Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership

Document SDRF-08-P-0004-V0.8.0

18 June 2008

Table of Contents

List of Figures

List of Tables

Executive Summary

This report describes how software defined radio (SDR) technologies can help achieve the public/private partnership goals of the national broadband network planned for the 700 MHz frequency band. The reference to SDR technologies also covers cognitive radio (CR) and dynamic spectrum access (DSA) technologies. By national broadband network, we are specifically referring to the proposed network defined by the U.S. Federal Communications Commission (FCC) in their Second Report and Order (FCC 07-132, released 10 August 2007) as part of the rules for the auction of spectrum in the 700 MHz band, specifically for the 10 MHz of spectrum known as the D-Block. The D-Block is intended to be coupled with 10 MHz of spectrum already allocated to public safety for broadband use. While the initial auction of the D-Block spectrum closed without the reserve price being met, the FCC has indicated that they are committed to implementing the concept of a public/private partnership. We anticipate that the basic concepts will not change even if the specific rules for auction and use of the spectrum are modified as part of the plan to create the partnership.

This report identifies several challenges in implementing the proposed network, and details how SDR/CR technologies can help meet these challenges:

- **Challenge 1:** A national broadband network must be created that is commercially viable while simultaneously meeting public safety needs.
  SDR/CR Capabilities: SDR provides flexibility to meet diverse requirements. CR techniques can further leverage that flexibility to improve coverage and mitigate interference for critical communications on a system compatible while accommodating commercial coverage requirements).

- **Challenge 2:** The national broadband network infrastructure will need to adapt and change over time as operational experience is gained, as technology changes, and as commercial and public safety user-requirements evolve.
  SDR/CR Capabilities: SDR provides flexibility and cost-effective approaches to adapting the network to meet evolving requirements and technologies.

- **Challenge 3:** Design of the network to meet unique requirements of the public safety users may not be favorable solutions for commercial users.
  SDR/CR Capabilities: SDR provides capabilities to reconfigure devices and infrastructure to meet specific public safety needs as needed. CR capabilities leverage that capability to provide robustness and dynamic real-time resource management that can be tailored to specific public safety needs.

- **Challenge 4:** Based on the build-out schedule, there may be other 700 MHz networks that will need to interoperate with the national broadband network.
  SDR/CR Capabilities: SDR provides a cost-effective means to work with legacy systems and adapt to an evolving network architecture. CR capabilities provide additional capabilities for seamless operation across multiple networks and transition/integration of new capabilities.

- **Challenge 5:** Meeting the technical and operational challenges for building a national broadband network should not add significant cost or detract from the usability of the subscriber equipment.
  SDR/CR Capabilities: SDR can reduce costs by providing over-the-air reprogramming

and approaches to managing varying technology refresh cycles. CR provides user interfaces that hide the technical details of the radio system so that the user interface is based on user job functions rather than the details of the radio system.

In addition, SDR/CR capabilities referenced in the preceding bullets will require more sophisticated evaluation and certification techniques because of their ability to modify performance in ways that go beyond today's devices.

The SDR Forum is well positioned to consider the role of these new technologies in the 700 MHz band since its membership includes commercial mobile radio service providers, public - safety representatives, technology developers, systems integrators, and equipment manufacturers and test & measurement equipment vendors. The information and recommendations in this report focus on technology and related policy considerations to (a) prospective bidders and service providers, (b) potential grantees of the Public Safety Broadband License (PBSL), (c) equipment manufacturers, and (d) regulators[1].

[1]It is not the intent of this report to suggest any changes to FCC rules, regulations, or orders.

1 Introduction

The U.S. Federal Communications Commission (FCC) has set forth an innovative concept to create a public/private partnership to develop a national broadband wireless network. In particular, this concept is based on sharing the network among public safety users and commercial users in a manner by which commercial users can have secondary use of public safety spectrum during normal operations, and public safety users can pre-empt commercial users in the commercial spectrum during emergencies. This shared network concept, outlined in the Second 700 MHz Report and Order (FCC 07-132, released 10 August 2007), was defined as part of the rules associated with the auction of spectrum in 700 MHz. Specifically, 10 MHz of spectrum, known as the D Block, was to be auctioned with the stipulation that it be coupled with 10 MHz of spectrum allocated for public safety broadband use. The network created from the adjacent D-Block and public safety spectrum blocks is for both public safety and commercial use under terms to be negotiated by the D Block auction winner and the designated licensee for the public safety spectrum, the Public Safety Spectrum Trust (PSST). The result of the 700MHz auction did not derive a winner of the D-Block as the reserve price was not met. The FCC is currently developing a revised plan for a public/private partnership, but the specifics of such a plan leading to the creation of this network has not yet been announced. However, the SDR Forum recognizes that: the basic concept of a shared national broadband network is still viable; The public safety community continues to support the concept; and the FCC is committed to continuing to pursue an approach that will result in some means of realizing the original concept.

This additional supply of spectrum and the associated rules and regulations present new opportunities and accompanying challenges for spectrum access and deployment of advanced broadband wireless technologies. The SDR Forum believes that software defined radio, and cognitive radio are technologies that are key to addressing those challenges. Designing and implementing a network to leverage existing and evolving SDR and cognitive radio techniques will significantly enhance the ability of the network to realize the vision defined by the FCC.

In this report, the SDR Forum provides specific examples of how these technologies can be used to address critical implementation challenges of systems that meet the FCC’s defined service rules and regulations. An integrated approach incorporating SDR and CR in both the system infrastructure and subscriber units provides a highly flexible end-to-end network solution. This approach can meet diverse requirements and develop over time in concert with technology and operational evolution.

The challenges in implementing a 700 MHz national broadband wireless solution can be generally described as developing a network that can meet the inherently diverse needs of a Public/Private Partnership. The specific challenges described in this report were derived from requirements defined by the FCC.

2 Definitions and Key Concepts

There are a number of terms used extensively in this report. To ensure clear understanding of the concepts and approaches described in this report, definitions for key terms are listed in this section. The definitions are quoted from the SDR Forum's set of definitions for software defined radio and cognitive radio.[2]

Software Defined Radio (SDR): Radio in which some or all of the *physical layer* functions are *Software Defined*.

Physical Layer: The layer within the wireless protocol in which processing of RF, IF, or baseband signals including channel coding occurs. It is the lowest layer of the ISO 7-layer model as adapted for wireless transmission and reception.

Software Defined: Software defined refers to the use of software processing within the radio system or device to implement operating (but not control) functions.

Cognitive Radio: (CR) a.) Radio in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information and predefined objectives. The environmental information may or may not include location information related to communication systems.

b.) Cognitive Radio (as defined in a.) that utilizes *Software Defined Radio*, Adaptive Radio, and other technologies to automatically adjust its behavior or operations to achieve desired objectives.

Waveform: A waveform, also known as a communications standard, is the set of transformations and protocols applied to information that is transmitted over a radio channel.

Note that for the purposes of this document we are using the terms software defined radio and cognitive radio in a general sense. We recognize that there are more precise terms such as adaptive radio, policy-controlled radio, intelligent radio, and so on that describe particular characteristics of an advanced radio. In many cases those distinctions are based on the way in which the radio is implemented. Because this report is intended to address the overall technology rather than specific implementations, we use the term SDR/CR technologies as an inclusive term.

[2] *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011. Note also that these definitions are the same as the definition of these terms in IEEE P1900.1.

