**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| **In the Matter of** | ) | |
| | ) | |
| **Regulatory Issues Arising from** | ) | |
| **Health Care Devices that Incorporates** | ) | **ET Docket No. 10-120** |
| **Wireless Communications Networks** | ) | **FDA Docket No. FDA-2010-N-0291** |
| | ) | |
| | ) | |

# Comments
# Submitted for the Public Meeting
# on
# Converged Communications and Health Care Devices
# Impact on Regulation

These comments[1] are offered as a contribution to the joint FCC/FDA Public Meeting addressing Converged Communications and Health Care Devices Impact on Regulations. The conclusion of these comments is that with appropriate planning and careful implementation, wireless has a beneficial and growth contribution to be made to health care. The development of dynamic spectrum access as a spectrum management methodology is a key enabler to releasing the beneficial potential of wireless technology for health. To release the beneficial value of these new health care applications the FCC

[1] These comments are the personal views of Stephen Berger. They were formed through involvement in a number of related issues, including:

- involvement with numerous FCC dockets,
  - currently including modification to the UPCS Band service rules under docket 10-97 and
  - the proposal for a Medical Micropower Network (MMN) under docket 09-37,
- Chairing multiple ANSI and IEEE standards committees, several of which have subsequently been adopted by the FCC or been recognized by the FDA,
- A long history of involved in disability and rehabilitation engineering issues,
- Work as a laboratory assessor and development of conformity assurance systems.

should release the potential of unused spectrum by moving to dynamic spectrum access service rules. These rules must be crafted so as to allow devices to select from and implement a range of interference management and mitigation measures, so as to achieve a level of reliability appropriate to that specific device. The FDA should then insure that medical devices implement an appropriate set of interference management and mitigation measures to insure a level of reliability needed by the specific purposes a device serves.

In order to maximize the beneficial use of wireless for health care applications three issues must be resolved in a satisfactory manner:

1. Operating spectrum
2. Reliability
3. Conformity Assurance

Health care applications require spectrum in which to operate. Those spectrum assignments must be planned so as to coexist with other wireless services. It is increasingly clear that the historic methods of "command-and-control" spectrum management have passed the end of their useful life. Paper-and-Pencil assignment of unique spectrum for every application is too wasteful of spectrum to go into the future. The alternative, developing increasingly refined dynamic spectrum access methodologies, opens up the under utilized capacity of spectrum, so as to allow many socially beneficial new wireless applications to be introduced.

Concurrent with the operating spectrum issue, wireless services, especially for health care, must achieve levels of reliability appropriate to their application. The required level of reliability varies with the application. Within the range of health care applications are certainly some of uses of wireless that demand the highest levels of reliability. Equally, other applications are quite tolerant of interference. In these applications the consequences of interference are both trivial and mitigations readily available. One can contemplate a wireless link carrying life-critical, time-dependent patient monitoring data in an ICU versus another that delivers a patient's entertainment selection. For the first example, time is critical, and the potential consequences of a communication failure are enormous. There is little time for alternative solutions to be employed. In contrast if a patient's remote control is interfered with, a friend or nurse can

change the channel manually. Even if no assistance is available the consequences are minor unless it occurs during the final 2 minutes of an important NFL game. However, both links potentially could be using the same frequency band and the same RF protocol.

Conformity assurance is a term to describe the combined set of systems and processes that assure that products meet requirements in the field, during actual use. Regulatory compliance testing and engineering standards are important components are important parts of conformity assurance. However, a conformity assurance system includes far more. A complete assurance system must include feedback loops that provide information about the fielded performance and trigger appropriate remedial measures, when necessary. A conformity assurance system must consider laboratory accreditation and testing quality. It must also include manufacturer quality control and configuration management systems.

## I. Primary Conclusion is that FCC and FDA have different but interdependent roles to play

The primary conclusion of these comments is that the FCC and FDA have different but interdependent roles to play. When these are understood with specificity each agency can facilitate the work of the other and together assure the required levels of reliability and performance are delivered. For manufactures, a well articulated coordination of roles will facilitate device certification because it will be known with clarity what issues must be addressed for each agency.

The FCC's authority and responsibility make it best equipped to deal with the spectrum occupancy issue. It will be argued that the only solution that takes spectrum management into the future is to transition to dynamic spectrum access methods for spectrum coordination. In doing this the FCC should establish in each band a framework that will support a range of interference techniques.

The FDA then, in its role of qualifying medical devices should insure that each device is equipped to provide an appropriate level of reliability for the purpose it serves.

Both agencies have a role in the conformity assurance process. Both must have good sources of information on how devices operate in the field and both must be able to apply remedies when deficiencies are identified.

## II. There is a New Grey Area between Radio Coexistence and RF Immunity

Assuring the coexistence of radio systems has been a core responsibility of the FCC. The Commission carefully coordinates the use of spectrum to insure that different radio services can coexist and not cause harmful interference to each other. In contrast RF Immunity, insuring that devices have adequate immunity to the electromagnetic environment in which they will operate has not been an area the Commission has dealt with much. With unlicensed devices the Commission generally has generally dictated that devices must accept any interference from primary users of the band and left it to manufacturers to determine how they deliver adequate quality of service to their customers. In contrast the FDA routinely requires testing of medical devices to demonstrate that they have adequate RF immunity to protect their users from harmful interference.

There is a new grey area being created between these concepts with the increasing necessity of using dynamic spectrum access and more intense sharing of spectrum. RF immunity has traditionally mean that a device is adequately immune to the electromagnetic spectrum in which it will operate. However, when that device uses wireless communications it must extend its immunity into the realm of coexistence and reliable communication in the presence of a complex and ever changing spectrum environment. RF immunity and communications coexistence become parts of a continuum with significant overlapping areas of concern.

Secondary users of spectrum will need to have support from the band rules so as to be able to provide adequate levels of reliability. This support does not mean that they must have primary use of the band. However, they will require support in the band rules, so that they can implement interference mitigation techniques that are sufficient for them to deliver the reliability they users require. Two examples are standard frame times and notification of intent to transmit. In the UPCS band all devices are required to transmit using frame times that are an integer fraction of 10 ms. The consequence of this rule is that any device that monitors a frequency for 10 ms will know if any other device is currently operating on that frequency. A requirement to announce an intention to transmit provides a similar support. In many applications the critical element to avoiding harmful interference is that a transaction once started can be completed. If a primary user must announce in some manner its intention to initiate operation in an area, then secondary users potentially have the time to complete a transaction and make

plans to either change channels or transition to an alternative mode of operation. In both examples the service rules for the band enable devices to implement measures that are appropriate for their needs.

A simple logic is suggested in which the FCC in setting the service rules for a band makes available a range of interference management techniques and the FDA evaluates devices to insure that they implement the techniques required to achieve a level of reliability appropriate for their purpose.

## III. 'Command and Control' Spectrum Management is no longer viable

As the Commission well knows the old 'command and control' method of spectrum management has passed the end of its useful life.

