost endless possible modulated waveforms that could be candidates to use as an interfering signal, especially if the device will be deployed in a variety of environments. However, until such a generic test signal is developed and standardized, most testing (interference and coexistence) will employ modulated waveforms specific to available wireless technologies.

Along with using specific wireless modulations as interference test signals we can construct a “generic” signal composed of many individual sine waves. This “multisine” waveform could be constructed to have similar statistical properties as specific complex modulation schemes [31] and is well-suited to testing electronic circuits. This flexibility to generate specific statistical properties

may also be useful for radiated interference testing. More research is needed to clarify what statistical properties would represent a wide variety of possible interfering signals.

A different approach is demonstrated in [32]. Here the authors used a filtered and up-converted white Gaussian noise signal to emulate some key characteristics of wireless network transmissions. The properties of interest included occupied bandwidth, power spectral density, average total radiated power, and amplitude fluctuations. This technique also has some characteristics that may prove useful for a generic interference test signal.

Another alternative to the traditional 61000-4-3 AM signal has been proposed in IEC 60601-1-2 [33]. This standard, focused on EMC testing of medical devices, proposed use of a pulsed signal. The frequency and amplitude of the pulse are varied, depending on which communications technology is being mimicked. Though this pulsed testing is not a perfect match when compared to a 10 MHz LTE signal, the results are promising. Appendix B provides some additional details and test data to demonstrate the impact of the use of a pulsed signal for immunity testing.

The design of a generic interference signal is also influenced by parameters of the DUT. The signal characteristics that are adequate to test, for example, a microprocessor controller or other passive electronic system for RF immunity may not give meaningful results when testing an active wireless communication system. The communication system will interact with the interference in more sophisticated ways through error-correction, frequency hopping, and other techniques. An interference test method will have to account for the more intelligent interaction of the DUT and the interfering signal. The communications device is also part of a network. This may be two devices (point to point) or any number of nodes in a wider network. The interference evaluation should also consider the effects on the network. There are a number of interference models that can be used to evaluate the channel interference caused by unwanted RF energy. The authors in [34] provide some guidance and discussion on the effects of choosing or developing an appropriate model to analyze wireless channel interference.

3.2.4 In-band vs. Out-of-Band Interference

The measurement setup used in the test example in Section 1.3 and Appendix B considers only the case where the interfering signal completely overlaps the cable channel. The DUTs were not characterized for interference outside the tuned channel, nor any kind of interference from the wireless and cable channels being adjacent to each other. Given that a 4G/LTE signal could have three times the bandwidth of an intended signal (as is the case with the testing described in Appendix B), a single LTE channel could potentially interfere with multiple channels simultaneously. This is an extremely unlikely scenario, but it does raise the question “How much signal overlap does there need to be before a failure is caused?” If we assume that there is zero overlap between the interfering signal and the active channel, the field level at which the DUT

fails would be significantly higher, and thus not something likely to be radiated from a device in compliance with the appropriate legal regulations. Something else to consider is whether or not the DUT is digitizing more than one frequency/channel at a time. Some devices have the ability to tune multiple channels simultaneously. While one channel is being utilized by the user, another may be digitized and stored for other purposes. As this technology continues to evolve, new devices may be able to continuously digitize the entire band of operation. This ability would change the way “in-band” interference testing is viewed.

3.2.5 Choice of Bandwidth

Before discussing the effects of signal bandwidth on immunity measurements, consider the following quick experiment. We connected an LTE signal generator directly to a spectrum analyzer and examined the characteristics of a fully allocated LTE signal with three different bandwidths: 1.4 MHz, 10 MHz, and 20 MHz, but all with the same drive power (which roughly translates to the same RMS field). The consistency of the drive power was verified by measuring the channel power of the received signal on the spectrum analyzer. The spectral results averaged over approximately 1 minute are shown in Figure 10. The key features of the signals in Figure 10 are the approximately flat spectrum (over the signal bandwidth) and the relative amplitudes as a function of signal bandwidth. As the bandwidth increases, the apparent amplitude (power density) decreases. This is a natural consequence of spreading a fixed channel power over a larger and larger bandwidth.

This experiment leads to a simple question: how does the bandwidth of the signal affect an immunity test? To address this question for an arbitrary DUT (with or without some communication link) is difficult, but we can make a few simplifying assumptions that will allow a rough analysis. The susceptibility of a device is rarely flat with frequency. If we focus on those frequencies where a device is most susceptible, we find that the device is not susceptible to individual frequencies, but is instead susceptible over a band of frequencies. We can define the width of this band as the “susceptibility bandwidth” and assume that we can roughly model this effect using a simple bandpass filter and any frequency content outside of the pass band will not interfere with the operation of the DUT.

This definition of susceptibility bandwidth for interference testing may be useful, but it does have a few implications. First, assume that any DUT failures are a function of the average channel power coupled through the bandpass filter. For any interfering signal centered on the DUT pass band, failure levels should be roughly independent of signal bandwidth as long as signal bandwidth is less than the susceptibility bandwidth. As the signal bandwidth increases beyond the susceptibility bandwidth, the DUT will appear to be less susceptible (will require more transmitted power to cause interference) because more of the transmitted spectrum will be removed by the bandpass characteristic of the DUT.

Consider the testing described in Appendix B, where the intended channels are 6 MHz wide. We can then assume that the DUT's susceptibility bandwidth is also equal to 6 MHz. If the DUT fails as a function of average channel power through the 6 MHz filter, it should appear to be most susceptible to a 1.4 MHz signal, followed by the 10 MHz signal, and then the 20 MHz signal. Since the transmitted spectrum is roughly flat over the signal bandwidth, we can estimate the effect of reducing the channel bandwidth to 6 MHz. For a 10 MHz signal, the channel power will be reduced by 40 %, giving a reduction in estimated field of 2.2 dB. For a 20 MHz signal, the channel power will be reduced by 70 %, giving a reduction in the estimated field of 5.2 dB. These predictions were verified by use of a direct injection measurement (described in Appendix B) in which the integration bandwidth was changed for various signal bandwidths.

To make things more interesting, we can consider the case where the spectrum of the interfering signal is not flat with frequency. The examples in Figure 10 show a roughly flat spectrum over the pass band. But there is no requirement to force a flat spectrum. So what happens if some transmitted frequencies are amplified and others are attenuated while maintaining the same total channel power? The examples in Figure 10 are a special case, where the 10 MHz signal can be interpreted as a 20 MHz signal that has been attenuated on the edges and amplified in the center. This implies that not only is bandwidth important, but so is the spectral envelope.

In the end, when considering which interfering signal should be used, we can best use an integration bandwidth equal to the signal bandwidth, and avoid any parameters specifically related to a DUT characteristic (such as bandwidth), since most DUTs cannot be characterized so well before testing. However, we should keep this effect in mind and avoid using very large bandwidth signals to test devices that are known to have narrow receiving bandwidths.

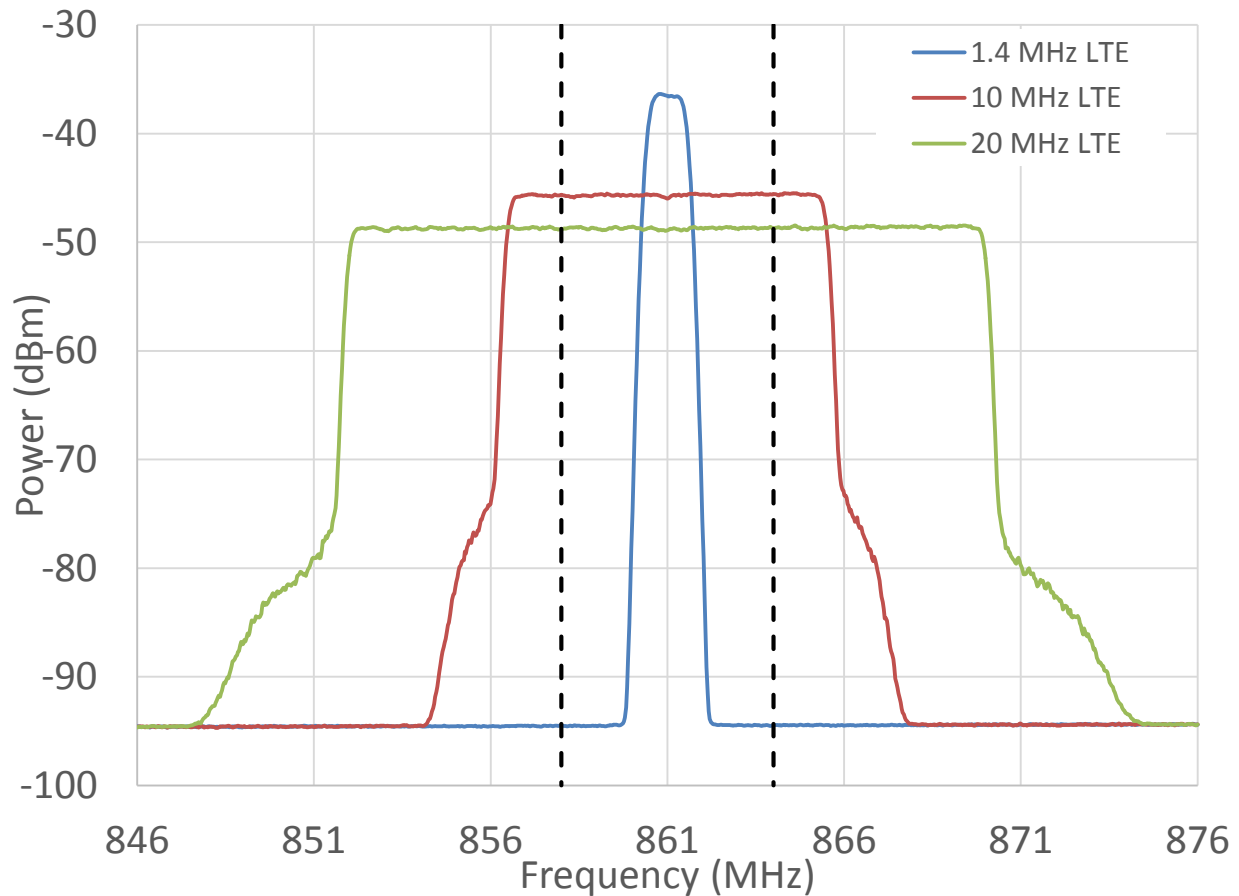


Figure 10. LTE signal envelopes with three different bandwidths: 1.4 MHz, 10 MHz, and 20 MHz, but all with the same channel power.

3.2.6 Definition of “Failure”

The DUT performance criterion for immunity to interference testing in many product and test method standards usually follows these general guidelines (e.g. IEC 61000-4-3, section B.7 [8] or [35] section 10.4.4 or similar).

1. No degradation when the immunity test is applied to the product.
2. Some degradation occurs during the test but the device still operates within manufacturer’s specifications both during and after the test.
3. Momentary degradation sufficient to cause some disruption to the operation of the device (outside of the manufacturer’s specifications) but when the immunity test signal is removed, the device returns to its normal operation without operator intervention.
4. Disruption of the use of the device (outside of the manufacturer’s specifications), which does not recover without manual intervention when the immunity test signal is removed.
5. Physical damage to the device requiring replacement or repair.