3 Challenges and SDR Technologies for a Public/Private Partnership

In reviewing the rules for licensing and use of the 700 MHz spectrum, and in reviewing the stated position of the Public Safety Spectrum Trust (PSST)[3], the SDR Forum identified several challenges that can effectively be addressed using SDR/CR technology. The 10 MHz public safety broadband spectrum in 700 MHz and the adjacent 10 MHz D-block spectrum are intended to be used in a national broadband network that meets both public safety and commercial user requirements. While there is significant commonality among such requirements, there are also key inherent differences. These differences make it challenging to create and sustain an economically viable network that meets both public safety and commercial user needs.

Wireless communications systems have long been designed within a network architecture that predates SDR/cognitive radio capabilities. The evolution of standards and requirements for both public safety and commercial networks has been based on static network architectures. For instance, public safety networks have traditionally been designed to meet channel capacity and reliability (backup power and redundant backbone circuits) best practices that set the network requirement at the "worst case" level –that is the capacity and reliability necessary during an emergency or catastrophe. It is not assumed that the network will *always need* these levels of capacity and reliability during "day to day" operations, but that the network must *always have these levels of capacity and reliability available when needed*. To do so, traditionally, the public safety community has set the standards bar for extra capacity and reliability in the network architecture very high, so that these assets are always available, and "stockpiled" when unused.). A public safety network design is based upon the design necessary for the worst possible case.

On the other hand, commercial networks, which must be profitable, are designed to balance profitability and customer service, rather than to operate without degradation during a catastrophic event. This is because the added levels of channel capacity and reliability at the edges of the worst case model are too expensive to implement everywhere in the network, for the few times that they may be needed. Instead, commercial networks must be "good enough" during a disaster, and designed to most optimally meet the day-to-day profitability/use scenario.

Both public safety and commercial best practices for capacity and reliability are, in reality policies about what is most important for the network to do, based on the static traditional network design. The adaptability and flexibility of SDR/cognitive architectures provide a new network design where networks and devices *can adapt to real-time conditions encountered in specific places in the network.* In a cognitive framework, the network is smart enough to allocate resources dynamically to a public safety emergency when needed, in real time. A cognitive framework includes ad hoc networking, dynamic spectrum access (frequency reallocation in real-time), the ability for radios to sense their environment and change their operating policies on the basis of real time conditions, and the ability for network management to send policy updates in real time to specific portions of the network and network users.

SDR and cognitive radio technologies changes how networks are designed, and what network best practices are. In an SDR/cognitive framework, standards do not have to apply to the whole network all the time. Since cognitive networks are not static – they can be designed to change in

[3] Public Safety Spectrum Trust, *Public/Private Partnership Bidder Information Document,* Version 2.0, 30 November 2007, Public Safety System Trust, available at www.psst.org.

real time and in response to specific conditions--standards are also dynamic, and can change in response to operating policies in place at a given time, for given circumstances, for specific users, and at a given location.

Thus in general terms, SDR technologies provide the ability to include greater degrees of flexibility into the the network. That flexibility can then be used to more economically reconfigure the network and subscriber equipment to meet multiple sets of requirements and to adapt to changing situations in real-time. Cognitive radio technologies provide tools to collect, manage, and act on the vast amount of information that is needed to make those decisions.

More specifically, key challenges posed by the concept of a public/private partnership, by the terms of the Block D regulations, and the SDR and CR capabilities that can address those challenges, are listed in Table 1. Each challenge area is analyzed in more detail in a subsection which follows.

Table 1, Key Challenges and SDR/CR Capabilities

	Challenge	SDR Capabilities	CR Capabilities
1	A national broadband network must be created that is commercially viable while simultaneously meeting public safety needs.	SDR provides flexibility to meet diverse requirements.	CR techniques can further leverage that flexibility to improve coverage and mitigate interference for critical communications on a system compatible while accommodating commercial coverage requirements).
2	The national broadband network infrastructure will need to adapt and change over time as operational experience is gained, as technology changes, and as commercial and public safety user-requirements evolve.	SDR provides flexibility and cost-effective approaches to adapting the network to meet evolving requirements and technologies.	Cognition capabilities can further leverage that flexibility by providing tools to automatically or semi-automatically configure devices and/or the network as needed.
3	Design of the network to meet unique requirements of the public safety users may not be optimal solutions for commercial users.	SDR provides capabilities to reconfigure devices and infrastructure to meet specific public safety needs as needed.	CR capabilities leverage that capability to provide robustness and dynamic real-time resource management that can be tailored to specific public safety needs.
4	Based on the build-out schedule, there may be other 700 MHz networks that will need to interoperate with the national broadband network.	SDR provides a cost-effective means to work with legacy systems and adapt to an evolving network architecture.	CR capabilities provide additional capabilities for seamless operation across multiple networks and transition/integration of new capabilities.
5	Meeting the technical and operational challenges for building a national broadband network should not add significant cost or detract from the usability of the subscriber equipment.	SDR can reduce costs by providing over-the-air reprogramming and approaches to managing varying technology refresh cycles.	CR provides user interfaces that hide the technical details of the radio system so that the user interface is based on user job functions rather than the details of the radio system.

3.1 Creating a Commercially Viable Network that Meets Public Safety Needs

Challenge 1: A national broadband network must be created that is commercially viable while simultaneously meeting public safety needs.

The proposed public/private partnership envisions building a national broadband network that meets the needs and requirements of the public safety community with sufficient financial return from commercial operation to support the buildout and self-sustainment of the network. The requirements, architectural approaches, and business models for building and maintaining public safety networks have historically been significantly different from those of commercial networks. Designers of the system will be faced with an unfamiliar and difficult set of design trade-offs.

Commercial networks are built with the goal of high utilization and low surge capacity with assumed acceptable amount of blocking. This model allows commercial providers to balance their capital expenditures (CAPEX) and Operational Expenditures (OPEX) against potential revenues. Requirements published by the Public Safety System Trust (PSST) for the broadband network define a higher tolerance to network downtime than have traditionally been engineered into commercial systems.[4] Commercial providers accept the risk of overloading and blocking during times of extreme network usage (e.g., limited surge capacity).

Public Safety designs their networks with a goal of moderate utilization to provide a significant surge capacity with minimal blocking of priority communications. This network design model increases the CAPEX. OPEX is affected to a lesser extent. Public safety agencies have a very low tolerance of any network downtime. The PSST envisions the proposed network to accommodate mission-critical data with high availability that must work all the time and most importantly in times of catastrophe.

One approach to meet this challenge would be to seek commercial users whose mission critical communications requirements are similar to those of public safety users and who would be willing to pay a premium for this level of reliable service. However, it appears unlikely that there is a sufficiently large market segment of this type to make the proposed nationwide 700 MHz broadband network economically viable. Even if there were, it would be desirable to serve a larger commercial user base by providing competitively-priced services. Higher revenues from an extended commercial user base will both improve returns for the network operator and provide funds for higher levels of service and faster buildout for public safety users. The national broadband network must effectively support multiple user communities with different requirements and business models.

The requirement to provide competitively-priced commercial services significantly affects the technical design of the network. While the SDR Forum has not conducted an economic analysis, it is the Forum's concern that it may be difficult to provide competitively-priced commercial services to a broad enough market base using only a service level and feature set defined as public safety requirements. Providing service that is economically appealing to other users, which is essential for the success of the public/private partnership, requires optimizing for progressively higher levels of efficiency and capacity as user requirements are progressively relaxed. This relationship is highlighted in Figure 1.