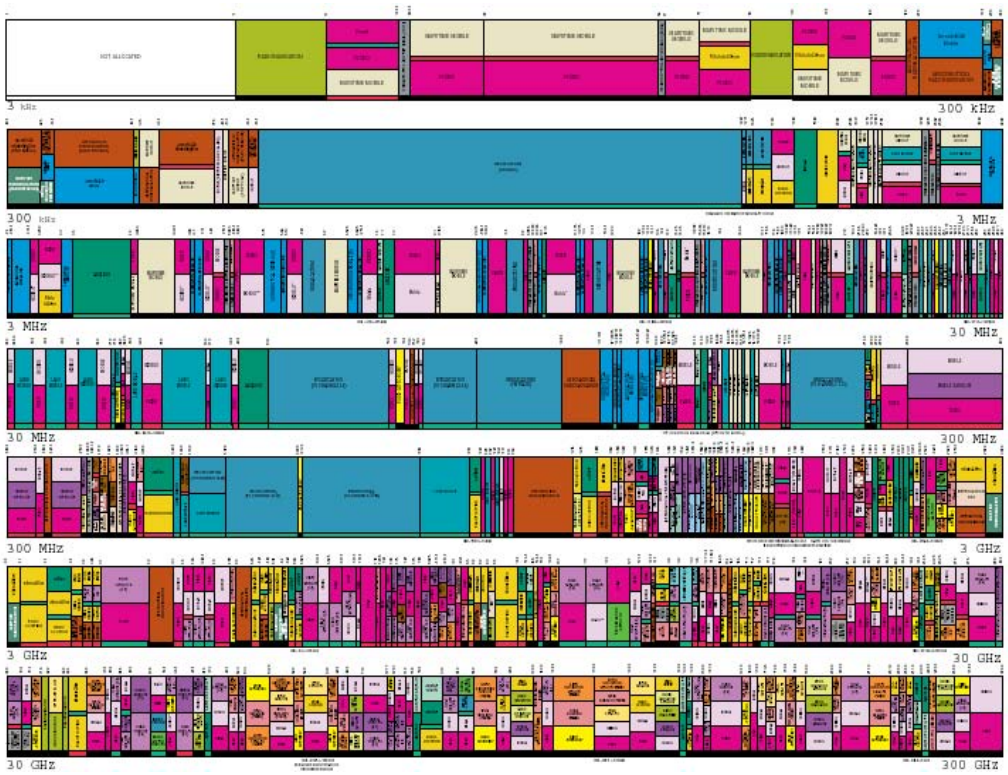


**Figure 1 – Table of Frequency Allocations**

There simply is not spectrum available for the multitude of new wireless services seeking to make their benefits available to society. As Figure 1, the Table of Frequency Allocations, quickly make obvious, there simply are no unallocated frequency available. A 2005 NSF study of spectrum occupancy stated:

*The need to assure access to radio spectrum is at a crossroads. More and more technological alternatives are becoming available and demand for spectrum from both public and private sectors is increasing very rapidly, if not exponentially. Increasingly, there is recognition that most of the spectrum is actually unused and that real root of the problem is that the present system of spectral regulation is grossly inefficient. Current spectral regulation is based upon the premise that slices of the spectrum, representing uses within specified upper and lower frequency bounds, must be treated as exclusive domains of single entities – who are the recipients of exclusive licenses to use specific frequency bands.*[2]

The FCC Spectrum Policy Task Force, NSF and DARPA studies have reported that below 3 GHz, at any specific time and place typically only 5.0% of the spectrum is being used.[3,4,5] This implies that secondary use applications will usually have unhindered access 95% of the time. If interference avoidance and management measures can effectively address the potential for interference in the remaining 5%, where interference is even a possibility, then there is the opportunity to unleash enormous amounts of spectrum for new, beneficial uses.

The general trend of the spectrum occupancy data that shows typically 95% of the spectrum is unused does not deny that there are locations and conditions under which the spectrum is more heavily utilized. For specific bands situations can usually be identified where the spectrum is heavily used. Addressing these unusual cases must be part of a total spectrum management plan. It is important to achieve a balance and neither denigrating the importance of effectively addressing the small percentage of cases were congestion is an issue does, nor to deny the potential of dynamic spectrum management to open up the potential of unused spectrum.

---

[2] Shared Spectrum and IIT Wireless Interference Laboratory, NSF Project: NeTS-ProWIN: Wireless Interference: Characterization and Impact on Network Performance, Subcontract No. SA301-0905 - Spectrum Occupancy Measurements - Chicago, Illinois, November 16-18, 2005,pg. 1.

[3] Report ET Docket 02-135, Spectrum Policy Task Force (SPTF), FCC, Nov. 2002..

[4] Report of the Spectrum Efficiency WG, Spectrum Policy Task Force (SPTF), FCC, Nov. 2002.

## IV. The Myth of Dedicated Spectrum

Some who are accustomed to the beliefs underlying the old "command and control" method of spectrum management will represent dedicated spectrum as the ideal solution. "If only every service could have its own band to operate it all problems would be solved.", some say directly or imply. As has been discussed, assigning unique spectrum to every service is simply no longer possible. This is particularly true for frequency bands having unique characteristics that make it particularly useful for a variety of applications.

However, dedicated spectrum is a myth as a solution for interference problems because, while it might separate different services, it does nothing to deal with the resulting problems of band crowding and coexistence among users of the band. The problem of coexistence is exacerbated as increasing spectrum demand requires restrictive assignments be made, in order to support all the applications crying for bandwidth. With health care applications the user does not care if their device fails because of interference from a similar or a different kind of devices. They only care that they are not receiving the reliability they need from their device. Tight frequency assignments hasten the development of band crowding, as similar devices interfere with each other in high occupancy locations. Future service rules are needed that minimize interference and maximize operational coexistence. It doesn't matter if those rules are coordinating spectrum use among similar or very different devices.

The effectiveness of service rules is maximized as devices are given increase operational options. The more channels and operating modes available, the greater will be the probability that devices will be able to find a channel and mode to operate without interference. In this vein, if a device is given secondary use of bands with a variety of primary users, then the probability that it will find itself in a location where all bands are blocked by primary users becomes increasingly improbable. When considered as an alternative to the old methods of dedicated band assignments, dynamic spectrum promises significantly reduced interference because device can be given more operating options in which to find those that allow coexistence with other devices operating in their area.

---

[5] M. McHenry, Reports on Spectrum Occupancy Measurements, Shared Spectrum Company, www.sharedspectrum.com/?section=nsf_summary, 2007

## V. Predicting the Transmission of Others is the Key to Sharing Spectrum

The key to establishing service rules that enable spectrum sharing is enabling one device to predict the transmissions of another. When one device can predict the transmissions of another, then it can plan its own transmissions to be non-interfering or interfered. There are a number of techniques that enable this. Listen-before-Talk is a category of related techniques, which at its heart assumes that past behavior predicts future behavior. If another device has transmitted in the past on this channel, then it will do so in the future, and that channel is to be avoided. This clearly is not always true, but it has a high probability of being true.

Other service rules enable predictability of other transmitters. A fixed frame time allows one device to know how long it must monitor a channel to sense another device's operation. Fixed pairing of transmit and receive is a significant help because if a monitoring device can sense the operation of either side of the transmission, it knows the other side is operating, even if it cannot sense that sides transmission. Hence, a monitoring device must only be close enough to one device in a communication link to know and avoid interfering with both sides of the link.

Intelligent communication is a set of methods that are not yet used in dynamic spectrum applications but have enormous potential for improving predictability. If all devices in a band have a way of communicating their transmission plan to other devices then the ability of those devices to coordinate their own transmissions is greatly improved.