Items 1 and 2 are generally acceptable. Item 3 may be tolerated for non-critical functions and items 4 and 5 are not acceptable.

The above criteria are logical for many applications where there are well-defined metrics that define the operation of the DUT. The problems increase when the DUT has multiple complex parameters that can be affected by the interfering signal, when the DUT applies sophisticated error correction algorithms, or if the failure is subjective (i.e., picture or sound quality). In the case of standard EMC product testing, these parameters or specifications are usually determined by the device manufacturer.

In cases when complex, intelligent devices are the subject of testing, the objective of the device needs to be carefully considered when developing the interference metrics. Depending on the device's function a variety of metrics could be used. For consumer devices that feature a user-interface or interaction, higher-level metrics such as screen pixilation or distortion of audio may be appropriate. However, for devices that don't interact with users in an audio or visual manner, other, lower level metrics may suffice. These lower level metrics include information about the number of packets correctly decoded, the number of uncorrectable packet errors, the signal to noise ratio, or measurements of the error vector magnitude.

Before choosing a metric for failure, careful consideration should be given to what elements influence that parameter. For example, choosing a high-level parameter (e.g., video quality) means that to determine the cause of the interference will be difficult. It could be the result of the interference signals coupling to the cable, connector, internal circuits, or something else. Thus, choosing lower-level indicators can have the advantage of being somewhat descriptive as to what part of the system is being impacted by the interfering signal.

4. Future Research

Spectrum sharing involves the coordinated and uncoordinated use of spectrum to achieve the most efficient use of this limited resource. An emerging sharing paradigm envisions a tiered approach, with a combination of incumbent/primary, secondary and tertiary users, and both coordinated and uncoordinated access techniques [36, 37]. Regardless of the underlying sharing approach, the competition for spectrum access creates interference and coexistence challenges. Interference in its basic form is simply an unwanted RF signal or emission that disrupts the communication link. However, robust testing requires knowledge of multiple interfering signal characteristics, such as the power level variations, transmission duty cycles, frequency location; e.g., in-band versus out-of-band and harmonics. Coexistence testing, in contrast, requires simultaneous measurement of

multiple system parameters from a heterogeneous mix of communication technologies. Thus, both testing and measurement processes are inherently complex and vital.

From an information standpoint, most smart grid technology can be assumed to have low data transfer amount requirements, i.e., a small number of bits relative to channel capacity. However, the latency and availability of the smart grid data may have very tight requirements since some of the data will be process and control information. Thus, interference and coexistence research must consider the timing of channel access aspects as well as the overall channel usage.

In general, coexistence is the merging of the information and physical domains. Thus, information and physical domain metrics must be identified specific to smart grid infrastructure requirements. While the metrics may be the same as in other coexistence challenges such as the medical or manufacturing settings, the acceptable quantitative ranges for such metrics must be investigated. The metrics and appropriate values should be pursued by a combination of theory, simulation, and measurement.

Hence, additional research into interference and coexistence issues related to smart grid and other critical infrastructure will need to consider the emerging concept of shared spectrum, and the impacts of a shared spectrum on the communication infrastructure. In particular, the focus will be on:

1. Establishing interference and coexistence metrics for smart grid. In the case of interference, this extends beyond simply the power (or field) level and may include measures such as duty cycles, bandwidths, and modulation schemes;
2. Interference/coexistence of current technologies (e.g., IEEE 802.11, 802.15.4) in the existing ISM bands, 900 MHz, 2.4 GHz, and 5 GHz;
3. Interference/coexistence for the use of LTE in the ISM bands;
4. Quantifying/measuring interference between broadband wireless networks and consumer devices.

Research in interference and coexistence requires research related to the following topics, which also apply to the broader spectrum sharing problem:

1. Low-cost, distributed, calibrated spectrum measurements and monitoring;
 - a. Needed to obtain accurate, real-time picture of the smart grid interference/coexistence environment;
 - b. Example environments including meter locations (both dense and individual) and manufacturing facilities;
2. The interference/coexistence implications of multiple-input-multiple-output (MIMO) and Massive MIMO technologies on the communication infrastructure.

5. Conclusions

We have presented an overview of emerging issues related to the interference and coexistence of wireless communications systems that may impact critical infrastructure such as the smart power grid, public safety, health care, smart manufacturing, and similar. As such we have generated more questions than answers and called for continuing research in these areas. The primary goal of this future research is to develop test methods and performance metrics that will enable designers, manufacturers, and customers of new smart communications systems to understand and predict the ability of a device or system to resist interference and coexist within a particular RF environment.

Acknowledgments

The authors thank Dr. Chris Greer and Dr. David Wollman of the NIST Smart Grid and Cyber-Physical Systems Program Office and Dr. Michael Kelley and Dr. Perry Wilson of the NIST RF Technology Division for patiently supporting this work. We also acknowledge the contributions of Mr. David Hunter and Cable Television Laboratories, Inc. in the interference measurements referenced in this report.

References

- [1] Pew Research Center, Fact Tank, June 6, 2013. <http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/>
- [2] International Telecommunications Union, ICT Facts and Figures 2014. <http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>
- [3] OECD (2012), “Machine-to-Machine Communications: Connecting Billions of Devices”, *OECD Digital Economy Papers*, No. 192, OECD Publishing. <http://dx.doi.org/10.1787/5k9gsh2gp043-en>
- [4] M. Beale, Y. Morioka, “Wireless Machine-to-Machine Communications,” 2011 41st European Microwave Conference (EuMC), pp. 115-118 (2011)
- [5] NIST Cyber-Physical Systems Home page: <http://www.nist.gov/cps/>
- [6] ANSI C63.14-2009, “American National Standard Dictionary of Electromagnetic Compatibility (EMC) including Electromagnetic Environmental Effects (E3)”.
- [7] ETSI EN 301 489-1, Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements. <http://www.etsi.org>

- [8] IEC 61000-4-3 ed3.2, Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test. http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/43958
- [9] IEEE Std 1900.2™ - 2008, IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence between Radio Systems.
- [10] IEEE Std 802.15.2™ - 2003(R2009), IEEE Recommended Practice for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands.
- [11] IEEE Std 802.19.1™ - 2014, IEEE Standard for Information technology-- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 19: TV White Space Coexistence Methods.
- [12] IEC 62657-2:2013 - Industrial communication networks - Wireless communication networks - Part 2: Coexistence management.
- [13] CTIA - The Wireless Association (CTIA) and Wi-Fi Alliance (WFA), “Test Plan for RF Performance of Wi-Fi Mobile Converged Devices,” Version 1.3, June 2009.
- [14] IEEE Std 802.15.1™ -2002 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), <http://standards.ieee.org/findstds/standard/802.15.1-2002.html>
- [15] IEEE Std 802.11b™ -1999 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band. <http://standards.ieee.org/findstds/standard/802.11b-1999.html>
- [16] IEEE Std 802.15.4™ -2006 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs). <http://standards.ieee.org/findstds/standard/802.15.4-2006.html>
- [17] NISTIR 7761 Rev. 1, NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications, David Cypher (editor), June 2014.
- [18] Cable Television Laboratories, Inc. CableLabs, <http://www.cablelabs.com/about-cablelabs/>
- [19] J.B. Coder, J. M. Ladbury, D. F. Hunter, Characterizing a Device’s Susceptibility to Broadband Signals: A Case Study, Proc. 2014 IEEE International Symposium on EMC, Raleigh, NC, Aug. 2014, pp. 295-300.

- [20] M. McKinley, K. Remley, M. Myslinski, J.S. Keyyey, D. Schreurs, and B. Nauwelaers, EVM Calculation for Broadband Modulated Signals, 64th ARFTAG Conf. Dig., Orlando, FL, pp.45-52, Dec. 2004.
- [21] IEC 61000-4-22:2010, Electromagnetic compatibility (EMC) - Part 4-22: Testing and measurement techniques - Radiated emissions and immunity measurements in fully anechoic rooms (FARs). <http://webstore.iec.ch/webstore/webstore.nsf/artnum/044599!opendocument>
- [22] IEC 61000-4-21 ed2.0, Electromagnetic compatibility (EMC) - Part 4-21: Testing and measurement techniques - Reverberation chamber test methods. http://webstore.iec.ch/Webstore/webstore.nsf/Artnum_PK/44777
- [23] E. Genender, C. L. Holloway, K. A. Remley, J. M. Ladbury, G. Koepke and H. Garbe, Simulating the multipath channel with a reverberation chamber: Application to bit error rate measurements, IEEE Transactions on Electromagnetic Compatibility, vol. 52, no. 4, pp. 766-777, 2010.
- [24] C. Orlenius, M. Franzn, P.-S. Kildal and U. Carlberg, Investigation of heavily loaded reverberation chamber for testing of wideband wireless units, Antennas and Propagation Society International Symposium 2006, IEEE, Albuquerque, NM, 2006.
- [25] C. L. Holloway, H. A. Shah, R. J. Pirkl, K. A. Remley, D. A. Hill and J. Ladbury, Early time behavior in reverberation chambers and its effect on the relationships between coherence bandwidth, chamber decay time, RMS delay spread, and the chamber buildup time, IEEE Transactions on Electromagnetic Compatibility, vol. 54, no. 4, pp. 714-725, 2012.
- [26] X. Chen and P.-S. Kildal, Theoretical derivation and measurements of the relationship between coherence bandwidth and RMS delay spread in reverberation chamber, EuCAP 2009, pp. 2687-2690, 2009.
- [27] M. I. Andries, P. Besnier and C. Lemoine, On the prediction of the average absorbing cross section of materials from coherence bandwidth measurements in reverberation chamber, International Symposium on Electromagnetic Compatibility, Rome, 2012.
- [28] X. Chen, P.-S. Kildal, C. Orlenius and J. Carlsson, Channel sounding of loaded reverberation chamber for over-the-air testing of wireless devices: coherence bandwidth versus average mode bandwidth and delay spread, Antennas and Wireless Propagation Letters, IEEE, vol. 8, pp. 678–681, 2009.
- [29] Ma, R.; Meng, W.; Chen, H.; Huang, Y; Coexistence of Smart Utility Networks and WLAN/ZigBee in Smart Grid, IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012, pages 510-520.
- [30] M. Sarijari, et al., Coexistence of Heterogeneous and Homogeneous Wireless Technologies in Smart Grid Home Area Networks, 2013 International Conference on Parallel and Distributed Systems (CPADS), 2013, pages 576-581.
- [31] N.B. Carvalho, K.A. Remley, D. Schreurs, and K.G. Gard, Multisine Signals for Wireless System Test and Design”, IEEE Microwave Magazine, Vol. 9, Issue 3, 2008, pp. 122-138.