[4] The *Public Safety Broadband Statement of Requirements"* requires availability based on "Either highly reliable (99.999%) individual network elements or operating them in a fail-over redundant manner.

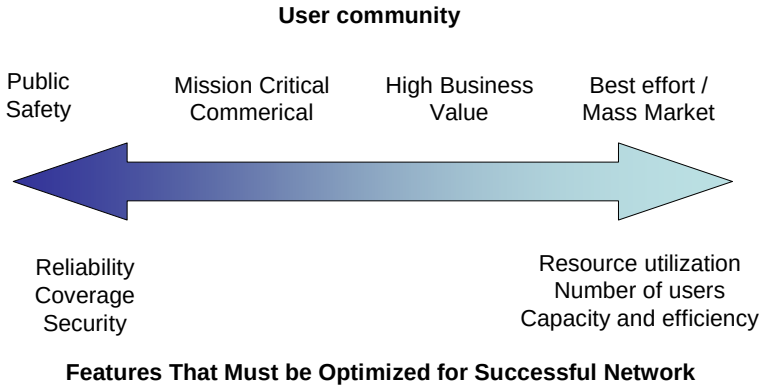

Figure 1. Divergent Requirements on a Public/Private Shared Network

The critical tensions represented/depicted in the figure include the following:

- The high reliability requirement for public safety is directly opposed to the economic requirement for high resource utilization in a commercial network. High reliability against service unavailability due to failures is achieved by provisioning redundant equipment, overlapping cells, excess link budget, and similar features. High reliability against service unavailability due to overload is achieved by provisioning greater capacity than is needed in normal operation. Both forms of over-provisioning increase investment in the network, reducing the commercial return on that capital expense.
- The universal coverage requirement for public safety is opposed to the commercial mandate to maximize usage levels, and hence revenues, given a particular amount of investment. Providing coverage in rural areas with low population density reduces the commercial return on investment. Similarly, ensuring coverage in tunnels, elevators, underground garages, and similar hard-to-reach places diverts investment and capacity from locations where larger numbers of users are located.
- The security requirements for public safety are opposed to the commercial mandate to maximize capacity and spectral efficiency. Measures for high security, particularly those that defend against denial of service attacks, add spectral occupancy and time occupancy overheads that reduce capacity and efficiency. These effects reduce the number of users that can be supported and thus the network's return on investment.

These divergent requirements create significant challenges for network design and implementation.

Software Defined Radio/Cognitive Radio Capabilities

Flexibility

The key to solving issues created by divergent requirements is flexibility. Divergent user communities may require diverse operating modes that cannot be provided by a single network. However, if the network can offer multiple operating modes, and can reallocate its resources as the mix of users and applications changes, it is possible to satisfy a wide range of user needs.

SDR techniques can provide a cost-effective way to support multiple operating modes and flexible resource allocation. CR techniques assure that the network allocates its resources

appropriately. These technologies can be the critical components that enable a network to meet both public safety and commercial requirements while achieving commercial success.

In particular, SDR technology enables four key types of flexibility:

1. Waveform flexibility. SDR technology enables the use of multiple different waveforms on a single hardware device. It may be appropriate for different user categories on the public/private shared network to use different waveforms or to select different options within a single waveform standard. For example, one waveform can prioritize reliability and coverage by encoding data bits in a way that is highly noise-tolerant, while a different waveform prioritizes capacity by using encoding that allocates less time and energy per bit. One waveform may have packet headers with sufficient redundancy and authentication information to defend against spoofing and denial-of-service attacks, while another may omit these features to achieve more compact headers that enable higher efficiency. Software defined radio provides the flexibility to offer different waveforms or options to different users without duplicating hardware.
2. Resource allocation flexibility. SDR technology enables a device to flexibly reallocate resources such as computational capacity among different tasks. Consider the case of an individual call. In a traditional radio the allocation is fixed: there is a certain amount of hardware circuitry devoted to each task. In an SDR the resources are fungible. For example, if a high priority user encounters difficult channel conditions, such as when a public safety officer enters a tunnel, the nearby infrastructure base station as well as the user's radio can activate a more loss-tolerant waveform and/or more sophisticated receive processing and increase transmit energy for that user to compensate for the link loss. The resources required to do this can be recovered by making small adjustments that reduce processing requirements and transmit power for a number of lower-priority users, any one of whom will notice only a small reduction in performance. Another view of this capability is that the base station only needs to allocate resources to provide coverage in the tunnel at times when there are public safety officers actually located there and using the system. Those resources are free at other times to improve commercial capacity at other locations. SDR used in this way can enable the network to significantly increase commercial capacity without reducing its support for public safety requirements, at the same level of investment. Cognitive radio capabilities then facilitate the management of resources for enhanced performance (the Autonomous Adaptive Base Station concept[5] is one example of an architecture designed for this purpose.)
3. Software modification. An SDR's capabilities can be flexibly modified and upgraded over time, without hardware modification. The network can be configured to offer different behaviors and different services in different geographic areas, by using different software versions in different devices. These benefits of SDR aid the public/private network to cost-effectively meet user requirements that vary by location or that evolve over time.
4. Over the air programming. The items listed above provide significantly flexibility in radio configuration that can be exploited for mutual commercial / public safety benefit, including use of the 700 MHz national broadband network. However, if reconfiguration

[5] Akabane, K., Shiba, H., Matsue, M., and Uehara, K., "An Autonomous Adaptive Base Station that Supports Multiple Wireless Network Systems," Proceedings of DySPAN, 2007, Dublin Ireland, April, 2007.

> and updates require a physical connection to a device, it becomes a challenging configuration management and logistics problem to update or load new software into radios. Over the air programming provides an approach which allows devices to be updated simultaneously and without requiring each device to be physically transported to a location where it can be reprogrammed. In addition to simplifying the configuration management and logistics problems, over the air reprogramming can facilitate incident specific reprogramming as needed.[6]

The flexibility of SDR technologies provides an opportunity to achieve nationwide interoperability goals and network economic viability without imposing specific a priori requirements such as a common air interface for all users. Thus public safety could still accrue the benefits of leveraging mass-produced components and hardware while benefiting from functionality customized for their specific needs. The next sections describe in more detail how SDR flexibility coupled with the automatic control features of CR can be used to address some specific challenges of a public/private shared network.

Coverage Flexibility

Of all requirements that a public safety system must meet, coverage is one of the most important requirements to the public safety user, and one of the most difficult challenges for the public safety communications system design. Coverage to a public safety user means being able to communicate with high quality throughout a large percentage (usually in excess of 95%) of a specified service area, which often includes tunnels as well as buildings with signal penetration losses 30 dB or higher. Geographic coverage for public safety users is required for areas where they need to monitor or respond to incidents. While this includes populated areas, it also includes unpopulated areas as well (consider the needs of a law enforcement officer making a traffic stop on a rural road, or a firefighter fighting a wildfire). Coverage for commercial networks is generally far less ubiquitous, and for economic reasons is generally concentrated in areas sufficiently populated to generate adequate usage revenue.