## VI. Interference Management Measures Should be Matched with Operating Flexibility and Application

It has already been suggested that the degree of interference protection should be appropriate match with the application for a device and from that the consequences of interference. For devices where the consequences of interference are significant, the effectiveness of the interference protection should be correspondingly high. A continuum, matching consequences of interference to consequences of interference is envisioned as the appropriate path into a future where spectrum is used with increasing efficiency.

A related concept is that a device should be allowed greater operating flexibility as its ability to avoid causing or receiving interference increases. An example is found in the spectrum etiquette for the UPCS band. In this band, devices may optionally implement a least-interfered-channel rule. Those devices that do implement the least-interfered-channel are allowed to operate with up to 20 dB more energy in the band. This rule requires that devices sample a minimum number of channels, spread of the band, and use the channel with the least interference. Under crowded band conditions this allows more devices to operate, so long as they have taken the required measures to minimize their impact on other users of the band.

Both these concepts envision service rules that allow devices to implement a range of interference avoidance and management techniques. The service rules of the band should be crafted so as to allow devices to effectively implement a variety of techniques. Devices may then implement the level of interference management that is required for the reliability it requires and the operating flexibility it desires. To pursue this vision new service rules would identify the range between the least and highest levels of interference protection required in a band. The service rules would then be crafted to require devices to implement the least interference protection but also provide support required to enable other devices to achieve the highest levels of interference protection. With increasingly sophisticated interference avoidance capability devices would be granted increased operational flexibility, which in many cases would be necessary to achieve the required levels of interference protection. Crafting these service rules would be the job of the FCC. Identifying the range of interference protection would be a joint responsibility. Insuring that devices implemented the level of interference protection appropriate to it would be the role of the FDA.

## VII. There are a Wide Variety of Interference Management Techniques

There are a wide range of interference avoidance techniques that have been developed. In Annex A many of these techniques are identified and categorized. Used in appropriate combinations, these techniques have the ability to provide surpassing levels of interference protection and enable unused spectrum to be released for use.

## VIII. The UPCS Band as an example

The Unlicensed Personal Communications Services (UPCS) band may be considered as an example. This band, currently 1920-1930 MHz, illustrates a number of points made in these comments. First, it is a band with a spectrum etiquette. Second, parts of that etiquette allow additional operating flexibility for devices that implement additional interference management measures, e.g. the least-interfered-channel rule. Third, the band was relatively unused for many years, but when the service rules were adjusted to meet market needs, its use increased dramatically. Forth, the UPCS band demonstrates the need for bands with good interference protection. When the service rules were changed in 2004 cordless phones largely operated in the 2.4 and 5.8 GHz ISM bands. These bands offer almost no interference protection and with increasing utilization of those bands, interference, due to band crowding, is an increasing problem. In just 6 years, between 2004 and 2010, over 50% of the cordless phones sold in the US have moved to the UPCS band.[6] Since the rule changes, the dramatic move from those bands into the UPCS band by cordless phones demonstrates that a real need was meet by a band with good interference protection. Finally, the band is currently dominated by devices that use the DECT industry standard. The DECT standard provides a number of additional benefits for those devices, some of which are:

- DECT provides additional interference mitigation, beyond the FCC rules. For example:
    - all DECT devices use the same frequency and channel timeslots. Features like this further improve transmission coordination between devices.
    - DECT devices use fixed pairing of the transmit and receive timeslots, which allows a device sensing one side of the transmission to know of the existence of its paired half.
- There are low cost chip sets due to the combined volumes offered by DECT devices.
- There is substantial development and marketing support provided for DECT devices.

[6] See comments in FCC Docket 10-97 by the DECT Forum and others.

- DECT devices are interoperable, facilitating consumer choice and allowing companies to focus their efforts on their core competence.

What is clear is that

The UPCS band was originally established to as a 20 MHz buffer between the PCS transmit and receive bands. Later its 20 MHz, 1910-1920, was reduced because the band had not been heavily utilized and there were significant needs for additional PCS and AWS spectrum. It was originally an unlicensed, lower power, buffer that was needed to avoid interference between the PCS licensed transmit and receive bands.

In 2004 two changes in the UPCS band service rules stimulated dramatic increase in the use of the band. The rules for the UPCS band were modified so that the DECT protocol could operate in the band and the non-nomadic requirement was removed. For the first consumer devices could use the band, based on an industry standard.

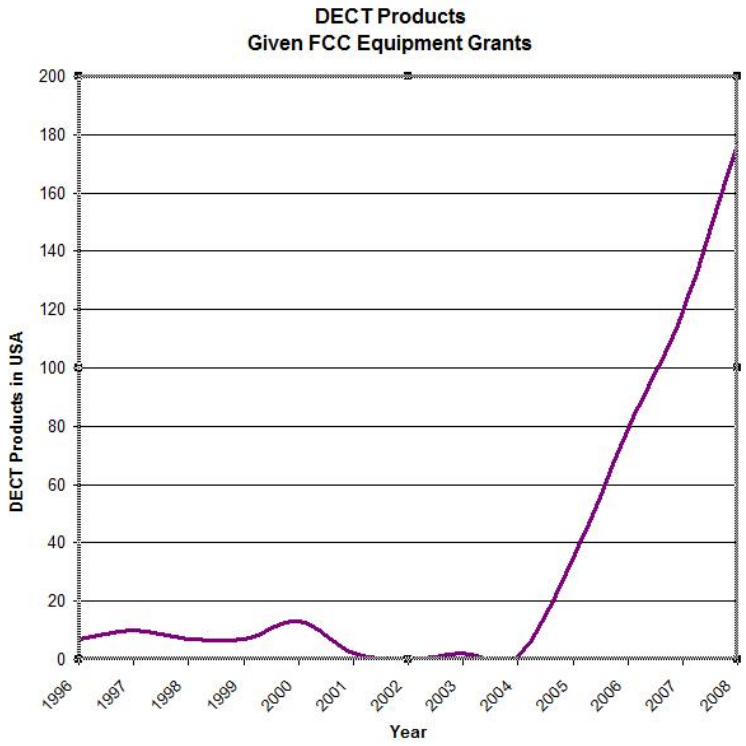


**Figure 2 – FCC Equipment Grants for UPCS Band**

Figure 2 illustrates the trend, showing the in equipment grants from 2004 to the present. In 2003 there were only 2 equipment grants for the UPCS band.[7] In 2004 only 1 grant was issued.[8] All of these grants were for cordless phones.

In 2008 there were 177 equipment grants.[9] The vast majority for voice communication products, mostly cordless phones using the DECT 6.0 standard. However, an increasing number of new applications are being introduced to the band.

Based on the FCC grants, information from UTAM filings and other sources it is estimated that the UPCS band saw approximately 500,000 individual units shipped each year, from 2003 to 2005.

---

[7] FCC ID O4M9P23 and AY5SN531PSTH-A

[8] FCC ID AY5PS3D

[9] FCC equipment grants database.