- [32] C. Lins-Morstadt, M. Slocum, and G. Tait, Emission Source for Compatibility Testing of Wireless Networks in the Below-Deck Environment on Ships, IEEE International Symposium on Electromagnetic Compatibility, 2012, pages 480-485.
- [33] IEC 60601-1-2 Ed4.0, Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests.
http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/49272!opendocument&preview=1
- [34] Iyer, A.; Rosenberg, C.; Karnik, A; “What is the Right Model for Wireless Channel Interference?”, IEEE Transactions on Wireless Communications, Vol. 8, No. 5, May 2009.
- [35] Electromagnetic Compatibility and Smart Grid Interoperability Issues, SGIP 2012-005, Version 1.0. : <http://www.nist.gov/smartgrid/research-reports-presentations.cfm>
- [36] Report to the President, “Realizing the Full Potential of Government-held Spectrum to Spur Economic Growth”, PCAST Spectrum Report,
http://search.whitehouse.gov/search?affiliate=wh&form_id=usasearch_box&query=spectrum+sharing
- [37] “Spectrum Sharing”, International Telecommunications Union, ICT Regulation Toolkit, Chapter 5.4, <http://www.ictregulationtoolkit.org/5.4#s5.4.3>

Appendix A. Standardization Activities for EMC and Coexistence

There are many standards development organizations that are active in EMC. The list includes the Institute of Electrical and Electronic Engineers (IEEE³) and the American National Standards Institute (ANSI⁴) (in particular ANSI Accredited Standards Committee C63), and the International Electrotechnical Commission (IEC⁵). The IEC is an international standards organization which develops and maintains a widely referenced and comprehensive collection of EMC standards and technical reports. The IEC 61000 series of EMC standards are detailed basic standards related to EMC test methods. The standards of most interest to radiated immunity testing are IEC 61000-4-3 along with others related to specific test facilities (e.g. 61000-4-20 TEM structures, 61000-4-21 reverberation chambers, and 61000-4-22 fully anechoic rooms). The technical committees within the IEC responsible for these basic EMC documents are TC-77⁶ and the International Special Committee on Radio Interference (CISPR⁷). Topics related to interference immunity are generally addressed in the TC-77 subcommittees while unintended emissions from devices are the focus of CISPR. An exception to this is CISPR 16-2-4 which outlines basic considerations for immunity testing in various facilities. According to the IEC website, the basic measurement standards developed by TC-77 and CISPR provide test and measurement guidelines for 47 distinct product families within the IEC.

Also, many product or industry standards developed by other organizations, for example International Council on Large Electric Systems (CIGRÉ⁸) SC C4, European Committee for Electrotechnical Standardization (CENELEC⁹), National Electrical Manufacturers Association (NEMA¹⁰), Society of Automotive Engineers (SAE¹¹), and International Organizations for Standardization (ISO¹²) to name a few, directly reference or are harmonized with IEC standards. EMC aspects of telecommunications standards developed by the International Telecommunications Union – Telecommunications Standardization Sector (ITU-T¹³) and the European Telecommunications Standards Institute (ETSI¹⁴) also use the IEC basic test standards. Since EMC issues are a concern for virtually all electrical and electronic equipment and are covered by a multitude of standards, we will not attempt to categorize or identify all the possible standards that reference IEC EMC documents.

The majority of product specific EMC standards refer to basic test and measurement standards. These basic standards define the test methodology, facilities, and general descriptions of the test instruments, test levels, and guidance on test documentation. The basic test standard often

³ <https://www.ieee.org/index.html>

⁴ <http://www.ansi.org/>

⁵ <http://www.iec.ch/>

⁶ http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1265,25

⁷ http://www.iec.ch/emc/iec_emc/iec_emc_players_cispr.htm

⁸ <http://www.cigre.org/>

⁹ <http://www.cenelec.eu/>

¹⁰ <http://www.nema.org/Pages/default.aspx>

¹¹ <http://www.sae.org/>

¹² <http://www.iso.org/iso/home.html>

¹³ <http://www.itu.int/en/ITU-T/Pages/default.aspx>

¹⁴ <http://www.etsi.org/>

referenced for radiated immunity testing by product or generic standards is IEC 61000-4-3. The guidelines in this standard give general requirements for the testing equipment, shielded enclosure, uniformity of the radiated field, test levels for the field strength, arrangements of various classes of equipment-under-test (table top, floor standing, body mounted), test procedures, and test reports. The test is simply using an antenna to radiate an RF signal toward the device-under-test (DUT) inside a shielded enclosure that has sufficient RF absorbing material to control reflections and provide uniform field strength over the surface of the DUT. Since this is a basic standard, the product committees are expected to tailor specific parameters of the test (frequency range, signal strength, etc.) to the needs of their product while adhering to the essential test process of the standard. The following Table A.1 includes three examples of product standards that reference IEC 61000-4-3 and their specifications.

Table A.1. A comparison of the basic standard and three product standards that reference IEC 61000-4-3.

Test Parameter	IEC 61000-4-3 Basic Standard	IEC 62052-11 electricity meters	CISPR 24 – information technology equipment	ETSI EN 301 489-1 EMC for radio equipment and services
Frequency Range (MHz)	General purpose 80 – 1000 or Cellular telephone 800 – 960 and 1,400 – 6,0000	80 – 2000	80 – 1000	80 – 1000 and 1400 – 2700 with exceptions for specified exclusion bands.
Frequency increments	Continuous	As specified in 61000-4-3	As specified in 61000-4-3, plus more detailed tests at selected frequencies if specified in Annex A.	Stepped at 1% of current test frequency
Test signal Modulation	80% AM at 1 kHz	80% AM at 1 kHz	80% AM at 1 kHz	80% AM at 1 kHz (or 400 Hz)
Test signal strengths (unmodulated CW carrier)	Level 1 – 1 V/m Level 2 – 3 V/m Level 3 – 10 V/m Level 4 – 30 V/m Level x – special	With Current: 10 V/m No current: 30 V/m	3 V/m	3 V/m

Test Parameter	IEC 61000-4-3 Basic Standard	IEC 62052-11 electricity meters	CISPR 24 – information technology equipment	ETSI EN 301 489-1 EMC for radio equipment and services
Test chamber	Absorber lined shielded enclosure (ALSE)	ALSE	ALSE	ALSE
Transmit Antenna to DUT distance	3 m	3 m	3 m	3 m
Cable exposure	Minimum of 1 m cable exposure	1 m Table top configuration	As specified in 61000-4-3	As specified in 61000-4-3
DUT exposure angles	Each side of DUT is exposed in both polarizations unless more or less exposure is justified.	As specified in 61000-4-3	4 sides unless most sensitive side is determined with certainty	As specified in 61000-4-3

The communications technologies in use today employ sophisticated techniques to optimize and overcome many technical challenges like multiple users, limited bandwidth, and poor received signal to noise ratios. The perspective of these specifications is to ensure the highest probability that the communications will be successful within the legal limits of bandwidth and transmit power. Interference mitigation is typically viewed as a measure of how the technology is able to function in the presence of co-channel and adjacent channel signals from known sources. Several communications technologies suggested for smart grid applications (NISTIR 7761 Rev. 1, table 3, page 46)¹⁵ are listed in Table A.2 along with references to specifications that address interference considerations.

Table A.2. Communications technologies suggested for use in Smart Grid applications

Wireless Technology	Sub-network	Licensed (L) or Unlicensed (UL) Spectrum	EMC Test Requirements
ITU-T G.9959 and Z-Wave wireless technologies	HAN ¹⁶	UL	Refer to ITU-T Series K Recommendations

¹⁵ NISTIR 7761 Rev. 1, NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications, David Cypher (editor), June 2014.

¹⁶ Home Area Network (HAN)

Wireless Technology	Sub-network	Licensed (L) or Unlicensed (UL) Spectrum	EMC Test Requirements
IG Band (450 MHz - 470 MHz)	NAN ¹⁷ , WAN ¹⁸	L	FCC Industrial-Business frequency allocations
IEEE Std. 802.11	HAN, FAN ¹⁹	UL	Manage interference as per IEEE Std 802.11
IEEE Std. 802.11ah – Indoor / Outdoor	HAN, FAN, NAN	UL	
IEEE Std. 802.11n	HAN, FAN	UL	
IEEE Std. 802.11ac	HAN, FAN	UL	
IEEE Std. 802.15.4	HAN, FAN, NAN	L, UL	Manage interference as per IEEE Std 802.15.4
IEEE Std. 802.16-2012 / WiMAX	WAN, FAN, NAN	L, UL	Manage interference as per IEEE Std 802.16
IEEE Std. 802.16.1-2012 / WiMAX 2	WAN, FAN, NAN	L, UL	Manage interference as per IEEE Std 802.16.1
IEEE Std. 802.16.1a-b / WiGRID	WAN, FAN, NAN	L, UL	
GSM / EDGE Radio Access Network (GERAN)	WAN	L	Managed as per 3GPP 45.050
cdma2000 1x	WAN	L	Designed to operate in presence of all known interferers
cdma2000 High Rate Packet Data (HRPD / EV-DO)	WAN	L	Designed to operate in presence of all known interferers

¹⁷ Neighborhood Area Network (NAN)

¹⁸ Wide Area Network (WAN)

¹⁹ Field Area Network (FAN)

Wireless Technology	Sub-network	Licensed (L) or Unlicensed (UL) Spectrum	EMC Test Requirements
Extended High Rate Packet Data (xHRPD)	WAN	L	Designed to operate in presence of all known interferers
Universal Terrestrial Radio Access Network (UTRAN) (a.k.a. Wideband CDMA (W-CDMA))	WAN	L	
Evolved High-Speed Packet Access (HSPA+)	WAN	L	Managed as per 3GPP 25.942, 25.943
Evolved Universal Terrestrial Radio Access Network (E-UTRAN) (a.k.a. Long Term Evolution (LTE))	WAN	L	Managed as per 3GPP 36.101, 36.104
Mobile Satellite Service (MSS) in L / S-Band	WAN	L	
Fixed / Mobile Satellite Service (FSS / MSS) in Ku/Ka-band	WAN	L	

While most of the standards development continues to be focused on EMC standards, coexistence testing is beginning to see some activity. Standards such as IEEE 1900.2 and others referenced in this document have worked to define the coexistence problem, but usually stop short of measuring and quantifying a device's ability to coexist with other wireless devices. Development of a method to measure coexistence is the focus of the ANSI C63.27 working group. Building upon the definitions set forth in IEEE 1900.2, ANSI C63.27 is working to define a set of test methods and metrics that, when measured, will give an indication of a device's ability to maintain an acceptable level of performance when in the presence of other wireless devices operating in its vicinity (both physically and in terms of frequency). The C63.27 standard is also being written to differentiate different use environments for devices. This would enable different "levels" of testing for devices placed in special use environments (e.g., hospitals).

Combined with other types of interference and wireless communications testing, measuring coexistence will enable device manufacturers, users, and regulators to make better informed decisions about the reliability of wireless data links.

ANSI C63.27 will not solve all of the coexistence measurement problems, rather it only focuses on half the problem, namely how the DUT operates in the presence of other devices. Future

versions of the document may incorporate test methods to evaluate the other half of coexistence, namely the device's impact on others as it transmits. From a testing perspective, this is a much more difficult problem because it requires monitoring other devices for changes in their performance when a DUT is introduced into the environment. This portion of the coexistence problem remains an active area of research.