A solution that enhances coverage for public safety and yet can be tailored in real-time to meet specific network resource demands would be an enabling factor for accommodating these divergent requirements. Real-time reconfiguration enables use of more robust waveforms (beyond the capabilities of the "normal" waveforms used for day-to-day operations) for critical situations when coverage extension is needed. Coverage is limited by insufficient link budget or excessive interference. Both limitations can be substantially mitigated, and flexible and scalable coverage solutions achieved through the capabilities offered by SDR and CR in both the radio and the network. Table 1 summarizes the capabilities afforded by SDR and CR for coverage enhancement and flexible, scalable coverage solutions. Some techniques in the table and following discussion are better suited for "one to one" (i.e., individual) calls than for "one to many" (i.e., group) calls. However, it is presumed that initial broadband communications will

[6] Significant research is underway to develop the protocols and security procedures necessary for reprogramming devices over the air. For example, the End-to-End Reconfigurability (E²R) project aims at bringing together a wide range of systems, such as Cellular, Wireless Local Area and Broadcast, to devise, develop and trial architectural design of reconfigurable devices and supporting system functions.

more likely be data transmissions of a one to one nature (e.g., database lookup, uploading of video and imagery to an Emergency Operations Center.)[7]

Table 2, Examples of SDR/CR Mechanisms for Coverage Enhancement and Flexibility

Communications Benefit	Implementation mechanisms
Interference Mitigation	Flexible mode-dependent receiver filtering
	Dynamically adaptable modulation
	Dynamically adaptable frequency selection
	Smart network-wide frequency selection to: find unoccupied spectrum avoid use of adjacent channels by devices in close proximity[8]
	Intelligent transmit power control
	Adaptive beamforming
Link Budget Improvement	Flexible mode-dependent receiver filtering
	Reconfigurable radios to support coverage extension [9]
	Dynamically adaptable modulation
	CR-based mesh networks for coverage extension[10]
	Intelligent transmit power control

For an in-depth technical discussion of these implementation mechanisms and how they enhance coverage, see the Appendices. Here we summarize a few of the mechanisms for the general reader.

Adaptable Modulation and Frequencies

The modulation influences the link budget and thus the coverage. Higher data rate modulations in a given bandwidth have less coverage range than lower data rates. Similarly, the higher rate modulations tend to have less tolerance to interference than those with lower rates and often have a wider bandwidth transmit spectrum that tends to cause more interference to others. Hence, radios that can rapidly change waveforms, such as the radios already employed in many commercial data systems, can dynamically modify the balance of coverage versus data rate. Even though SDR is not necessarily required to enable these waveform changes, it does offer enhanced flexibility over a hardware radio, enabling a wider range of waveform parameters to be changed with more precision. For example, SDR can better balance coverage versus data rate, accommodating both commercial and public safety users. CR algorithms can adjust waveform bandwidths and frequency selections based on information relevant to the situation, such as geolocation and the relative positions of the users.

[7] Mission critical dispatch voice support has not been identified as a primary service on this network, but nevertheless, analogous one to many voice/data services can be readily supported in a "secondary" fashion via IP networking techniques, such as multicasting, and SIP based Voice services, perhaps reducing traffic level on primary voice systems.

[8] including avoidance of “near-far” interference situations

[9] SDR enables radio reconfiguration to mesh

[10] CR enables optimal setup/control of the mesh

Coverage Extension

Scalable coverage can also be extended through means external to the infrastructure. For example, a method employed today by public safety systems is to use vehicular repeaters to retransmit signals received from the infrastructure to a portable within a building to achieve in-building coverage that the infrastructure alone could not provide. SDR and CR are key enablers of flexibility for configuring operating frequencies of the repeaters, base stations, and portables to mitigate interference in these types of systems.

Another concept for coverage extension that has been receiving considerable attention is to use the radio flexibility afforded by SDR and intelligence afforded by CR at the network level to adaptively configure ad-hoc mesh networks using a group of radio subscribers to extend coverage beyond that of the infrastructure.[11] Examples include subscribers in tunnels and in outdoor areas where there is a coverage "hole" in the infrastructure. This network extension approach would allow transmissions to be passed back and forth from the incident site along a network of individual responder radios operating in peer-to-peer mode to a radio which can communicate with the main radio system/network. A radio could be positioned where it could maintain connectivity with the infrastructure (such as at an opening to a tunnel) and function as a repeater to bridge between the otherwise disconnected radios and the infrastructure. Depending on distribution of radios required to extend the network, additional radios could also be automatically reconfigured to act as repeaters among the disconnected radios.

Intelligent Radio Resource Control

Transmit power control systems employ open and/or closed loop transmit power control algorithms for efficient utilization of spectrum. In cognitive radio systems, non-cooperative and cooperative transmit power control strategies can be employed for efficient spectrum utilization and sharing. Non-cooperative power control involves radios participating in the network making individual transmit power decisions based on the local environment that they individually see. In case of cooperative power control, centralized decision is made by a centralized network controller based on data gathered from two or more radios in the network.

This capability is relevant to manage the secondary commercial use of the public safety spectrum during normal operations. The main challenge to spectrum sharing lies in striking a balance between the conflicting goals of minimizing the interference to the primary or mission critical users and maximizing the performance of the commercial and public safety users. One approach to addressing this issue is adapting the transmit power based on the information gathered by the Cognitive Radios using either cooperative or non-cooperative strategies. Cognitive radios can vary individual and aggregate transmit power based on user, spectrum, network, application and environment awareness. The operation of the cognitive radio network can be governed by its peak transmit power constraint and an average interference constraint, which can be varied based on location and environment. The cognitive power adaptation strategies can be characterized to maximize the network SNR, coverage and capacity. In general, power adaptation to optimize capacity requires decreasing the transmit power from the peak power to zero in a continuous fashion as the probability of the primary/mission critical user being present increases. In addition, it may require increasing the peak power for mission critical users to increase their

[11] SDR Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems, Volume 1: Review of the 7 July Bombing of the London Underground, SDR Forum Report No. SDRF-07-P-0019-V1.0.0, November 2007, available at www.sdrforum.org.

coverage and SNR. The cognitive-based power control approach can be extended to include location and density of different kinds of users.

Prioritization and Managing Quality of Service

Another of potential divergent requirements between the commercial use of the shared network and the public safety use of the network is in the management of resources to provide dynamic levels of Quality of Service (QoS) in voice systems. Current public safety systems have limited management of priorities. For example, in trunked voice systems some talk groups may be given a higher priority than other talk groups, and emergency alarms are given priority over other communications. However, beyond those capabilities there is little real-time control over network resources, and priority assignments cannot be changed dynamically. However, CR capabilities provide an opportunity to provide much greater dynamic control of network resources that can allow the communications resources to dynamically meet evolving needs of an incident.

Commercial protocols do not currently provide that level of dynamic resource management. WiMAX and LTE allow for service classes and are sensitive to multiple methods of determining quality of service at a layer 2 and layer 3 levels, including 802.1Q flags, VLAN tagging, MAC or IP address, protocol port. In WiMAX and LTE, the service class defines the priority of the traffic within the system. The ability of the WiMAX or LTE system to sort and accommodate prioritized traffic flows depends on the triggers and logic placed into the system by the manufacturer. WiMAX and LTE treat prioritized traffic using the gatekeeper theory; each user has an equal chance of applying to the system for access, the system then decides if the user is granted access. When the user requests access, the system determines the proper service class based on a pre-defined set of parameters. The user is then allocated a sub-channel or sub-channels based on pre-defined parameters.

Prioritization schemes become more complicated when public safety voice communication is also carried by the broadband network. The challenge for the national broadband network is two-fold. The: first challenge, is to define the hierarchy of service classes for normal operation; second, is to define emergency operating service classes. It is expected that public safety will continue to operate their voice networks and depend on the voice networks for primary communications. However, the 700 MHz national broadband network may be used for secondary voice communications in addition to data access. In an emergency the data and secondary communication needs of public safety dynamically change and evolve as the events unfold and the public safety response is coordinated.