However, with the rule changes in 2004-2005 the shipping volume rose dramatically with an estimated 1,850,000 units in 2006 and 3,500,000 in 2007. The DECT Forum projects that worldwide shipments of DECT CAT-iq products will reach 30 million units in 2009. DECT CAT-iq is the latest advance in the DECT standard. The percentage of that number projected to be shipments in the USA is currently unavailable but is expected to represent a significant portion of worldwide shipments.[10]

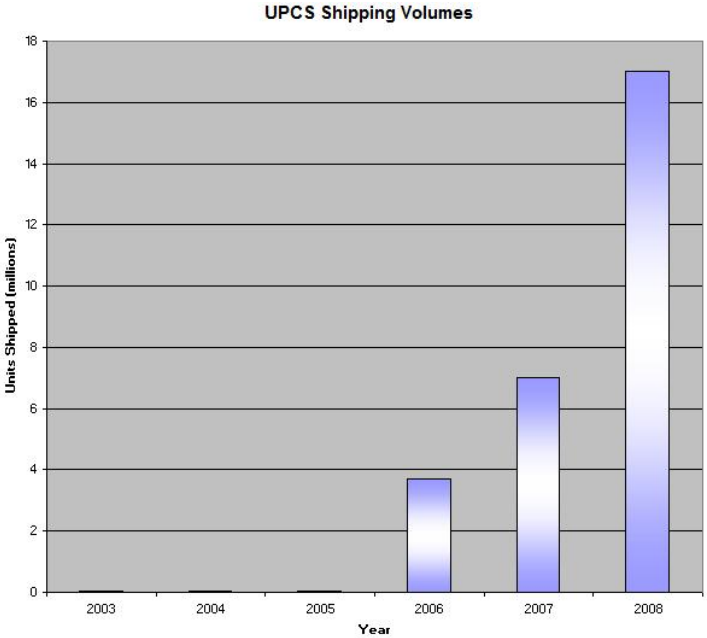


**Figure 3 – Estimate of UPCS Units Shipped**

It is proposed that health care applications share some common characteristics with cordless phones. Among these is the need for operating spectrum with good interference protection. Cordless phones and many health care applications require real-time, guaranteed throughput of data. In addition, the ability to extend the service rules to provide the additional benefits of an industry standard are similar. The UPCS rules were crafted in a way that facilitated an industry standard extending and adding additional value in response to market needs. The UPCS band service rules require features that allow

[10] The information in this section was largely derived from the Dec. 12, 2009 Ex-Parte filing of the DECT Forum in WT Docket No. 04-356, which contains additional detail about the UPCS band, its history and growing adoption by cordless phones and devices with similar spectrum needs.

devices to achieve levels of reliability required by cordless phones. Similarly bands used by health care will require features that allow health care devices to achieve the levels of reliability they require. Based on their application not all health care devices will require as much interference protection as others. However, the service rules should allow that differentiation but insure that devices can achieve the highest level of reliability needed for the applications that use the band.

## IX. Conformity Assurance

The need to establish full and robust conformity assurance systems is not to be minimized or its challenges underestimated. Good ideas can fail for poor implementation. Inadequate implementations of dynamic spectrum access could undermine the great benefit promised. To avoid this both the FCC and FDA should carefully consider what kinds of conformity assurance systems are required.

To begin, good type approval processes require labs that are competent at separating compliant implementations from those that are deficient. This assumes the labs have test methods that have been scientifically validated as being accurate, repeatable and highly correlated to field performance. Good test methods do not happen by accident and in this area many new test methods will be needed.

Lab proficiency is another area that will require attention. The current methods of lab assessment and accreditation are inadequate for the demands of this emerging field. Careful work with the assessment bodies will be required. However, beyond the work of assessment bodies laboratories need proficiency testing services by which to monitor the effectiveness of their own testing in these new areas of wireless. Type certification can only be as good as the testing upon which it makes its decisions.

Both the FCC and FDA will require good sources of information to confirm the efficacy of past decisions and guide future decisions. Both agencies would do well to consider where their data will come from and how they will utilize it. It may be that data logging of early devices should be required in order to develop a database of experience and provide a foundation of objective evidence to support future decisions.

Remedial measures should also be planned. If a problem develops what remedies will be available to rectify the situation? Establishing the ability to apply remedies, before they are needed, will only increase the effectiveness of these new services as any problems that do arise will be quickly addressed by pre-planned responses.

## X. Summary

In these comments I have suggested that there is an interactive relationship between the FCC and FDA when it comes to the use of wireless technologies for health care applications. Both agencies should determine the range of interference required in a band supporting health care applications. The FCC should then take the lead to establish service rules that enable the appropriate level of interference protection for each individual device. The FDA's role is to insure that individual device properly implement the level of interference protection required by its application.

Particularly for health care high levels of interference protection will be required. It has been argued that the old "command and control", "paper and pencil" methods of spectrum management past the end of their useful life some time ago. More importantly, as far as interference protection those methods offer only the appearance of a solution. In reality they resulted in tight frequency assignments, resulting in band crowding and in-band interference problems.

Dynamic spectrum methods for managing spectrum are the only choice if new frequencies are to be made available and improved interference protection provided. Dynamic spectrum has proven effective in the UPCS band and other bands where it has been used. However, dynamic spectrum is not trivial to implement. It requires careful planning and effective implementation by product developers. Further laboratories must be proficient in evaluating dynamic spectrum access devices. However, done well, dynamic spectrum access and the spectrum sharing it enables offers tremendous benefits, as it enables new exciting health care applications.

I think both the FCC and FDA for hosting this workshop and inviting these comments. I wish both agencies every success as they pursue the effective realization of the promise offered by this field.

Respectfully submitted,

**H. Stephen Berger**

/s/ H. Stephen Berger

Date: July 19, 2010

## XI. Annex A – Categories of Interference Management Techniques

*{This annex contains an currently unpublished article titled "A Categorization of Dynamic Spectrum Access Behaviors for Certification and Validation of Cognitive Radios" by John V Thommana, Rockwell Collins, John Chapin, MIT, Stephen Berger, TEM Consulting, LP., Douglas C. Sicker, University of Colorado. It is included here to illustrate the wide variety of techniques that can be employed when developing service rules supporting dynamic spectrum access in a band that requires a significant level of interference protection. The authors have not been asked if they support the statements and conclusions in the body of these statements. Their support for any specific conclusion should not be assumed, unless they choose to state it.}*

# A Categorization of Dynamic Spectrum Access Behaviors for Certification and Validation of Cognitive Radios

**John V Thommana, Rockwell Collins**
**John Chapin, MIT**
**Steve Berger, TEM Consulting, LP**.
**Douglas C. Sicker, University of Colorado**

The objective of this article is to classify the proposed approaches for dynamic spectrum access technology into a set of behavior groups. This provides a framework for understanding DSA technology – initially a survey of DSA methods. It also provides a starting point for evaluating the different approaches that might be used in DSA technology. Lastly, it provides a framework for conformance testing, such as required by regulatory bodies for testing spectrum compliance for radio device operation. For example, a device should be validated to ensure that it has implemented the etiquette correctly and hence can be certified to operate correctly in the field. Often a cognitive device will use multiple spectrum etiquettes simultaneously, for example, a cognitive device can use the "Listen before talk" etiquette in conjunction with a "Location based Usage" constraint. In this case, the device has to be validated for correct operation under both criteria to obtain certification for usage in the field.

When a manufacturer develops a DSA device with a novel etiquette, two steps are required for regulatory conformance or customer acceptance. First, the manufacture must validate that the etiquette employed is adequate to protect the primary user. This may involve analysis, simulation, use of a test bed, field trials or most likely some combination of these methods.