Appendix B. LTE Interference to Cable TV

B.1 Introduction

As has been discussed earlier in this technical note, NIST, in conjunction with Cable Television Laboratories, Inc. (known as CableLabs), conducted some research on the ability of wireless networks to interfere with the conducted cable communications network. Here, we discuss that effort in some detail in order to provide a more complete picture. Though the cable communications network may not be considered “critical infrastructure” in the same context as discussed earlier, the measurements, the method, and the lessons learned do carry over to testing wireless devices in the critical infrastructure realm. The measurements shown here are discussed in more detail in [B1].

Over the past few years, there have been reports of LTE signals from cellular networks interfering with cable television networks [B2, B3]. With over \$200 billion in distribution infrastructure and in-home equipment, quantifying the risk of an LTE signal interfering with any portion of that infrastructure is an important economic problem. As part of this effort, equipment found in the consumer’s home, in the distribution plant, and above or below ground in between the two should be investigated. Here, we focus on the in-home equipment because our most extensive testing and research involved these devices. The same method described here was used to test the distribution hardware.

The in-home equipment had all been subjected to IEC 61000-4-3 tests by the manufacturer prior to being purchased by the cable company. Test levels ranged from 3 V/m to more than 10 V/m. In general, new equipment was tested using higher electric field strengths. Per the IEC standard, all equipment was tested in an anechoic chamber at a limited number of device orientations and field polarizations. Given these results, should an interference problem be expected when the equipment is exposed to an LTE signal with a 5 MHz - 20 MHz bandwidth?

Intuitively, the potential for interference between a cable television system and a wireless 4G/LTE data system may seem low. The RF signals used in cable television systems are entirely conducted (either coaxial cable or fiber optic), and the 4G/LTE system is almost entirely wireless. Further, the two networks are designed to be independent of one another and exchange no data with each other. The networks can however, share the same frequency spectrum. Currently, the overlap is small, but future auctions of spectrum may significantly increase the amount of overlap [B4].

Even in cases where the 4G/LTE and cable networks share the same frequency space, interference is not inevitable. As an example, consider a 4G/LTE network operating at 819 MHz. Assume this wireless channel is being used heavily by a person physically close to a cable set-top box (STB) who is also watching television. If the channel being viewed (and tuned by the STB) does not occupy the same frequency slot as the wireless 4G/LTE channel, the potential for interference is negligible. If the cable STB is tuned to a channel adjacent to or overlapping with 819 MHz, the

chance of interference is higher, but still low. Now consider the case where the tuned STB channel and the 4G/LTE channel occupy the same frequency space. Here, the potential for interference is the greatest, but still depends on the equipment and its configuration. In addition to the frequency overlap, the amplitude of the wireless signal must be sufficiently high and some portion of the signal must be coupled into the STB in order to create interference. The amplitude of the signal is proportional to the LTE transmit power and inversely proportional to the distance between the LTE and cable devices. When the interference reaches some critical level, the output of the STB (video signal to a television screen) will pixelate or macroblock, and video frames may be dropped and not displayed.

In reality, cable television channels are spread across the cable spectrum. Similarly, 4G/LTE channels are spread across a variety of frequencies depending on the network provider and geographic location. However, with large deployments of LTE devices and a large installed base of STBs and cable modems, even a small probability of interference can result in hundreds of thousands of affected users.

B.2 Experiment Design

To help quantify the potential for interference, we designed several reverberation chamber tests. The use of a reverberation chamber was selected because it provided an environment in which the device under test could be exposed to an interfering signal from all incidence angles and polarizations (as the stirrer turns). One disadvantage of using a reverberation chamber is that we cannot replicate the exact results of the 61000-4-3 tests, which are done in an anechoic chamber. Measuring and calculating the electric field strength of a radiated broadband signal is not trivial.

Figure B.1 depicts the test setup for the reverberation chamber tests. Like most radiated susceptibility tests, there is an RF signal generator outside the test chamber feeding a broadband antenna inside the chamber. For these tests, the signal generator was setup to simulate a 4G/LTE signal emanating from a mobile device at a user-specified carrier frequency and channel width. To monitor the field level inside the reverberation chamber, we use a second broadband antenna connected to a spectrum analyzer.

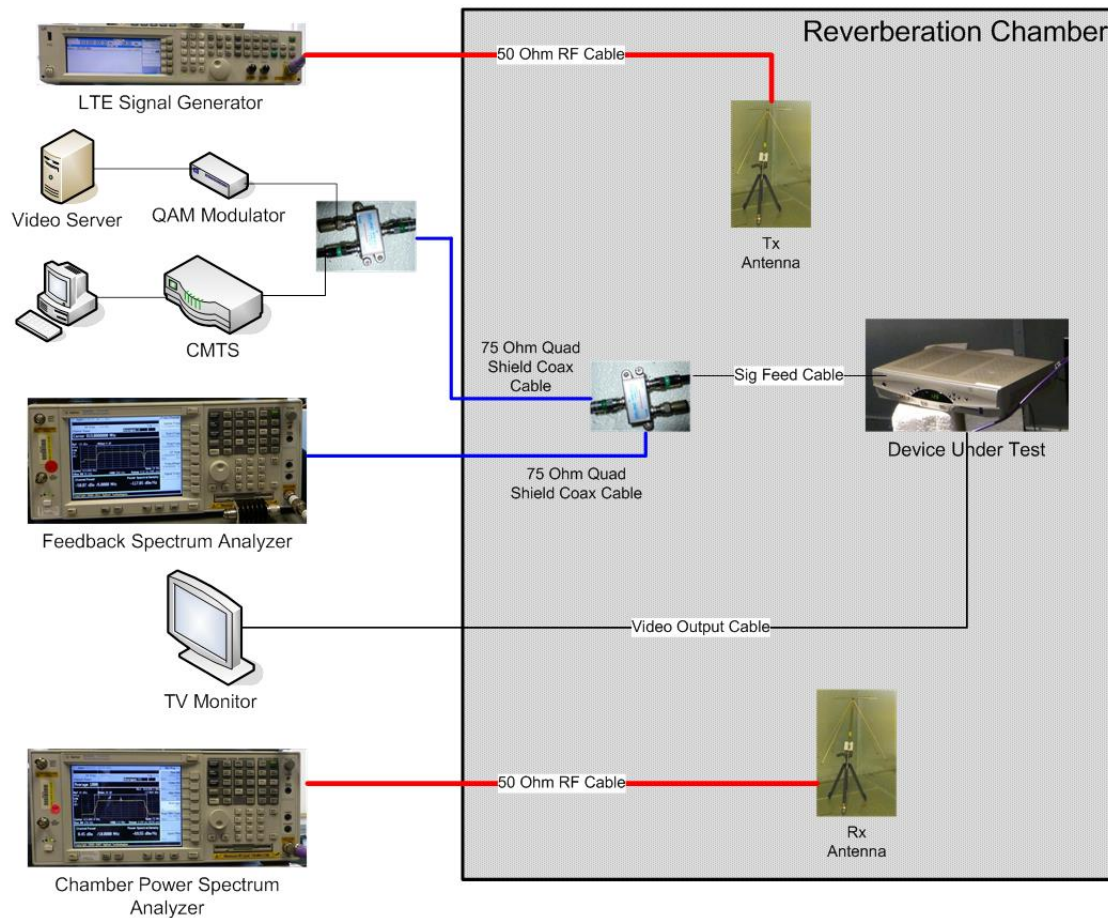


Figure B.1. Interference test performed in a reverberation chamber.

To simulate the cable STB (the DUT) being connected to a real cable network, it was fed with data from a streaming video server and RF modulator located outside the chamber. The video output from the STB was fed to a TV monitor located outside the reverberation chamber. To monitor the signal going into the STB, a splitter was placed as close to the STB as possible. One output was connected to the STB input and the other was fed outside the chamber to a spectrum analyzer.

The reverberation chamber used in this testing has dimensions of 4.2 m x 3.6 m x 2.9 m. It is equipped with two stirrers, one spanning floor to ceiling and one spanning wall-to-wall. Both of these stirrers moved continuously during the testing of the STB. While the stirrers were moving, a 4G/LTE signal was radiated into the chamber at the carrier frequency matching the downstream channel frequency to the STB.

Three carrier frequencies were tested for each STB: 627 MHz, 711 MHz, and 819 MHz. These frequencies were chosen as a representative sample of existing and possible future overlap between the cable and wireless systems. In all cases, the LTE channel was fixed at 10 MHz wide. The maximum number of resource blocks allowed in the LTE channel were used and populated with

simulated data. Figure B.2 shows a time plan for a frame of the LTE signal used in most of this testing.

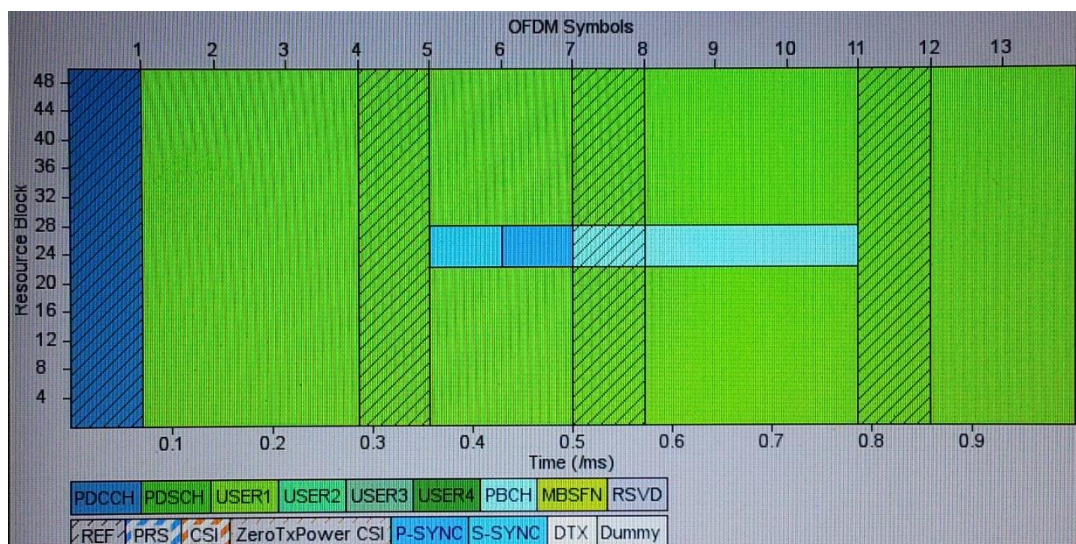


Figure B.2. LTE Signal time plan for each frame.

The output of the STB was monitored as the power of the radiated LTE signal was stepped by a fixed increment until the DUT “failed.” A failure was defined to be when the video picture became pixelated for any period of time. Depending on our chosen definition, the results could be shifted one way or the other.