4G network prioritization schemes can be utilized to prioritize public safety data communications, both with respect to non-public safety communications and as a way of managing bandwidth resources among public safety users. The key to maximizing the utility of the 4G prioritization schemes is to be as flexible as possible in the assignment of prioritization of public safety communications as a function of an ongoing response.

Extending the existing network protocols with CR technology can provide tools for providing public safety with more effective dynamic network resource allocation. Information such as the role of a responder, the type and criticality of the data being transmitted, the location of the responder, the RF environment, and the overall incident command organization can be incorporated into network decisions on best allocation of network resources. Resource management can match communication demand requirements to available capabilities by

reducing video transmission requirements by using higher compression techniques or lower frame rate, or reducing priorities for non-critical communications. Cognitive radio capabilities are also useful by providing inputs for prioritization decision logic. Such inputs can include the role of the responder whose device is transmitting, the nature of the transmission, the location of transmitters and intended receivers, and/or the RF environment. Broadly stated, the value of cognitive radio technology here is the ability to incorporate application level information into lower layer control decisions, and thereby assure that all resources are optimally allocated given the prioritization of network uses.

Adaptive Beamforming

The term "Adaptive Beamformer", often used interchangeably with the term "Smart Antenna" is by no means a new or unproven technology. Radar systems have used such techniques for decades to reduce interference from jamming and other interference sources such as radar returns from the ground or weather clutter. The SDR Forum recognizes the value of smart antennas as a SDR technology. In fact, the Forum has a working group dedicated exclusively to smart antennas and also devoted an entire session to these technologies at their 2007 technical conference. Park et al, from a paper presented at the 2007 conference[12] defines a smart antenna as follows:

> "For (a) smart antenna system the desired signal, of desired direction, can be selectively transmitted/received controlling the phase of (an) array antenna as well as drastically decreas(ing) the effect of interference. That means, the smart antenna system …. minimizes the powers of undesired signals by beamforming, maximizing the gain to the desired direction. Thus, as it can decrease the noise of the received signal drastically, the smart antenna technology can improve the communication capacity and quality forming the adaptive beampattern to each receiver."

Simply stated, traditional smart antennas improve signal quality by maximizing antenna gain in desired direction(s) and minimizing gain in undesired direction(s), such as the direction(s) of received interference sources.

The processing algorithms used by traditional adaptive beamformers could conceivably be made even more effective by introducing additional intelligence provided by a cognitive radio terminal or network. For example, if the CR terminal or system has knowledge of locations of interference sources, this can augment the interference direction estimates made by the traditional beamformer to improve accuracy, algorithm convergence time, and/or effectively increasing the "degrees of freedom" of the beamformer to enable additional interference sources to be nulled and/or directional beams to be formed.

Adaptive beamformers will be most effective for the "one-to-one" type of communications (i.e., individual calls) envisioned for the shared system as apposed to a system that use predominately "one-to-many" (i.e. group) calls that would require forming several simultaneous beams.

[12] Park, S., Seo, S, and Chung, J., "Implementation Of A MIMO Evaluation Platform For SDR Base Station", presented at the 2007 SDR Forum Technical Conference, November, 2007, Denver, CO.

3.2 Evolving over Time

Challenge 2: The national broadband network infrastructure will need to adapt and change over time as operational experience is gained, as technology changes, and as commercial and public safety user-requirements evolved.

One of the keys to the success of the proposed network is its ability to evolve over time. The build-out period of the network is 10 years; the utilization period will be much longer. Even with a well-constructed network sharing agreement in place, evolving commercial and public safety needs will place competing pressures on the network. The PSST Bidders document acknowledges this as well in requiring that the common air interface "shall allow migration to future technology upgrades."[13] There are a number of factors that will drive evolution of the network.

Operational experience. The proposed network is an ambitious undertaking that will involve secondary use of public safety spectrum by commercial users and pre-emptible use of commercial spectrum by public safety users. This concept of operations involves associated issues of governance, operational control, and technology to support divergent requirements on an unprecedented scale, so adjustments will be required as operational experience is gained in using the system. The challenge is to ensure sufficient flexibility in the network to allow changes to be rapidly implemented.

Additionally, it is difficult to predict a priori how different design choices will affect key goals such as capacity, efficiency, robustness and coverage. In order to guarantee that public safety users' strict requirements are met, network designers must make conservative choices in any area where modeling or small-scale experiments provide uncertain predictions. As operational experience with the network is gained, the most conservative design choices may be able to be relaxed to provide greater capabilities without incurring greater risk.

Technology refresh cycles may differ. Technology refresh cycles of public safety networks and commercial networks historically have been vastly different. Part of the benefit to public safety of the commercial partnership is to leverage commercial developments and take advantage of the more rapid technology refresh cycles to ensure that public safety benefits from technology upgrades. However, public safety must also manage the implications of evolving technology in training, policies, and procedures. Such factors may naturally drive differences in technology refresh cycles between commercial users and public safety users. Also, as public safety technology refresh cycles shorten, expensive public safety equipment will need to be upgradeable rather than replaced to preserve the investments that have been made. (We recognize that while software upgrades can extend the life span of a hardware device, increasing software demands on hardware components such as memory and processing speed often drive the replacement of hardware as well as software.)

Requirements evolve over time: Communications requirements for public safety agencies evolve over time. Demographic changes cause changes in coverage requirements; building construction and vegetation growth change RF performance; organizational changes cause policy and procedure changes; availability of new data changes capacity requirements; and operational lessons learned cause reviews and changes to policies and procedures and possibly radio

[13] Public Safety Spectrum Trust, *Public/Private Partnership Bidder Information Document*, Version 2.0, 30 November 2007, Public Safety System Trust, Section 2.3.2(4).

features. Given the historical life-span of public safety networks and the expected life-span of the 700 MHz broadband network, one can anticipate a variety of desirable changes over the lifetime of the network to ensure that users' requirements continue to be met.

Software Defined Radio/Cognitive Radio Capabilities

In the new 700MHz system, provision must be made for performance issues that appear during deployment, upgrades, changes in requirements, new operations policy, and introduction of new technology as operational experience is gained in its use. SDR supports sufficient flexibility in the network to allow rapid implementation and deployment of necessary changes.

With SDR in the infrastructure, it becomes practical to validate new behaviors on a small scale to validate their performance in actual operation. A new radio device with a waveform modification can be deployed to a single agency (or even a single fire engine). The software necessary to support that waveform can be remotely loaded onto all the infrastructure base stations in the operating area of that agency. However, no resources need be dedicated in any cell to supporting that waveform, except when a user with the new device is actually present in a given cell and using the feature. The feature can be used for a time, its correctness and interaction with other aspects of the system checked, and the operational concepts (CONOPS) to employ it developed—all without visiting a single infrastructure site or taking significant resources away from the primary operational system. Once the new feature or waveform has been approved for wider use, it can be rapidly and cost effectively deployed, especially if SDR is used in the mobile devices in addition to the infrastructure.

The ability to "improve as you go," enabled by the flexibility of SDR, will be highly valuable given the complexity of the new network and the many challenges facing its designers. Initially the network can be built out with a highly conservative design, for example allocating significant processing and radio resources to public safety users. As operational experience is gained, the network can be gradually evolved through software downloads towards an operating mode that frees more resources for commercial operation, while still meeting all public safety requirements. New changes in this direction can be evaluated in small-scale use, than deployed more widely once all stakeholders have developed trust that the changes are safe. The flexibility of SDR to evolve over time enables the network operator to achieve much higher efficiencies and commercial returns over time than would be possible if all design decisions had to be made before the network is built or deployed.