Second, the manufacturer must validate that the device implements the specified etiquette correctly. This involves thorough testing and analysis.

DSA etiquettes can also be used as a device or system performance optimization criteria. For example, a cordless phone operating in the US 900 MHz unlicensed band is permitted to choose any of the ten channels allocated for this purpose. Some manufacturers of cordless phones implement the “Least Interfered Channel” etiquette to provide the best possible voice quality. In cases like this, the correctness of the DSA etiquette implementation does not affect the conformance of the device with the spectrum usage regulations. Therefore, regulatory conformance testing need not validate that the device implements the DSA etiquette correctly.

## XI. A. Methodology

Dynamic spectrum access enables multiple overlapping users or networks to operate in the same frequency band(s) without causing harmful interference. DSA may be employed by all users or networks in the band to achieve effective spectrum sharing without harmful interference to any of the users. Alternatively, one or more users may be designated as primary users with protected access to the frequency band(s). Primary users normally do not employ DSA techniques. It is the responsibility of the other users, called secondary users, to avoid causing harmful interference to the primary users.

A transmission opportunity can be defined as a window of time in a particular channel associated with a transmission envelope, such as modulation or maximum transmit power, in which a DSA device can transmit without causing harmful interference and violating any regulations or usage contracts. [1] Many factors contribute to determining valid transmission opportunities.

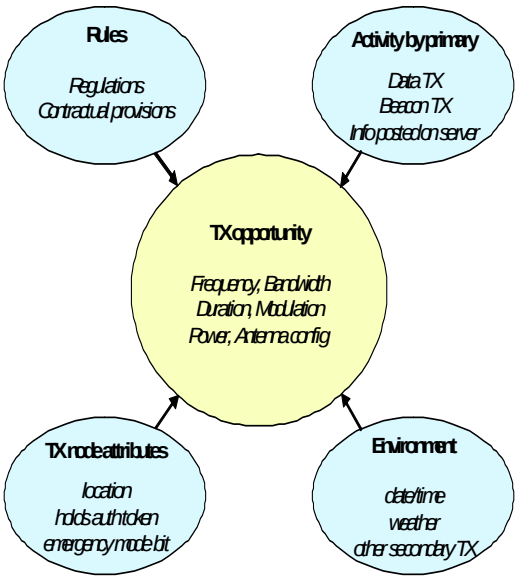


**Figure 4 - Transmission Opportunity Contributing Factors**

Figure 4 highlights that transmission opportunities, which can include aspects such as frequency, power, bandwidth or duration, can be influenced by rules, primary user activity, environmental conditions and the attributes of the radio devices.

The definition of spectrum etiquette can be expanded to "an algorithm or set of behavioral rules that permits a device or network to identify and exploit transmission opportunities". [1] The remainder of this article deals with grouping etiquettes into categories with criteria that contribute to determining valid transmission opportunities. These categories correspond well to an intuitive understanding of different classes of DSA behavior. Given these categories, it is then possible to ask, "What criteria need to be correct for a device in this category to avoid causing harmful interference?

## XI. B. DSA Device Categories Not Specific To an Etiquette

We begin by considering categories of factors not specific to a particular DSA technique. As depicted in Table 1, these categories include: Universal characteristics, Health characteristics, Spectral sensor characteristics and Antenna characteristics.

**Table 1: DSA Device Categories Not Specific To An Etiquette**

| Etiquette | Parameters |
|---|---|
| Universal Characteristics | Emission mask within operating channel(s) |
| | Emission mask outside operating channel(s) |
| | Emissions during power on initializations |
| | Emissions during band or mode change |
| Health Characteristics | |
| Spectral Sensor Characteristics | Sensor sensitivity and selectivity |
| | Sensor calibration and recalibration |
| | Sensor dynamic range |
| | Sensing duty cycle |
| | Sensing performance |
| | Sensor location |
| Antenna Characteristics | Directionality |
| | Frequency band and gain |
| | Multi-antenna systems |

### 1. Universal Characteristics

Formatted: Bullets and Numbering

Universal characteristics are features that are applicable to all radios. Some of these features create conformance-testing challenges when used by DSA devices. The classification of a device as a DSA device does not exempt the device from satisfying traditional conformance tests. Some of the key characteristics of interest are:

Emission mask within operating channel(s). This criterion becomes very important when operating in wideband modes. For example, Orthogonal Frequency Division Multiplexing (OFDM) devices exploit several discontinuous sub-carriers to avoid interference to narrow band users operating within the band. Variable bandwidths, heteromorphic emissions and depth of spectrum adaptation notches are key parameters to be taken into account.

Emission mask outside operating channel(s)**.** The use of notches for spectral adaptation generally stimulates RF non-linearities that result in out of channel or out of band emissions. Linearity performance of power amplifiers must be taken into account to ensure conformance.

Radio devices create emissions during the power on initialization cycle. DSA devices may have RF hardware and antennas that have been designed for transmitting over a wide range of frequencies. The bands of operation may include safety critical frequencies like public safety, radio navigation or air traffic control bands. Accidental noise generation during power-on poses a higher risk of interfering with these critical services than legacy narrow band radios capable of operating in non-safety critical bands.

Emissions during band or mode change. DSA devices are generally frequency and band agile devices that opportunistically use spectrum during normal operation. This attribute combined with potentially wide transmit bands makes it crucial to validate the performance of DSA devices during mode and band changes to prevent spurious noise generation. Validating emission limits during mode and band changes will be a key criterion to avoid or limit harmful interference to primary users.

### 2. Health Characteristics

Formatted: Bullets and Numbering

Just like legacy devices, DSA devices must also be validated to ensure conformance to regulations that limit emissions in frequency bands used by common health monitoring devices. A key criterion of interest is generation of biological signals.

DSA devices have to conform to regulatory policies that inhibit devices from mimicking event signatures like heart attacks when transmitting in bands used by medical implants. This is a concern because common medical implants have low RF signal levels and life-threatening reactions can be triggered by an external signal that stimulates the telemetry receiver. The multi-band operational nature of DSA radios, coupled with specific waveform requirements, make this criterion a very difficult one to validate. The onus of conformance may be placed on the DSA radio manufacturer to guarantee correct operation of specific waveforms in all supported bands.

### 3. Spectral Sensor Characteristics

Formatted: Bullets and Numbering

DSA devices rely on some form of spectral sensor to find and exploit transmission opportunities. The compliance of these DSA devices depends on the correct operation of the spectral sensor. Sensor Dependent DSA (SD-DSA) devices can come in different forms. An embodiment of the simplest SD-DSA is a DSA device using its primary receiver as a spectral sensor. Other forms of SD-DSA include the use of sensing device(s) housed within or outside of the DSA device. There are several key criteria of interest that we will now discuss.

Sensor sensitivity and selectivity determines the primary user detection capability of the DSA device. In order to validate the sensitivity of the spectral sensor the sensor should be calibrated

for sensitivity using continuous wave, pulsed or signals of specific criteria (like beacons used) specified by the etiquette.

For sensor calibration and recalibration the manufacturers of DSA equipment may have to support factory calibration and on-demand dynamic calibration. The on-demand dynamic calibration capability permits the use of specialized signals mimicking realistic signal conditions and built-in tests to validate conformance.

Another aspect is a spectral sensor's dynamic range, which defines the ability of the sensor to detect weak signals in the presence of other strong signals. The ability of a DSA device to operate in a band may be dependent on being able to meet a minimum dynamic range requirement.