In addition to the radiated testing, we performed subsequent testing using a direct injection setup where the previously radiated interfering LTE signal was directly added to the cable signal via a splitter. This was done to eliminate radiated field variables from the test setup and focus on a few key attributes. Also, all of the direct injection testing shown was done with the same STB. The attributes being examined in the direct injection testing will be discussed in Section B.4, and are presented separate from the radiated test results given in Section B.3.

B.3 Radiated Measurement Results

For the measurement procedure described above, seven different STBs were tested. STB models ranged from legacy devices to new devices not yet deployed. In these tests, well-shielded cables were used throughout the conductive path to ensure that the results were indicative of only the DUT’s susceptibility and not the shielding of the cable or splitter. Figure B.3 shows the results of the STB testing. STB 1 is a legacy device that is mostly phased out and has been replaced with newer technology. STBs 2-6 represent most of the STBs currently deployed in the U.S. STB 7 is new, and has not been widely deployed.

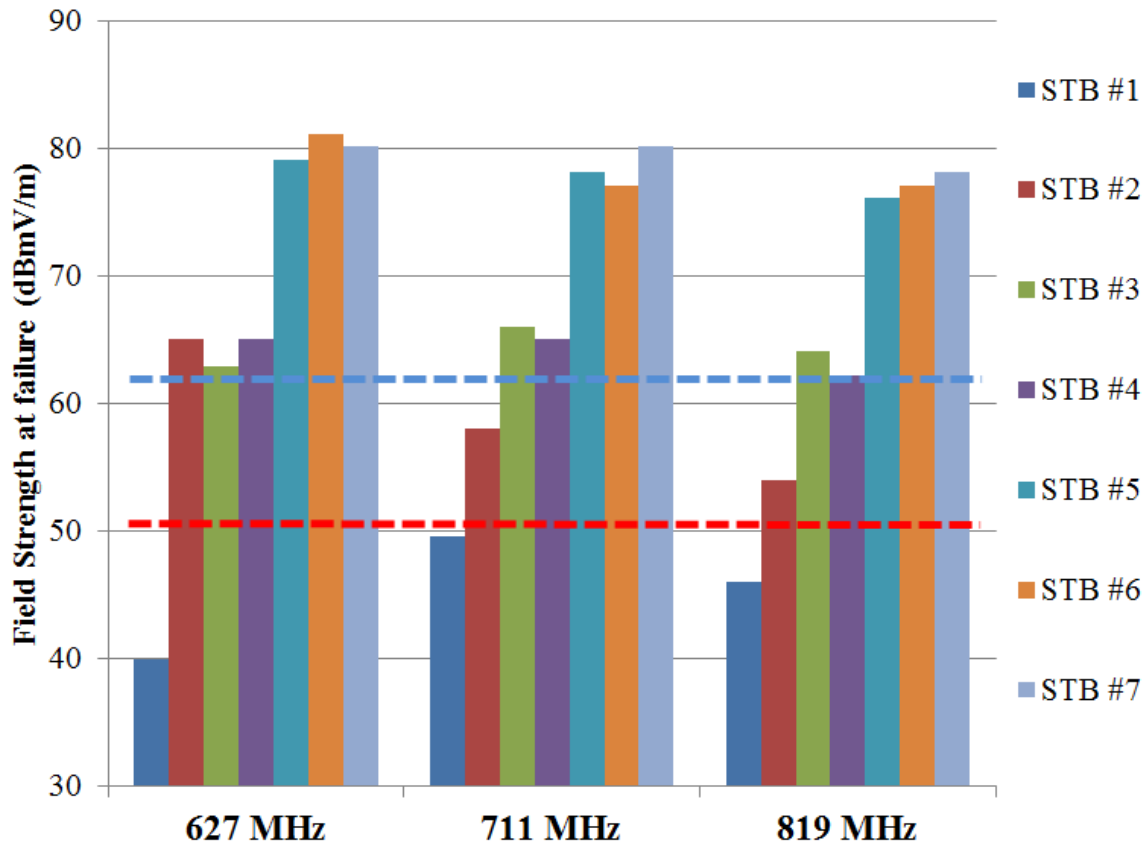


Figure B.3. Susceptibility test results for cable set-top boxes.

The results shown in Figure B.3 show the measured field strength [dBmV/m] at failure. This level represents the electric field strength of the radiated 4G/LTE signal present inside the reverberation chamber at the time the STB met the failure criteria.

Also shown on this graph are two dotted lines representing the estimated field strength levels that a commercial cell-phone may generate, assuming an isotropic radiation pattern at a measurement distance of 1.52 m. The upper line (blue) represents the maximum field strength corresponding to a cell phone transmitting +23 dBm EIRP (about 0.64 V/m), and the lower line (red) represents a typical field level corresponding to a cell phone transmitting +11 dBm EIRP (about 0.4 V/m).

The field strength at the time of failure was calculated from the measured channel power from the “chamber power spectrum analyzer,” shown in Figure B.1. This channel power was measured over a 10 MHz integration bandwidth that completely overlapped with the radiated 4G/LTE signal. It was also averaged as the stirrers rotated continuously. The averaged channel power measurement was then converted to approximate field strength following [B5]:

$$\langle E_R^2 \rangle = \frac{320\pi^2}{\lambda^2} \langle P_{rec} \rangle [V / m], \quad (1)$$

where λ is the wavelength in meters and $\langle P_{rec} \rangle$ is the average channel power measured in watts. Embedded in (1) are a few key decisions about the measurements that were conducted. Annex D of IEC 61000-4-3 [B6] requires that the maximum or average power density be used. Here, we chose to use the average field. This allows for more easily reproducible test results. This also avoids any ambiguity that might exist in the IEC standard regarding broadband, modulated signals.

B.4 Direct Injection Measurements

We showed above the results for the STBs themselves, using test method described in Section B.2. However, additional experiments were conducted using the direct injection setup that allowed us to focus on only a few variables, without having the added complexity of radiated measurements and a reverberation chamber. Using the direct injection setup, we examined the impact of a variety of test signals and the use of a pulsed signal as the interfering test signal.

The test signal chosen for the radiated test results shown in Figure B.3 was driven by the specific concern of 4G/LTE signals interfering with intended cable network communications. The signal used was generated to represent a typical 10 MHz signal loaded to capacity with data that might be transmitted from an LTE handset to a base station (i.e., up-link). If we set the specific concerns of this case aside, should an LTE signal be the one used to replace the AM signal shown in 61000-4-3? LTE signals are extremely prevalent in today's RF environment and indications are that the modulation will continue to exist for many years.

Let's assume that we did want to use an LTE signal (or any other complex modulated signal) for standardized immunity testing. Which LTE signal should we use? What bandwidth should the signal have? What (if any) data should the signal be loaded with? These are all important questions that need to be addressed as there are many different varieties of LTE signals.

To demonstrate this, we created two different LTE signals (in addition to the one used in Section B.3). The first signal was a 20 MHz wide LTE signal that had the maximum number of resource blocks allocated and loaded with data. The time-plan and frequency domain representation are shown in Figure B.4.

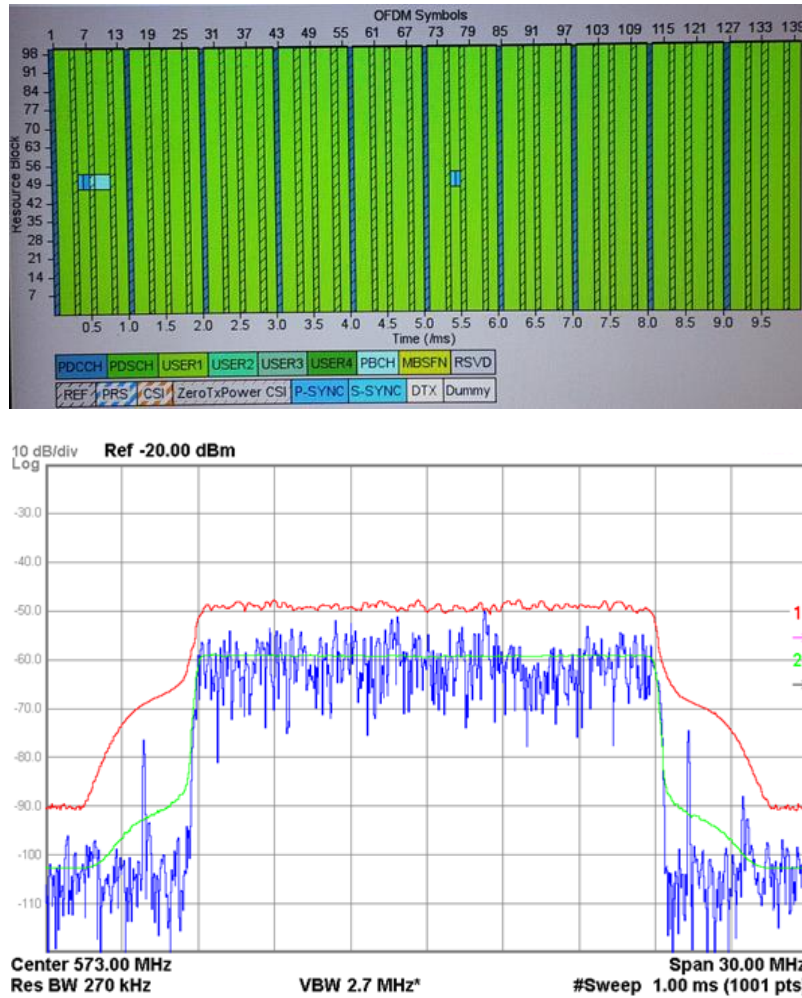


Figure B.4. Time plan (top chart) and frequency domain plot of the 20 MHz LTE signal (lower chart). Shown on the frequency domain plot are the maximum (red), average (green), and instantaneous value (blue) of the signal.

The second signal we created represents a simulated voice-over-LTE (VoLTE) signal. Though VoLTE has yet to be widely deployed in the U.S., its signal is an interesting one. The idea behind VoLTE is similar to voice-over-internet protocol (VoIP), the voice communication is encapsulated into a data packet and sent over the data network. Given the total number of resource blocks that a 10 MHz LTE signal may contain, if the voice data are the only data that need to be sent over the channel at the time the user is making a call, much of the signal would be left vacant. This results in an LTE signal with many sharp transitions from high to low amplitudes. The frequency domain representation of our VoLTE-like signal is shown in Figure B.5.