Operating multiple waveforms could also provide the flexibility necessary to meet the evolving requirements of the system. For example, commercial users could adopt a new or modified protocol first, without requiring public safety users to do likewise. This approach ensures that commercial users are not restrained from adopting new technology, and public safety users are not pressured to adopt new technology that could put them at risk. SDR directly solves this problem; an infrastructure base station can host software for supporting multiple waveforms. If there are users with an older waveform in the local cell at the current time, resources such as spectrum and processing capacity can be allocated as appropriate to support them. If all users are on the latest waveform, the capacity of the base station can be focused on that waveform. The ability to support multiple waveforms enhances operability and interoperability while simultaneously enabling introduction of new technology, and allows network resources to be allocated as needed, regardless of the technology in use by the users on the system.

Therefore, SDR makes it feasible to evolve the network, a particularly critical capability given the unique and innovative nature of the public/private partnership concept.

3.3 Supporting Unique Public Safety Requirements

Challenge 3: Design of the network to meet unique requirements of the public safety users may not be optimal solutions for commercial users.

There are several aspects of the national broadband network that are specific to meeting the needs of the public safety users of the system. These requirements are typical for public safety systems, so in one sense they do not represent any requirement beyond the state of practice for network implementation. However, these requirements are not typical for commercial systems, and must be met in the context of a shared network rather than a dedicated public safety system. SDR/CR technologies can provide specific capabilities that facilitate the ability of the national broadband network to meet these requirements. In the sections below, we address the following public safety requirements:

- The network must maintain communications capabilities in the event of disastrous and emergency conditions, including loss of power.
- The network must effectively and dynamically manage resources to ensure the most effective use of communications resources when demand exceeds capacity.
- Local public safety agencies must manage incident response communications based on local policies and procedures while using the resources of a national network.
- The national broadband network must interoperate with other public safety networks in a "system of systems."

3.3.1 Operation in Adverse Conditions.

Public safety standard network configurations are required to be resilient to emergency conditions that threaten normal operations. Even well-designed networks can be subject to failure, especially in unanticipated events (natural or man-made). Economically viable approaches are needed to supplement the traditional approaches for providing redundancy and reliability to achieve and surpass public safety requirements.

There are three primary areas of vulnerability that can disrupt communications under emergency conditions. One is a dramatic increase of voice and data traffic, overloading some components of the system. The second is loss of power or damage to system components such as antennas and cables. The third is catastrophic failure, such as a tidal surge that immerses a base station under salt water.

Software Defined Radio/Cognitive Radio Capabilities

SDR/CR cannot directly repair physical damage. It can, however, augment the traditional techniques of physical hardening, replication, and redundancy of equipment by providing new and innovative ways to fill gaps in capability during disasters and emergencies.

One effect of a localized disaster or emergency in a public safety system's service area is increased traffic load for the base station sites that provide coverage to that location. If the sites do not have sufficient bandwidth to accommodate the additional traffic load, the Quality of

Service could be degraded to the point of precluding rapid channel access required during life critical situations.

SDR/CR can recognize when such a situation occurs (via traffic monitoring and geolocation capability) and perform dynamic reallocation of channel capacity throughout the network to support higher traffic volume in the disaster area. Such reallocation may be accomplished by a priori frequency coordination, with a number of preplanned resource reallocations established to respond to a variety of disaster scenarios. With SDR/CR the response may be extended to dynamic solutions, whereby the system recognizes in real-time sites with low volume or lower priority traffic from which to "borrow" additional resources for the duration of the disaster response.

SDR/CR brings additional potential solutions to system architecture disaster profiles. One is shedding traffic to lower power consumption and extend fuel operating time. The system can also perform an area-wide optimization of fuel reserves to direct higher traffic volumes to radio sites with the most kilowatt-hours of power availability.

Even with physical hardening of sites and equipment, a severe disaster (e.g., a category 5 hurricane disabling a site designed for category 3 hardening) can cause gaps in radio coverage if sites or equipment are submerged, severely damaged, or lose power backup. For these instances, SDR/CR capabilities are applicable for coverage re-optimization and extension into the coverage gap from nearby sites, so that users in their coverage areas are provided connectivity (as described in Section 3.1 under Coverage Extension). Air interfaces from the nearby sites' base stations and the subscribers within the disaster area could be changed to ones that provide enhanced coverage to improve the coverage overlap in the affected area.

Another potential benefit of CR used in conjunction with SDR radios that have multi-service capabilities (e.g., radios that have both public safety LMR for their primary service and a cellular commercial service) is to effect a combined network and radio change to the alternate service in the area where the primary service is down. This has the same effect as the requirement in the Report and Order for portables to have satellite capability, but may be more cost effective.

Careful site selection and emergency power resources are the foundation of disaster preparedness. Careful development of disaster scenarios and detailed response plans to deal with each of them are also essential. A whole new level of resiliency and responsiveness can be derived with the dynamic reaction provided by CR coupled with the flexibility of SDR and the extended operational flexibility they provide.

3.3.2 Dynamic Resource Management

The mission critical nature of public safety communications requires more complex bandwidth management than required for non-critical communications, particularly to meet competing public safety requirements when capacity limits are approached. Public safety networks are designed with the ability to manage network resources on a per-user priority basis. Network resources are assigned based upon the priority level that each user or talkgroup has been assigned in the network. Commercial networks, while providing users with different pricing schemes, generally do not implement the real-time per-user prioritization that is required by public safety.

Software Defined Radio/Cognitive Radio Capabilities

Capacity/Bandwidth Management

For a communications channel *i* with bandwidth B_i and signal to noise ratio $(S/N)_i$

Shannon's Theorem[14] states that the minimum bandwidth B_i for achieving capacity (in bits per second) C_i is as follows

$$B_i = C_i / \log_2[1+(S/N)_i] \quad (4)$$

The actual B_i (bandwidth) required to achieve a given throughput rate is modulation dependent and, in practice, larger than the value given by Equation 4. Since the modulation to be used for any 700 MHz public safety data system is unknown at this time, for purposes of this discussion (without loss of generality), the actual bandwidth Bi required will be assumed to be *equal to* the lower bound given by Equation 4. Defining B_{tot} as the total bandwidth of all licensed frequencies available to the communications system bandwidth for the system that is available for data communications, and M as the number of data transfers that will be allowed to occur simultaneously in the system, we have

$$\sum_{i=1}^{M} B_i = \sum_{i=1}^{M} \frac{C_i}{\log_2[1+(S/N)_i]} \leq B_{tot} \quad (5)$$

Equations 4 and 5 provide the following insights as to how cognitive radio might be used to maximize capacity within the fixed total system bandwidth B_{tot}.