Sensing duty cycle is another consideration. Some key performance criteria, like channel monitoring time, look through duration, abandon time and abdication time are all dependent on the spectrum sensing duty cycle. A single channel half-duplex SD-DSA device, that uses its primary receiver as a sensor, can only monitor the spectrum when it is idle, i.e., not transmitting or receiving. Similarly, a single channel full-duplex SD-DSA device can only monitor the spectrum when it is not receiving or when there is no transmission in a band that is within the receiver desense range. Both of these SD-DSA devices incur a performance penalty in terms of missed transmission opportunities even if the primary user detection criteria are met.

Sensing performance is yet another factor. The spectral sensor utilized by DSA radios will vary based on application. There will be a wide range of sensors, from those utilizing coarse sensing that uses simplistic RSSI measurements, to fine sensors relying on techniques like FFT, cyclostationary detection, wavelets, etc. Policies defining spectrum etiquette can define sensitivity metrics and granularity levels or dictate the use of specific sensing techniques to ensure reliable detection of the primary user.

Multi-channel SD-DSA devices that use one of their idle receivers as a spectrum sensor have to address co-site issues and will need to be validated to perform correctly under all conditions. If SD-DSA devices employ the services of other devices (like test and measurement equipment or other idle radios offering their receivers as spectrum sensing services), then device manufacturers must guarantee that its sensor selection algorithm is reliable.

SD-DSA devices that rely on non-collocated sensors or sensors that do not share the same antenna have to ensure that they have a common RF picture. Discrepancies in RF vision between the spectrum sensor and DSA device will lead to misdetection of primary users, interference with primary users and missed transmission opportunities. DSA device manufacturers and spectrum sensor manufacturers have to guarantee that the algorithm used to select a non-collocated sensor is reliable. Regulatory agencies can also impose additional policies like use of multiple distributed sensors requiring specialized algorithms for ensuring that the DSA device and its sensors have a common RF picture.

## 4. Antenna Characteristics

Formatted: Bullets and Numbering

The antennas used by the primary and secondary users impact the sensing characteristics of the spectrum sensor and hence the network performance.

Traditionally, regulatory bodies have not enforced the type of antennas used; they only enforce the transmitted power and the emission mask. Similarly the system/network designers and

test/compliance agencies may dictate VSWR, polarization and expected range, which is generally expressed in terms of receiver sensitivity. The type of antenna used is up to the device manufacturer and is generally a tradeoff between device cost and system performance. Some key criteria of interest are discussed below.

Directionality of antennas is an important criterion. The use of directional antennas by primary or secondary users will impact the sensing capability of the spectrum sensor. Key parameters like channel monitoring time, look through duration, abandon time and abdication time will be impacted by selection of directional antennas. Mobility is another factor that impacts directionality as it adds cost and complexity due to tracking requirements.

Frequency band and gain of antennas is a second criteria of interest. Generally, passive antennas are banded, i.e., optimized for a band of operation. Thus, wide-band, frequency agile DSA devices will have to select appropriate antennas for the band of operation. Devices that have switchable antennas will have to take added precautions to ensure that the appropriate antenna has been attached prior to operation. Antenna identification codes or other forms of antenna performance characterization may have to be put in place to ensure that DSA devices do not cause harmful interference.

Multi-antenna systems is another criteria to consider. The success of MIMO technology has led to the proliferation of multi-antenna systems that increase performance in terms of reliability and increased throughput. MIMO systems can offer better performance in multipath rich environments. DSA devices that switch antenna modes from SISO to MISO to MIMO have to ensure that harmful interference can be minimized during switching and normal operation.

## XI. C. DSA Device Etiquette Categories Already Used In Regulations Or Literature

We now consider the set of DSA techniques that are already in use by devices and referred to in regulations or literature. Commonly used DSA etiquettes like Listen-Before-Talk, Least-Interfered-Channel, Fixed-Frame Time Division, Transmit Power Control, Dynamic Frequency Selection and Access Control etiquettes are depicted in Table 2.

**Table 2: DSA Device Etiquette Categories Already Used In Regulations or Literature**

| Etiquette | Parameters |
|---|---|
| Listen Before Talk | Channel monitoring time |
| | Channel threshold |
| | Maximum transmit time |
| | Band abandon time |
| | Duplex system look before talk |
| Least Interfered Channel | Channel monitoring time |
| | Channel monitoring bandwidth |
| | Channel monitoring or power measurement threshold |
| | Channel confirmation time |
| | Monitoring reaction time |
| | Monitoring antennae characteristics |
| | Monitoring threshold relaxation |

| Etiquette | Parameters |
|---|---|
| | Alternate monitoring interval |
| Fixed Frame Time Division | Frame duration |
| | Slot duration |
| | Pre/mod/post-amble characteristics<br>Frequency stability |
| Transmit Power Control | |
| Dynamic frequency Selection | DFS monitoring time |
| | DFS detection threshold |
| | Look-through duration |
| | Channel abandon time |
| Access Control<br>- Positive and negative control beacons<br>- Positive control using networks<br>- Positive control using clear to send signals | Authorized frequency bands |
| | Denied frequency bands |
| | Security |
| | Designated authorization agents |

Formatted: Bullets and Numbering

### 1. Listen Before Talk

Listen Before Talk (LBT) is an etiquette that avoids transmission in the selected channel when it is in use by another device, through sensing immediately prior to transmission. Several key LBT criteria are considered below.

Channel monitoring time is an LBT criteria in which the amount of time that a DSA device has to monitor the channel to determine that the channel is vacant is dependent on the statistical properties of the primary user. DSA networks where the primary user is continuously broadcasting will have a different channel monitoring time as compared to a bursty primary user.

Channel monitoring threshold is a second LBT criteria, which determines the minimum amount of energy in a channel needed to classify the channel as busy. This parameter is also primary user dependent.

Maximum transmit time is a third LBT parameter, which determines the amount of time a DSA device can transmit once it has determined that the selected channel is empty. This parameter defines the time interval between look-through events (scheduled quiet periods for channel sensing). This parameter is also primary user dependent.

Band abandon time is a fourth LBT parameter, which determines the amount of time a DSA device cannot use the channel once it detects the presence of the primary user. This parameter can be channel/band specific or can be defined on a network wide basis.

Duplex system LBT is another consideration, where if transmit and receive frequencies are different, the transmitter must sense both frequencies and use the channel only if both are free.

### 2. Least Interfered Channel

Formatted: Bullets and Numbering

Least Interfered Channel (LIC) is an etiquette that selects a channel from a candidate set based on the total power measured in each channel of the set. There are implementations of LIC that randomly select a channel from a candidate set rather than selecting the one with least interference. These implementations switch channels until a channel is selected that meets the interference and operational requirements. Devices employing LIC etiquette generally determine if a channel can be selected for operation using some or all of the criteria listed below.

Channel monitoring time defines the amount of time a DSA device has to ensure that the energy in the channel is below a specified threshold before it can be used. Channel monitoring bandwidth is a criteria that defines the spectrum a DSA device plans to exploit. Typically this value is greater than or equal to the channel occupancy needed by the DSA device. Some implementations may consider adjacent primary user signal occupancy characteristics in determining the minimum monitoring bandwidth.