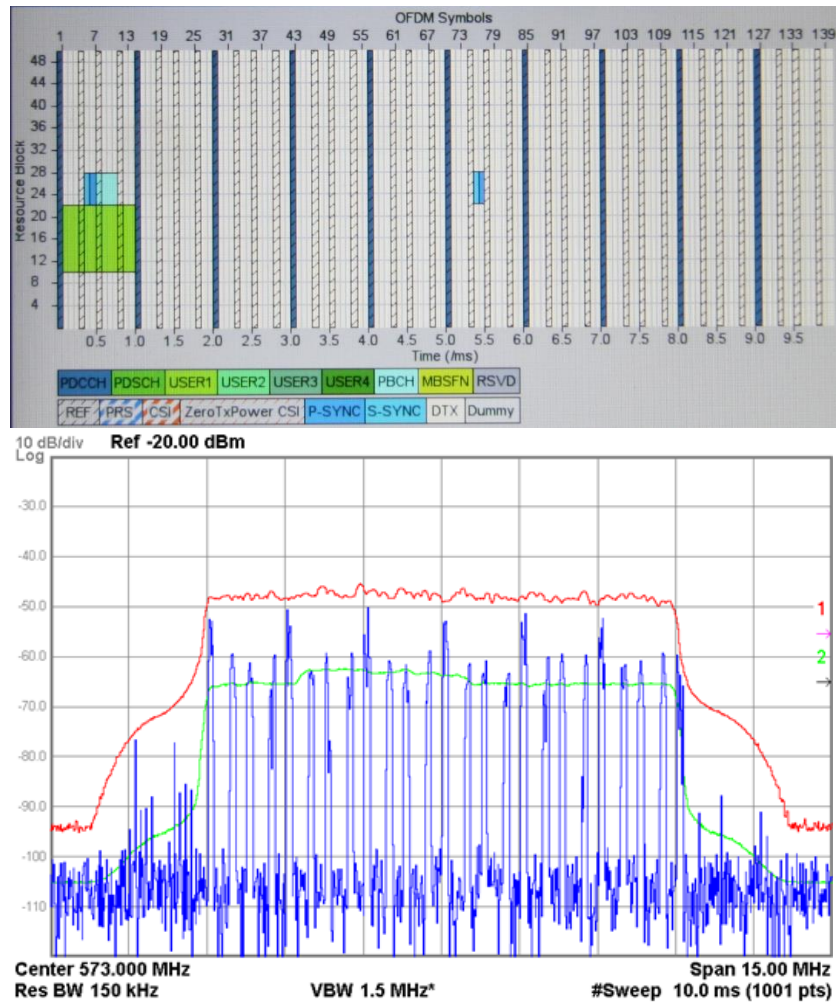


Figure B.5. Time plan (top chart) and frequency domain plot of the VoLTE-like signal (lower chart). Shown on the frequency domain plot are the maximum (red), average (green), and instantaneous value (blue) of the signal.

To examine what, if any, impact these different LTE signals have on the measured immunity performance of a device, we used the direct injection test setup described in Section B.2. This setup allowed us to focus only on the test signal, and eliminated many of the other variables that exist when conducting radiated testing. We began by testing the STB with the AM signal described in 61000-4-3. For comparison, we then conducted the same test using the 10 MHz LTE signal (also used in the radiated testing), 20 MHz LTE signal, and VoLTE signal. The results are shown in Figure B.6.

Figure B.6 also shows the results of testing when the spectrum analyzer's bandwidth is restricted to 6 MHz (instead of being the same as the signal bandwidth). The 6 MHz bandwidth of the spectrum analyzer mimics what the STB sees when tuning across a 6 MHz wide channel. The fact

that this result is different than the corresponding 20 MHz wide signal indicates that the bandwidth of the DUT may need to be something that is accounted for when testing. This is discussed in detail in Section 3.2.5.

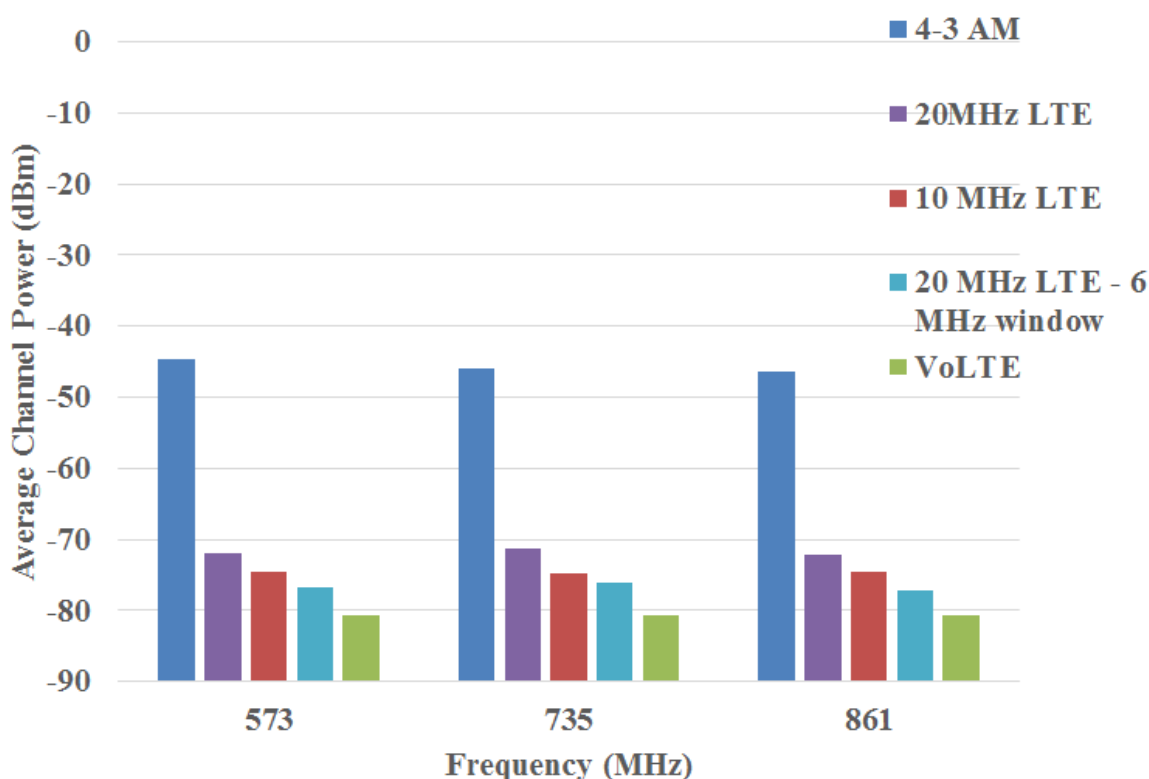


Figure B.6. Average channel power at failure for the direct injection testing of one STB, showing the variations caused by the choice of test signal.

Note that correlating these direct injection results to field strength levels is difficult (as was shown in Figure B.3), but the relative difference shown should translate. That is, the 35 dB difference between the AM signal and the VoLTE-like signal shown should also be seen if the same test were performed with the radiated setup discussed earlier.

The results shown are in terms of average channel power [dBm]. By itself, this does not completely describe the test signal. To be more complete, Table B.1 shows the peak to average ratio of the test signal. For the sake of brevity, only the peak to average ratio at 735 MHz is shown.

Table B.1: Peak to Average Ratios of Test Signals

Signal	Ratio [dB]
4-3 AM	3.3
20 MHz LTE	9.2
10 MHz LTE	8.7
VoLTE-like	14.6

Recently, there has been some discussion about the use of pulsed signals as a substitute to the original AM signal specified in 61000-4-3. Pulsed signals are thought to be a reasonable approximation to modern communication signals. As a result, the IEC 60601-1-2 standard has implemented a revised signal to be used in their radiated immunity testing of medical devices (see Table 9 of [B7]). Depending on the test frequency and the service being tested against (i.e., protocol; LTE, Wi-Fi, etc.), the test signal is a CW signal at some carrier frequency modulated at a 50% duty cycle and at either 18 Hz or 217 Hz. For the specific set of LTE frequencies discussed here, [B7] recommends an 18 Hz pulse modulation for the 704 MHz - 787 MHz band and a 217 Hz modulation for the 800 MHz - 960 MHz band.

For comparison, we tested a STB using a CW signal pulsed at a variety of frequencies. The same STB and measurement setup were used here as was used in the data shown in Figure B.6. Figure B.7 shows the pulsed testing results. The results of the testing with the AM signal and VoLTE-like signal (also shown in Figure B.6) are also shown.

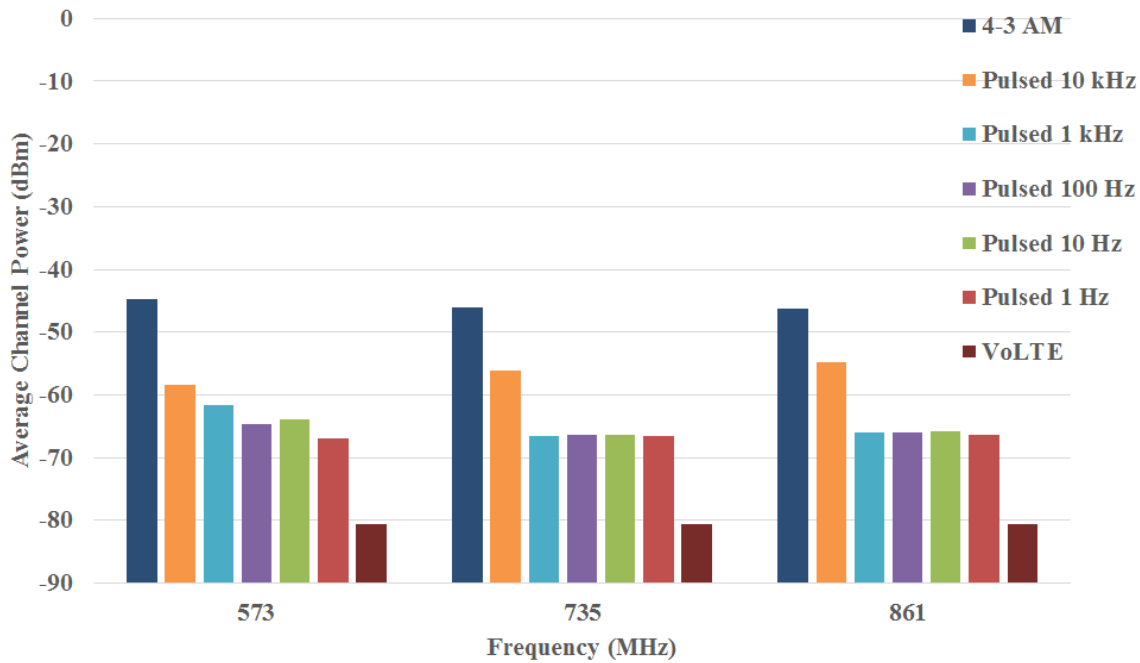


Figure B.7. Average channel power at failure for direct injection testing of one STB, showing the variations caused by the use of different pulsed signals. The results from the use of the AM signal and VoLTE-like signal are shown for comparison.

B.5 Discussion and Summary

We have shown, immunity testing of broadband signals is inherently complicated and many of the variables are intertwined with each other. For this reason, we have intentionally not given suggested solutions to the questions we've raised.

Significant research in many of the areas we've discussed is still needed in order to understand (not just demonstrate) what an adequate immunity test should be given today's modern RF environment and intelligent DUTs. As the challenges discussed here are researched, the community needs to discuss the best way to move forward. Because there are so many variables involved in this type of testing, standardizing the test method may be a good approach to ensuring that a repeatable method is established.