Adaptive Assignment of "Just Enough" Bandwidth per Data Transfer Path. Equation 4, a system with adaptive modulation and/or error rate control can achieve a given capacity C_i by allocating less bandwidth B_i to, communications paths with high $(S/N)_i$ can be allocated less bandwidth B_i to meet a capacity requirement C_i than paths with low $(S/N)_i$. This makes more bandwidth available for other communications paths thus enabling a greater number of paths *M* and/or higher path capacities C_i compared to blindly using the same large bandwidth for all paths based on worst case $(S/N)_i$. $(S/N)_i$ can be estimated by an intelligent system based on knowing the positions of the data subscribers by GPS (or other means) or by the subscribers measuring received signal levels and assuming reciprocity of the communications paths.
While current communications systems provide some mechanisms to perform this adapative assignment, CR capabilities provide much greater capabilities for bandwidth management, by incorporating application-level information (e.g., user's role in emergency response, location, data transmission type) into the control of lower level capacity/bandwidth management features

Per User Capacity Adjustments. From Equation 5, as the number of simultaneous transfers *M* increases (corresponding to more users trying to transfer data), a point is reached where the summation in Equation 5 does not meet the requirement of being less than or equal to the total system bandwidth available B_{tot}. At that point, an intelligent system can respond in one or more of the following ways, based on monitoring system traffic or other means:

[14] Shannon, C.E., *The Mathematical Theory of Communication*. Urbana, IL:University of Illinois Press, 1949, reprinted 1996.

Start limiting users (M). An intelligent system can start shedding users, perhaps those with lowest priority, so that M is decreased and the summation of Equation 5 correspondingly decreased to the point of satisfying the equation. In practice this can be accomplished by dropping calls or blocking calls.

Adjust Per User Capacity. Based on information about how this will impact perceived user QoS, an intelligent system can reduce the data rate C_i for some of the transmissions to reduce the summation of Equation 5.

Dynamic Bandwidth Allocation. In cases where the bandwidth occupancy of the system approaches B_{tot}, an intelligent system can "borrow" bandwidth from another less loaded or lower priority system (at the expense of decreased capacity of that system) to increase B_{tot} and enable more users and/or higher capacity C_i per user. One way of accomplishing this is to have a shared pool of frequency channels that are available for use in more than one system, but only used in one system at a time.

For example, if several video streams were pushing bandwidth requirements to capacity limits, one approach is reduce the frame rate or increase the compression of some (or all) of the video streams. Selection of method and specific transmissions could be accomplished by user direction or automatically (or semi-automatically) based on policy definitions, information content, or other criteria. A policy could be defined to limit the degradation of video being used for emergency medical reasons, or to prioritize the video from a bomb disposal robot over other video applications. Other approaches based on the frequency of movement or image changes could also be applied to temporarily reduce video quality to reduce bandwidth demands. Some of the management of bandwidth requirements could be incorporated into applications; for example, biometric information communicated from first responders could be reduced to only be communicated when outside of a pre-defined (normal) range.

Intelligent Routing: One approach to managing network resources is to align communications resources based on the content of the message. For example, a man-down alarm signal is the highest priority signal and is transmitted across the most robust communication link. Information which is not real-time critical can be sent via communications links that are less robust.

Dynamic Prioritization: To the extent that public safety networks today incorporate priority access, the priorities are statically defined based on how the radios are programmed. For example, in a voice network, a supervisor may have access to an incident command talk group which has priority over administrative talk groups. The PSST highlights the need for priority access to the national broadband network, including the concept of role-based priority assignment.[15] This is a valuable capability to allow network resources to be allocated to the most important communications needs. Note that this prioritization is not simply prioritization of public safety traffic over commercial traffic, but can allow for distinctions between the priorities of life-critical medical telemetry data and routine communications associated with incident logistics management.

Current capabilities generally associate priorities with individuals or devices, and remain static. However, in the SDR Forum's first report on cognitive radio use cases[16], dynamic prioritization

[15] Public Safety Spectrum Trust, *Public/Private Partnership Bidder Information Document,* Version 2.0, 30 November 2007, Public Safety System Trust, Section 2.8.3.

[16] SDR Forum, *Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 1: Review of the 7 July Bombing of the London Underground,* November 2006, available at www.sdrforum.org.

was identified as a potential use case for cognitive radios. The application of cognitive capabilities provides the opportunity to adjust priorities to accommodate unanticipated priorities or to manage priority access in real-time. First responders can be assigned a priority based on their role in support of the response (e.g., evacuation of critically injured could have a priority over traffic control at the incident perimeter). Priority modifications can be downloaded to the first responders' devices as needed. In addition, cognitive capabilities in the network management can recognize the increasing load level and congestion levels and block or reduce access to lower priority calls as needed. User devices can also have a cognitive capability that indicates that user access has been blocked so that the system loading is not made worse by persistent access attempts. The SDR Forum Report[17] provides more detail on different approaches that could be followed for the assignment and management of the role-based priority assignments.

3.3.3 Network Control

Local public safety radio managers often own and operate the infrastructure transport elements of the system. This gives them control over redundancy, maintenance, expansion, coverage, and other network operations and management functions. Many public safety networks, for instance, do not lease commercial towers or commercial circuits to interconnect towers. Instead they build microwave links that they own and control. In situations in which public safety agencies do lease components of the network, they are often dedicated to public safety use. Drivers for this organizational preference to own the infrastructure include the need to ensure build-outs in sparsely populated areas, and to avoid over-subscription from shared usage.

The D-Block 700 MHz licensee's infrastructure will be, by definition, shared with non-public safety uses and applications. Moreover, in any given area (city, county or region) many different "public safety" entities will be operating on the same network, which will be the D-Block licensee's facility. This common use requires the development of mechanisms that can be trusted, at least as well as current methods and mechanisms typical in existing public safety-only networks, to provide the public safety broadband licensee (PSBL) and its constituent agencies with controls. These controls must be more robust than simply enforceable contractual requirements, because these users will have no option to take their broadband business elsewhere—all broadband public safety spectrum will be subsumed under the D-Block license and cannot be disaggregated.

To adequately support the first responders, the FCC has recognized that the PSBL must be able to exercise operational controls in real time. This control must include built-in agility and network management capabilities to allow the PSBL to determine that the network is always configured to meet the needs of many types of first responders simultaneously responding to different events, of different duration, in different geographic areas, and constituting different levels of "emergency." The concept of operational controls could include the ability to actually control certain network infrastructure behaviors and to exercising operational and network management policy control in real time. This is consistent with the PSBL's responsibility to assist the D-Block licensee to meet the standard of "ensuring public safety requirements are met."

[17] SDR Forum, *Software Defined Radio Technology for Public Safety*, SDR Forum Report No. SDRF-06-P-0001-V1.0.0, available at www.sdrforum.org.

In addition to the shared operation control issue between the lessee and the PSBL, there is also a control issue with respect to ensuring that communications support the National Incident Management System (NIMS) while allowing local variations and implementations of NIMS requirements. NIMS defines a framework for incident response. The communications capabilities deployed for incident response, including the public/private broadband network, must support that response. However, NIMS is intended to be flexible to accommodate local and regional differences in public safety agency structure and functions, and incident variations. Thus, while NIMS provides overall direction and commonality in incident response command and control, communications policies and procedures will vary. Furthermore, responders may desire particular features of their “home” system that can be executed in the network while preserving interoperability.

Software Defined Radio/Cognitive Radio Capabilities

The application of emerging SDR and CR technologies in the PSBL's and D-Block spectrum helps ensure that the national broadband network for public safety and commercial users can be managed efficiently, meet commercial requirements for profitability, accommodate local and regional variations in policies and procedures, and allow the PSST to confidently manage its responsibilities to ensure public safety communications requirements are met today and into the future. Employing a policy-based radio architecture provides operational controls to meet these disparate needs and requirements. Perhaps the most important contribution a policy-based architecture can make is its ability to dynamically adjust the use and configuration of network assets to ensure both spectral efficiency and network performance—especially in disaster management and emergency conditions.