Channel monitoring threshold or power measurement threshold is another criteria that defines the minimum power level above the noise floor for declaring the channel usable by secondary users. Channel confirmation time defines the maximum wait time for confirmation from other radios in the network before repeating access criteria. This is used to ensure fair channel access in a multi-user environment.

Monitoring reaction time is a parameter that dictates the maximum time a monitoring system can take to detect a signal that is above the applicable threshold level. In this specific context, a specific time and spectrum window can be occupied for up to a specified duration without repeating the access criteria.

Monitoring antenna characteristics is a list of parameters used to ensure that the DSA antenna characteristics are similar to that of the monitoring spectrum sensor. Vendors of devices using antennas with different characteristics must ensure that they account for behavioral differences.

Monitoring threshold relaxation is a parameter that permits low power secondary users to relax their detection threshold based on the differential power levels between the primary and secondary users.

Alternate monitoring interval is a parameter used by paired channel frequency division duplex users. If the user is prevented from monitoring the intended transmit window (frequency and time) by the emissions of a collocated transmitter of the same system, it can monitor the paired receive frequency to determine the availability of the transmission opportunity.

### 3. Fixed Frame Time Division

Formatted: Bullets and Numbering

Fixed frame time division is an etiquette that utilizes unused time-slots in a time division multiple access (TDMA) communication system. This is generally very difficult to implement with a spectral sensor without actually decoding the primary transmission. There may be TDMA systems whose operational requirements are very relaxed or very lightly loaded of which secondary DSA devices can take advantage. Frame duration, slot duration, pre/mid/post-amble

characteristics and frequency stability and accuracy are key parameters that DSA devices have to consider.

Knowledge of slot duration and frame duration permits DSA systems to determine potential primary user burst arrival and also estimate channel usage to limit interference to primary users. Pre/mid/post-ambles used by the primary system has to be accurately detected by secondary users to maintain time synchronization. Frequency stability and accuracy permit DSA devices to adhere to the slot and frame timing to prevent interference to the primary users.

### 4. Transmit Power Control (TPC)

Formatted: Bullets and Numbering

Transmit power control is an etiquette that reduces the transmit power under specified operating conditions. Policies may allow for variable transmit power based on diverse readings (e.g., location, time of the day, link margin, QoS, etc.). Secondary users must have the capability to estimate the maximum transmit power that will not result in interference to primary users.

### 5. Dynamic Frequency Selection (DFS)

Formatted: Bullets and Numbering

Dynamic frequency selection is an etiquette that avoids a channel for a specified time after a primary user transmits in it. This differs from Listen-Before-Talk in that the protocol employs a frequency selection that abdicates channels based on explicit criteria. DFS monitoring time is a criterion that is dependent on the primary user waveform characteristics. This parameter plays the same role as channel monitoring time in an LBT system. DFS detection threshold is another parameter of interest that is equivalent to the channel monitoring threshold parameter in LBT systems. Look–through duration defines how often a DSA device must look for the reappearance of the primary user. Channel abandon time determines how long the channel must be avoided once a primary user transmission is detected. Channel abdication time is a parameter that allows DSA devices to determine how quickly a secondary user must stop its transmission and vacate the channel once a primary user transmission is detected.

### 6. Access Control

Formatted: Bullets and Numbering

Access control is a set of etiquettes employed by devices whose spectrum access is in part controlled by external factors. For example, maintaining a noise floor in an environment with multiple wireless devices by reducing the power of each transmitting unit when an additional unit is added. Another control mechanism would be to limit the number of simultaneously transmitting devices. There are several access control etiquettes.

A commonly used etiquette is positive/negative access control using beacons. Positive control etiquettes generally use presence of RF transmissions to disseminate permission information, while negative control etiquettes generally use absence of RF transmissions to disseminate permission information.

Positive access control using networks is an etiquette where the primary user disseminates permission information over a specific network or set of networks. Secondary users can access the specified network and obtain permission. Positive access control using request to send and clear to send signals is another etiquette where secondary users can send specific signals to obtain access to the primary user channel.

Each of these access control etiquettes have a specific set of parameters associated with it. Some of the commonly used parameters are authorized frequency bands, denied frequency bands, security and designated authorization agent. Authorized frequency band is an explicit policy designation of the frequency bands in which DSA operation is authorized. DSA operation outside these bands is prohibited. Denied frequency band is an explicit policy designation of the frequency bands in which DSA operation is prohibited. DSA operation outside of these bands may be authorized by the authorized frequency band policy. Security parameters define the cryptographic techniques used to ensure proper operation of access control etiquettes. Designated authorization agent defines a specific external server that will authorize the planned DSA operation.

## XI. D. Etiquettes Based On Characteristics Of The Device Or Its Environment

In this section, we consider etiquettes based on characteristics of the device and/or its environment. These etiquettes and associated examples are depicted in Table 3.

**Table 3: Etiquettes Based On Characteristics Of The Device Or Its Environment**

| Etiquette | Example |
|---|---|
| Location Dependent Access | - Absolute location dependent access<br>- Relative location dependent access<br>- Location dependent access with respect to RF signals<br>- Named location dependent access<br>- Location dependent access using databases |
| Time Dependent Access | - Absolute time dependent access<br>- Relative time dependent access<br>- Named time dependent access<br>- Time dependent access using databases |
| Mobility Dependent Access | - Absolute mobility dependent access<br>- Relative mobility dependent access<br>- Mobility dependent access using databases |

### 1. Location Dependent Access

Formatted: Bullets and Numbering

Location dependent access is an etiquette that places varying limits on transmission characteristics based on the transmitter's location. Location dependent access can be specified using absolute or relative means. Absolute location dependent access defines location using absolute terms like latitude, longitude and altitude above mean sea level. Relative location dependent access defines location relative to specific points or objects that have absolute location specifications. For example, US 3650 band rules prohibit transmission within a specified distance of grandfathered satellite ground stations. The operational policies can also include relative location with respect to objects (normally used indoors) or conditions.

Location dependent access based on RF signal strength is a variant location based access etiquette that is based on measured RF signal characteristics, like the signal strength of a positive control beacon above a specified threshold level.

Named location dependent access is another variant etiquette which prescribes DSA policies enabling or preventing DSA operation based on named regions like “Boston” or ”rural”.

In location dependent access using databases, DSA devices rely on databases hosted internally or externally to determine locations of primary users and/or areas where DSA operation is permitted.

### 2. Time Dependent Access

Formatted: Bullets and Numbering

Time dependent access is an etiquette that places varying limits on transmission characteristics based on time or date. As in the location based case time can be defined in absolute or relative terms.

In absolute time dependent access date and time can be based off of accurate timing sources with specific timing tolerances like atomic clock, GPS, internal real-time clock. In relative time dependent access date and time are specified based on delay after the occurrence of an event. An example of this is a policy that permits DSA operation based on non-occupancy of a DFS channel for a specified time after primary user transmission is detected.

Named time dependent access is another variant etiquette, which prohibits or permits DSA access based on named time intervals like “night” or “rush-hour”. In time dependent access using databases, DSA devices rely on databases hosted internally or externally to determines times when DSA operation is permitted; if users are mobile then a location dependent criteria may also be levied.