Once a primary standard/test method is established, each individual product type may require modifications in order to appropriately test the device for specific applications. For example, the test method developed and used for testing critical infrastructure equipment may be more rigorous than the method used to test in-home consumer electronic equipment.

Focusing on the cable equipment shown and tested here, there is one additional challenge to note. Once a STB is installed, its configuration can change over time. Typically, the STB is installed by

a properly trained technician in the user's home or business. However, after the installation, the user is free to change the configuration (e.g., move the STB to another room). This presents a difficult problem for immunity testing, namely, the DUT's configuration may be different than was tested, and may change after installation. This may also prove to be an important consideration in the testing of any critical infrastructure equipment; any changes in configuration or installation that differ from the test method could produce something more or less immune.

B.6 Appendix B References

[B1] J. Coder, J. Ladbury, D. Hunter, "Characterizing a Device's Susceptibility to Broadband Signals: A Case Study," Proceedings of the 2014 IEEE International Symposium on Electromagnetic Compatibility, August, 2014.

[B2] "Analysis of interference to cable television due to mobile usage in the digital dividend," University of Twente/Radio Telecommunications Agency, Netherlands, 2010.

[B3] B. Randhawa, I. Parker, S. Antwi, "LTE Interference into Domestic Digital Television Systems," Cobham Technical Services Report 2010-0026, January 2010.

[B4] T. Wheeler, "The path to a successful incentive auction," <http://www.fcc.gov/blog/path-successful-incentive-auction-0>, access December 15th, 2013.

[B5] J. Ladbury, G. Koepke, D. Camell, "Evaluation of the NASA Langley Research Center Mode-Stirred Chamber Facility," National Institute of Technology Technical Note 1508, January 1999.

[B6] IEC 61000-4-3 ed3.2, Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test. http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/43958

[B7] IEC 60601-1-2 Ed4.0, Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests. http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/49272!opendocument&preview=1

Appendix C. EM Field Measurements and Antenna Characteristics

C.1 Introduction

One of the challenges of determining the immunity or coexistence characteristics of a device is to first determine likely field exposure levels. This is complicated by the fact that the level can depend on when or where the field is measured. One possible measurement setup is given in Figure C.1. An antenna is placed in an unknown environment and a spectrum analyzer records the power received by the antenna. The measured power is then used to estimate the fields which generated that power. Unfortunately, for the arbitrary problem described here, there is no solution. We know nothing about the environment. Is it transparent to RF? Is it lossy? Is it highly reflective? Is the environment stable or can it change over time? We don't know where any sources might be relative to our antenna (and the sources may not be stationary), we don't know if the transmitted signal is stable over time or if it is modulated in some manner and we don't know the polarization of the incoming signal. To further complicate matters, the antennas used in these measurements are typically evaluated in a free-space environment and those evaluations may not be valid once the antenna is placed into a different environment. Due to these complications, several simplifying assumptions must be made to make the problem tractable.

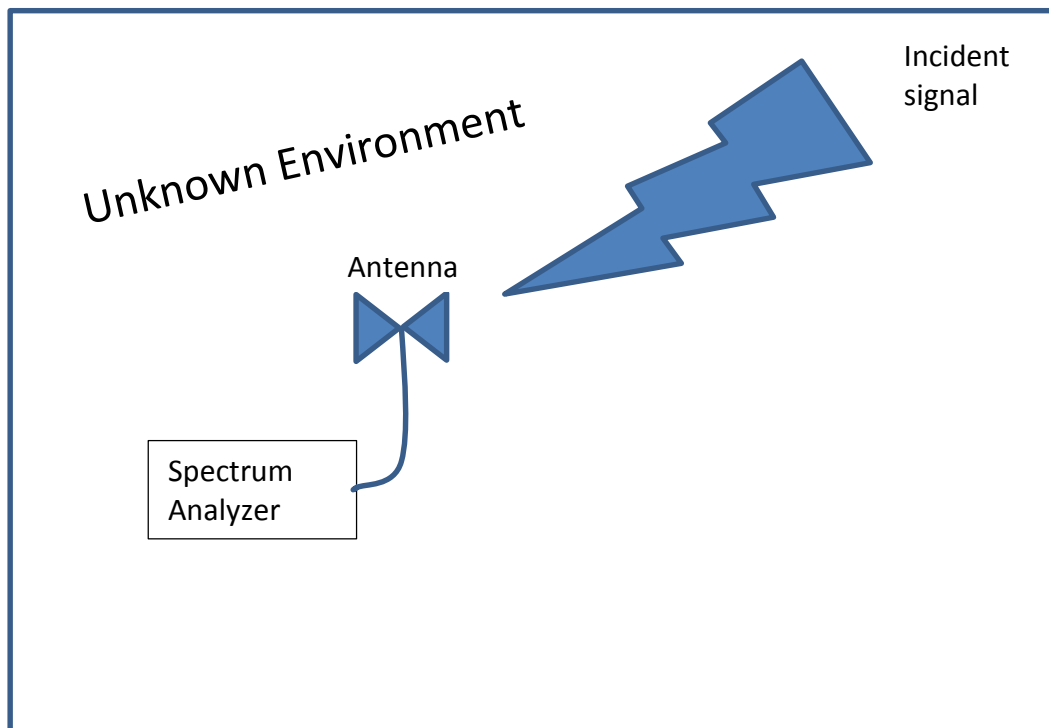


Figure C.1. Conceptual measurement setup for monitoring ambient fields.

For our purposes, we will simplify the problem using two sets of assumptions. The first is to model the problem by assuming a free-space environment and an incident plane wave emanating from a stationary source. The second is to assume a measurement in a highly reflective environment which can be modelled as a reverberation chamber.

Free-space Environment

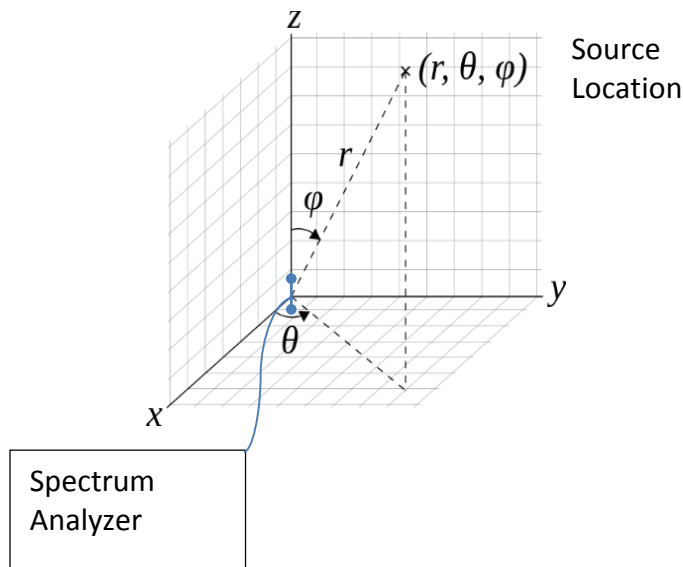


Figure C.2. Free-space measurement model.

C.2 Free-Space Model

The free-space model is shown in Figure C.2. A simple initial approach for converting received power to field level involves the application of the free-space broadside or boresight antenna factor which is used to convert received voltage (which can be determined from received power) to field for the very special case of a source aligned and copolarized with the antenna. This may be a reasonable first-order correction, but it will generally underestimate the actual field level. But how much of an underestimate and can we estimate some sort of bound? For now, we will assume that the receiving antenna is linearly polarized with an antenna-factor pattern given as $AF(\varphi, \theta)$ with coordinate system shown in Figure C.2. We will assume that the source and receive antenna are copolarized.

To evaluate the effect of not knowing the location of a distant source, we will assume that the source is equally likely to be located at any point on a sphere, and then calculate the coupling as a function of φ and θ . We will begin with a detailed evaluation of an electrically short dipole antenna located at the origin and aligned with the Z axis as shown in Figure C.2.

Our first problem is to generate uniformly distributed points on a sphere. This is a common problem with multiple methods for generating such points. We chose a simple geometric method [C1], for which we choose θ to have a uniform distribution $U[0, 2\pi)$, but φ is a little more complicated. We cannot simply choose φ to be uniformly distributed $U[0, \pi]$ or we wind up with too many points near the poles. The correct approach is to let v have a uniform distribution $U[-1, 1]$, and let $\varphi = \cos^{-1}(v)$.

For a short dipole, the antenna factor pattern is independent of θ and can be written as $AF\left(\frac{\pi}{2}, 0\right) \sin(\varphi)$, where $AF\left(\frac{\pi}{2}, 0\right)$ is the broadside calibration of the antenna factor, and $\sin(\varphi)$ is the error we make in assuming that the broadside calibration is good enough for a general conversion from received voltage to field. From this, we can determine a correction factor needed to give us the correct field, which is simply $1/\sin(\varphi)$. Notice that this correction factor is simply 1 for a true broadside source, but can be very large if the source is located near the poles. Fortunately, a source is unlikely to be near the poles, but we can still analyze the distribution of the correction factor assuming that the source location is equally likely over the surface of a sphere.

For that, we begin with $\varphi = \cos^{-1}(v)$, so $v = \cos(\varphi)$, $\sin(\varphi) = \sqrt{1 - v^2}$. This gives a correction factor $u = \frac{1}{\sqrt{1 - v^2}}$. Since we know that $v: U[-1, 1]$, we can compute the distribution of the correction factor, u . We know that $u \geq 1$, since the antenna factor is maximized for broadside illumination. We can determine the cdf (cumulative distribution function) of u as

$$\begin{aligned} F(u) &= P[u \leq U] = P\left[\frac{1}{\sqrt{1 - v^2}} \leq U\right] \\ &= P\left[-\sqrt{1 - \frac{1}{U^2}} \leq v \leq \sqrt{1 - \frac{1}{U^2}}\right] \\ &= \sqrt{1 - \frac{1}{U^2}} \end{aligned}$$

for $U \geq 1$ throughout.

$$\text{Hence, } F(u) = \sqrt{1 - \frac{1}{u^2}}, u \geq 1 \quad (1).$$

Differentiating the cdf gives the pdf (probability density function)

$$f(u) = \frac{1}{u^3 \sqrt{1 - \frac{1}{u^2}}}, u \geq 1 \quad (2).$$

C.2.1 Uncertainty Analysis for the Free Space Model

Given the pdf above, we can determine several characteristics related to bias and uncertainty for the assumed model. As mentioned above, use of the free-space model will generally underestimate the actual field. We can now estimate the average bias by determining the mean of the derived distribution, which is $\frac{\pi}{2}$. This implies that, on average, we underestimate the field by a factor of $\frac{\pi}{2}$.

Unfortunately, the tail of this distribution is quite long (falls off as roughly $\frac{1}{u^3}$ for large u), which implies an infinite variance. This implies that traditional approaches to uncertainty based on variance or standard deviation are not possible. Instead, we can estimate a range in which the actual field is expected to fall. Without correcting for bias, we know that the field will never be less than the field computed from received power, but could be substantially greater. However, we can show that for the model presented here, the correction factor will be less than 3.9, or 11.8 dB for 95 % of the possible source locations. Similar ranges can be calculated for other possible coverage intervals.

This analysis does not account for differences between the polarization of the incident field and the dipole. To do so is uncomplicated, but it would only increase the spread of the pdf and the associated uncertainty. The same is true for directional antennas, which increase the probability of “missing” a signal that arrives outside of the main beam of the antenna. Again, this will increase the spread of the pdf and the associated uncertainty.

C.3 Reverberation Chamber

The reverberation chamber model is shown in Figure C.3. Here, we assume RF energy is introduced into the chamber either through an internal source or from an external source and coupled through apertures in the chamber. If we assume that the receiving antenna is placed in a reverberation chamber, then conversions are relatively straightforward. From Hill [C2], there are simple relationships between average received power and squared field for any well-matched and lossless antenna. The received power P_r is simply the product of the scalar power density S_c and the effective aperture of the antenna $A_e = \frac{\lambda^2}{8\pi}$, which is identical for all matched and lossless antennas in a reverberation chamber:

$$P_r = S_c A_e = S_c \frac{\lambda^2}{8\pi}. \quad (3)$$

The power density can be given in terms of the average squared total electric field as $S_c = \frac{E^2}{\eta_0} = \frac{E^2}{120\pi}$, where η_0 is the wave impedance of free space. Substituting into the above equation (3), we have

$$P_r = \frac{E^2}{120\pi} \frac{\lambda^2}{8\pi} \quad (4)$$

From this, we can determine E^2 as

$$E^2 = \frac{960\pi^2}{\lambda^2} P_r \quad (5)$$

If we are interested in a squared Cartesian component of the field rather than the squared total field, we can simply divide by 3, since all components are assumed to be equivalent.

If the receiving antenna is lossy and/or poorly matched, the received power will be reduced by these imperfections resulting in underestimates of the electric field. However, if the imperfections are known, correction factors can be applied to account for them.

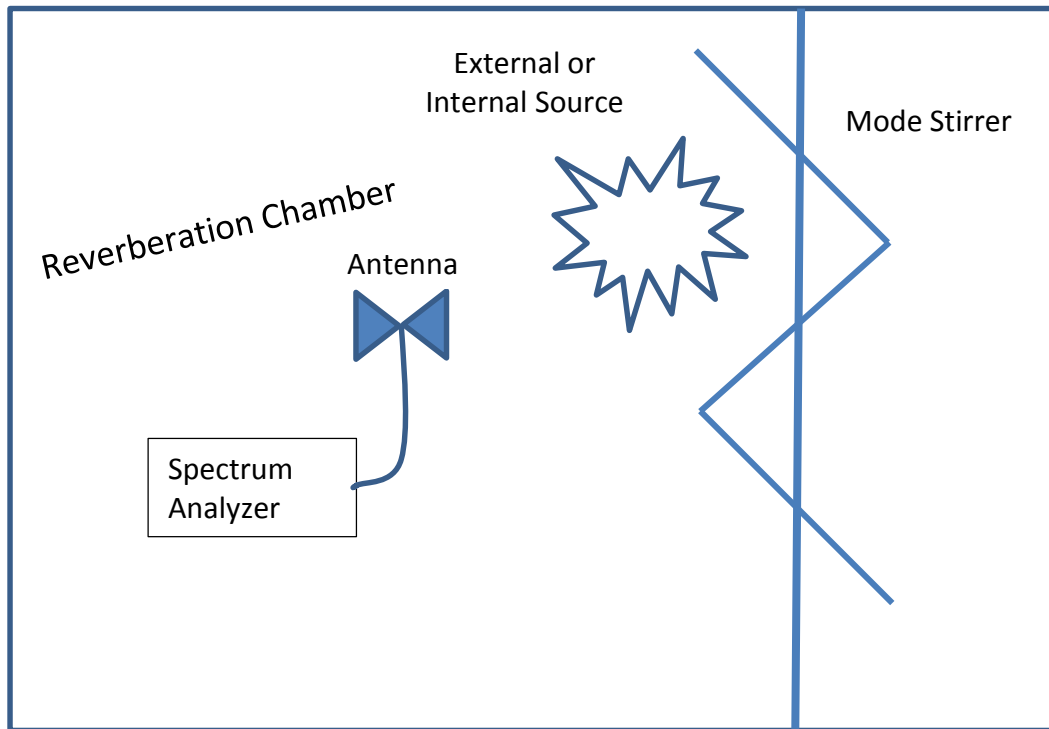


Figure C.3. Reverberation Chamber measurement model.

C.3.1 Uncertainty Analysis for Reverberation Chamber

In a reverberation chamber, uncertainty is often reduced by use of a movable reflective mode stirrer or other mechanical means of changing boundary conditions and recording and averaging measurement samples of the changing environments. This assumes a stable transmitted signal such that changes in the received signal are caused by changes in boundary conditions. The uncertainty analysis of this measurement model is complicated for modulated signals due to the dynamic nature of the measured signals. Signals can change simply due to changes in use requirements (telephones or radios used as needed, video over Wi-Fi while watching a movie but not before or after), modulation, changes in source location and orientation, but can also change due to movement of reflecting surfaces (elevators, automobiles). The movement of reflecting surfaces is analogous to moving a mode stirrer in a chamber, but we cannot separate changes due to moving reflectors from changes due to other mechanisms. Because of this, we present an uncertainty analysis assuming the measurement location is equivalent to a reverberation chamber with a single mode stirrer position (worst case). From analysis presented in [C3], if the true average received power is 1 mW, we can expect a measured received power at a given single mode stirrer position to fall between 0.026 mW and 3.69 mW with approximately 95 % probability. This allows measured values below 0.026 mW with 2.5 % probability and above 3.69 mW with 2.5 %

probability. Alternatively, we can say that for a given measured received power, the actual average received power could be 15.9 dB higher or 5.67 dB lower.

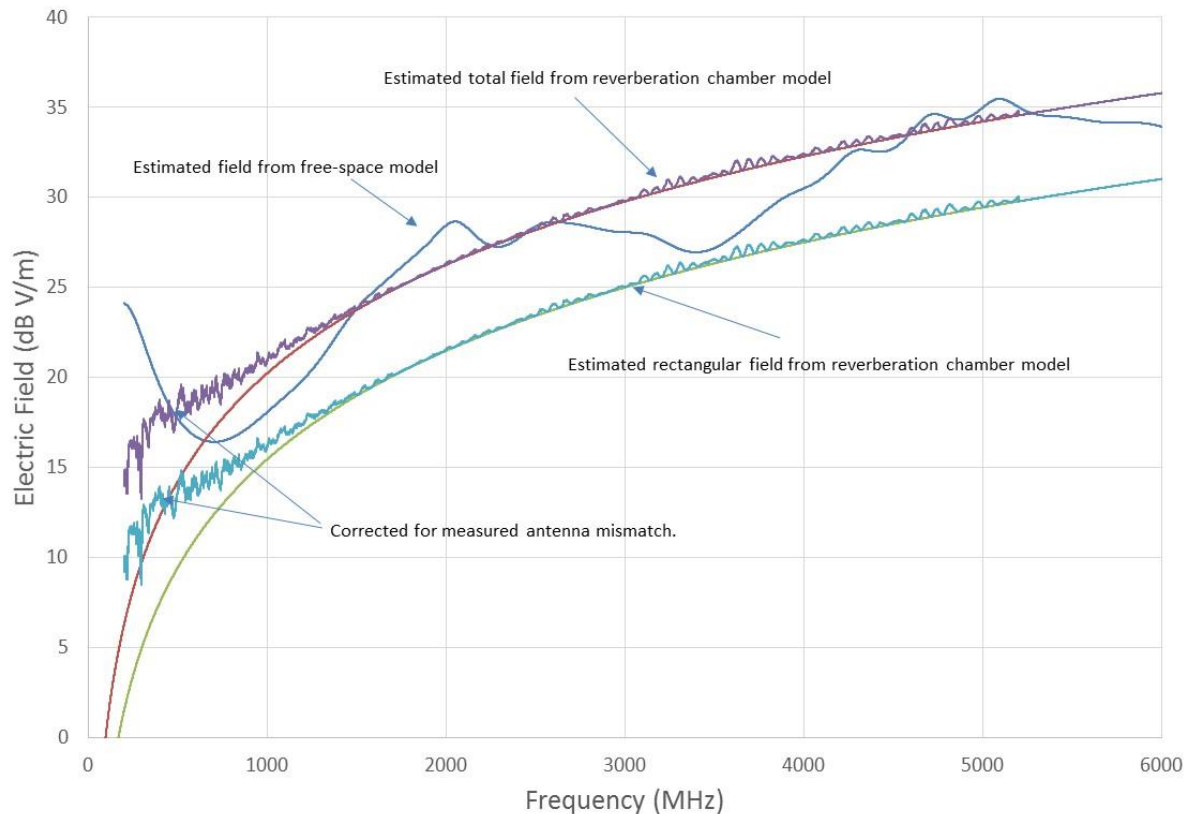


Figure C.4. Comparison of estimated field for free-space model and reverberation chamber model.

C.4 Comparisons

We can compare the two approaches, the receive antenna in free-space or in a highly reflective environment modeled by a reverberation chamber, and observe how well the estimates of electric field strength agree for a given received power. To do this, we used the characteristics (antenna factor and input impedance) of the antennas used for the apartment building measurements described in Section 2.1 and assumed a received power of 1 mW (0 dBm). We then computed the electric field (in dBV/m) generated by each procedure. For the free-space calculation, we used antenna factors that were evaluated both numerically and on the NIST Open Area Test Site (OATS). For the reverberation chamber, we assumed perfect antennas (smooth curves) and also applied corrections for the measured impedance mismatch of the antennas (jagged curves). The

results are given in figure C.4. Note that the estimated field, based on the free-space approach, is consistently greater than the estimated Cartesian electric field generated for the reverberation chamber approach, but generally less than the estimated total electric field, also generated for the reverberation chamber approach.

C.5 Discussion

Regardless of the method used to estimate field based on received power, these estimates will have very large uncertainties even if the measurements of received power have very low uncertainties. For the free-space model, this is due to the possibility that a source could be located in a null of the measurement antenna. This uncertainty could be reduced by measuring with multiple antennas simultaneously, as long as the composite measurement pattern of the multiples antennas removes the effects of antenna nulls. For the reverberation chamber model, the uncertainty can also be reduced by measuring with multiple antennas simultaneously. This would reduce the probability that all measurements are taken at nulls in the chamber.

[C1] _____, Wolfram MathWorld™, Mathematics Resource (web page), <http://mathworld.wolfram.com/SpherePointPicking.html>, (referenced Nov. 14, 2014).

[C2] D.A. Hill, *Electromagnetic Fields in Cavities: Deterministic and Statistical Theories*. Piscataway, NJ: IEEE Press/Wiley, 2009

[C3] J.M. Ladbury, G.H. Koepke, and D.G. Camell, *Evaluation of the NASA Langley Research Center Mode-Stirred Chamber Facility*. NIST Technical Note 1508. 1999.