### 3. Mobility Dependent Access

Formatted: Bullets and Numbering

Mobility dependent access is an etiquette that places varying limits on transmission characteristics based on the transmitter’s movement. Absolute mobility dependent access etiquette bases DSA operation performance criteria that are tied to the speed of the transmitter. Doppler correction and specific equalization techniques may be needed to ensure DSA operation without interference to primary users. Relative mobility dependent access etiquettes are based on radio channel characteristics such as coherence time. Relative mobility dependent access permits DSA operation as long channel characteristics are within prescribed limits. In mobility dependent access using databases, DSA devices rely on databases hosted internally or externally to determine conditions under which DSA operation is permitted.

## XI. E. Etiquettes Based On Information Other Than Characteristics Of The Device Or Its Environment

This section captures the etiquettes that are based on information other than characteristics of the device or its environment. These etiquettes are depicted in Table 4.

**Table 4: Etiquettes Based On Information Other Than Characteristics Of The Device Or Its Environment**

| Etiquette |
|---|
| Multiple Access Dependent |
| Duty Cycle Dependent |
| Upper Layer Mode Dependent |
| Composite Access |

| Etiquette |
| --- |
| Collaborative Access |
| Child/Parent Network Access |

### 1. Multiple Access Dependent

Formatted: Bullets and Numbering

Multiple access technology dependent access is an etiquette that specifies the sensing requirements based on multiple access technology used by the primary communicator.

Depending on the Multiple Access Scheme (DS-CDMA, FH-CDMA, TDMA, FDMA, etc.) utilized, the sensing requirements will change. If the sensor is not properly configured, there is a high probability that the primary communicator may not be even detected. For example, narrow band sensors may not be able to detect direct sequence spread spectrum primary users and will raise the noise floor and interfere with primary user communications. Wideband fast hopping primary users may get interfered with but may not be reliably detected even by wideband users.

### 2. Duty Cycle Dependent Access

Formatted: Bullets and Numbering

Duty cycle dependent access is an etiquette that places limits on the transmit duty cycle of DSA radios. For example, the limits on transmission power placed on devices operating in the US 900 MHz unlicensed band is duty cycle dependent.

### 3. Upper Layer Mode Dependent Access

Formatted: Bullets and Numbering

Upper layer mode dependent access is an etiquette that prescribes the operation of a DSA radio based on the mode of operation.

Mode dependent operation permits wireless devices to operate with characteristics that are not normally permitted. For example, cellular phones can make emergency 911 calls even if they are not currently a subscriber of a cellular service. In this case it is the dialed digit string (911) that switches the mode from normal operation to emergency mode operation. Another example is the man-down button on tactical and public safety radios that guarantees the user a higher priority access.

In the case of DSA devices, the term upper layer is broad. Upper layer can mean any of the following: user action, options on a user interface, commands or notifications from the network or neighboring radios, even sensors embedded into the radio or external sensors like battery status, fire, tilt, impact, location, etc. DSA devices must ensure that the device enters and leaves the alternative mode correctly.

Some examples are command set only when indicated and positive and negative set command. Command set only when indicated is where the user interface must be robust to prevent accidental reset by “double clicking,” or other means to ensure correct and timely operation. Positive and negative set command is where the user sets the mode explicitly or fails to prevent the radio from entering or leaving the specified mode.

Priority or preemption mode is another mode dependent access. Its importance and widespread use has prompted us to treat it as an independent etiquette.

### 4. Composite Access

Formatted: Bullets and Numbering

Composite access is an etiquette that specifies the operation of a DSA radio as a combination of different etiquettes controlled by decision logic to create complex usage scenarios. Composite access etiquettes permit combining of etiquettes using specified decision rules to create specialized etiquettes.

### 5. Collaborative Access

Formatted: Bullets and Numbering

Collaborative access is an etiquette that relies on sharing information among multiple secondary user devices to share resources. For example, secondary radios using beacons to determine whether they can form a network in the band. Another example is sharing spectrum sensing information or information databases to improve primary user detection capability and reduce hidden node interference issues.

### 6. Child/Parent Network Access

Formatted: Bullets and Numbering

Child/Parent network access is an etiquette that relies on sharing information between child and parent networks to share resources efficiently. In this type of DSA access, both the child and parent network must abide with the policies specified for the band. Changes in operational parameters of the parent network must be relayed to child networks and vice versa. The actions taken by the parent or child network must be coordinated to abide with the policies specified for the band.

## XI. F. Etiquettes Based On The Context In Which The Device Operates

In this section we consider etiquettes where the context of operation determines the DSA behavior. These etiquettes are depicted in Table 5.

**Table 5: Etiquettes Based tn the Context In Which The Device Operates**

| Etiquette |
|---|
| Platform Dependent Access |
| Aggregated Channel Access |
| Rights and Licensing Based Access |
| Priority and Preemption Based Access |

### 1. Platform Dependent Access

Formatted: Bullets and Numbering

Platform dependent access is an etiquette that controls the operating characteristics of a DSA radio based on the platform of which the DSA radio is a part. An example of this etiquette is the behavior of the same radio when used as a handheld device or a vehicle mounted device. When the device is not connected to the vehicle mount and power, it operates at a lower power output to protect the user. This device switches to a higher output mode when inserted into the vehicle mount.

DSA devices can exhibit different performance capabilities and behavior dictated by policies when operated as a handheld, mounted on a vehicle or mounted on a fixed structure.

### 2. Aggregated Channel Access

Formatted: Bullets and Numbering

Aggregated channel access is an etiquette that permits linking of multiple channels as one aggregate channel whose usage by DSA radios is dictated by satisfying the operating requirements of a channel subset. An example of this is an etiquette that controls or limits effects in one portion of the spectrum based on sensing in another portion of the spectrum. This is generally used by rule based or look-up table based paired spectrum devices like cellular phones where a channel number defines a pair of frequencies. If sensing in the transmit band is impaired due to co-site issues or adjacent channel de-sense then sensing the receive channel can be substituted for determining channel occupancy.

### 3. Rights and Licensing Based Access

Formatted: Bullets and Numbering

Rights and licensing based access is an etiquette that mandates that DSA radios use a channel to acquire operating rights and validate them with the channel controlling authority prior to channel use. An embodiment of this type of access is a DSA radio that must validate its planned operation in a certain band using a crypto-signed key provided by the owner of said band.

### 4. Priority and Preemption Based Access

Formatted: Bullets and Numbering

Priority and Preemption based access is an etiquette that authorizes specific DSA radios to preempt or have priority over other radios operating in the band. These are etiquettes with spectrum access affected by priority that is associated with a mission need, whether through pre-determined priority levels (e.g., service level agreements) or through a “manager” determining access based on the current situation (e.g., incident response).

## XI. G. Conclusion

In this paper we have considered a broad set of etiquettes that might be used in determining the operation of a DSA device. It is clear that while this set is rather large, it is likely that a small subset of the etiquettes will drive the initial operation of these devices and that these etiquettes will be the focus of most test laboratories. In addition to providing a starting point for considering the testing that might be required for the assurance of DSA devices, we hope that this paper also has provided a useful overview of the anticipated operation of DSA systems.

## XI. H. Acknowledgment

We want to thank the members of the IEEE P1900.3 working group who contributed ideas and edits to the draft standard on which this paper has been based.

## XI. I. References

[1] IEEE P1900.1 - Standard Terms, Definitions and Concepts for Spectrum Management, Policy Defined Radio, Adaptive Radio and Software Defined Radio, 2008.