Policy-Based Network Infrastructure

The concept of a policy-based network is based on real-time dissemination of policies. Policy-based wireless systems automatically adjust their operation based on new rules and constraints in terms of frequency bands, bandwidths, power levels, sensing configuration, and network topology. This enables a rapid automated network establishment and interoperability with other wireless systems without extensive planning while providing transparency to stakeholders.

CR-based capabilities can provide operational control of discrete network assets and infrastructure at any time. Even where infrastructure is damaged, or hasn't been built, some communications capabilities can be established without reliance on communications infrastructure such as towers, base stations and back-haul networks. For an ad-hoc policy-based radio system, policies define the network architecture rather than the physical infrastructure. Policy infrastructure is used to create the "stack" of operational protocols that the radios follow in any geographic, frequency, or time dimension. A CR can reconfigure itself dynamically in order to optimize spectral efficiency and performance, to operate in conditions where no radio infrastructure exists, and to avoid harmful interference under conditions where many non-cognitive radio signals are detected. It has not only autonomy to create, join and maintain networks, but also to follow enforceable parameters that oversee the correctness of the cognitive network operation as well as the operation of every cognitive-networked device.

Enforceable parameters included in downloadable policies might include:

1. Frequency bands, standards-based waveforms, and power output

2. System identifier and system key for any existing first responder system in any geographic region.
3. Tactical interoperability requirements. For example, elements of an Urban Area's Tactical Interoperable Communications Plan could be incorporated into policy definitions.
4. Mutual aid agreements. For example, the ability and authorization to use a specific frequency under conditions of a mutual aid agreement could be disseminated as a poicy.
5. Existing radio system talk groups and licensed channels.
6. Prioritization of use. Policices could define priorities based on responder roles and incident command structure.
7. Quality of service (QoS) as a function of user

Dynamic policies: Dynamic policies can be loaded onto radios at any time, including during the management of an incident. These might include:

1. Incident command structure ("virtual talk groups")
2. Incident awareness information
3. Routing policies for specific types of information (e.g. data and images)
4. Revisions to pre-determined policies (such as user prioritization)
5. Updated talk group information
6. Updated frequency use information
7. Updated geographic data

The benefits of CR technologies for operational management are:

- Flexibility: High-level specification policies apply to multiple heterogeneous devices simultaneously.
- Autonomy: Cognitive devices autonomously balance their resources and optimize networks as permitted by policies. Different models can be implemented to allow various approaches to human intervention; for example, cognitive radios could eventually be developed that execute general direction from the network manager or Communications Unit Leader based on policies and in reaction to their environment.
- Assurance: Policies from multiple stakeholders are enforced locally on every device at runtime, guaranteeing proper operation without violating any requirements.
- Transparency: High-level specifications can be verified by theorem-proving systems for correctness at any time.
- Ease of policy authoring: A policy may be able to abstract low-level requirements.
- Secure policy management and distribution: The management framework allows control of the policies a device is using as well as monitoring a device. Using a

distribution system model, policy commands and queries can be securely transmitted. The framework can be further secured for limiting who can control devices.

- Traffic management and control that can more efficiently (than non-CR systems) utilize network resources as needed across public safety and commercial uses. For example, SDR/CR technology can allow rapid reconfiguration to meet evolving incident response needs. CR can perform "smart" dynamic channel allocation, depending on user locations and the amount of traffic measured per geographic area. CR can perform load balancing at the network level, limiting lower-priority traffic in bandwidth and/or message times.

3.3.4 Systems of Systems.

The concept for public safety networks of the future is predicated on a system of systems concept. As described by the SAFECOM Program,[18] public safety communications is a system of systems that includes:

- Personal Area Network (PAN): Communication among devices associated with an individual.
- Incident Area Network (IAN): A temporary network created for communications required for a specific incident.
- Jurisdiction Area Network (JAN): The primary network of first responders that carries voice and data traffic not carried by the Incident Area Network, and connects to the Extended Area Network.
- Extended Area Network (EAN): regional, state, and national networks.

The national broadband network fits the definition of the Extended Area Network but could also support the Jurisdiction Area Network functions and, depending on the nature of an incident, the functions of an Incident Area Network as well.

Software Defined Radio/Cognitive Radio Capabilities

The flexibility of SDR/CR capabilities provides advantages for incorporating the national broadband network into the system of systems concept. As a national broadband network it fits the definition of EAN. But consistent with system of system concept, it may also provide capabilities that are incorporated into, or interface into, an IAN. IANs, by definition, are temporary networks established for the purpose of providing communications support to a specific incident. The flexibility provided by SDR technology, as noted in Section 3.1, provides tools for configuring the national broadband network to fulfill as needed requirements of the IAN. For example, as incident response communications grow, consistent with the network sharing agreement, a segment of the D-Block spectrum could be allocated specifically to support IAN requirements. The dynamic parameters of the IAN (such as channel assignments or priorities) could be downloaded to subscriber equipment as policies.

In other cases, an IAN may be established using licensed 4.9 GHz spectrum; in this case the national broadband network may need to establish gateways that provide an interface between

[18] Dept. of Homeland Security SAFECOM program, *Statement of Requirements for Public Safety Wireless Communications and Interoperability*, Version 1.2, October 2006, available at www.safecomprogram.gov.

the 4.9 GHz network and the national broadband network at 700 MHz. Rapidly reconfigurable gateways implemented using SDR technology can facilitate this process as well.

The result of these capabilities is a significant new resource for Public Safety users. Not only does the national network provide extended connectivity, it also serves as a pool of resources whereby Mobile Virtual Networks (MVN) can be quickly instantiated to meet local needs. Because these capabilities are supported by the public/private partnership, use of MVN capability is not restricted to emergency situations.

Reconfigurability at the subscriber device level is another potential application of SDR technology. Ideally a responder would not require different devices to access the different networks that are being used; SDR and cognitive radio technology can facilitate single devices that operate seamlessly on multiple networks.

3.4 Interoperability with other 700 MHz Networks

Challenge 4: Based on the build-out schedule, there may be other 700 MHz networks that will need to interoperate with the national broadband network.

Even with the aggressive, population-based build-out schedule required for the D-Block licensee, many areas of the country will not be served for several years, and areas with sparse population are unlikely to be covered at all. There may be vast geographic areas especially in the central and western states, mountainous regions and tribal lands, without national broadband services for either commercial or public safety use.

Recognizing this challenge in connection with public safety use, the FCC will allow local public safety entities to build out and operate separate systems. These systems must be operated at their own expense, in the 700 MHz public safety broadband spectrum, subject to several regulatory conditions and restrictions. The Public Safety Broadband Licensee must approve any such separate, independent network and enter into a spectrum leasing arrangement with the public safety entity (FCC 2nd R&O at Paragraphs 470-484; 47 C.F.R Sec. 27.1330). The rules also require these independent networks to (1) provide broadband operations; (2) be fully interoperable with the shared national broadband network; (3) be available for use by any public safety agency in the area; and (4) satisfy any other terms or conditions required by the PSBL. The Public Safety Broadband Licensee must also retain control of the entire spectrum associated with such local leases and exercise actual oversight of the spectrum lessee's activities. In areas subject to a build-out commitment, the public safety entity may not commence operations on the network until ownership of the network has been transferred to the D-Block licensee.

Constructing systems in remote areas with local funding (or limited federal grant money) in a way that meets these requirements may be difficult. Moreover, these sparsely populated areas may not be attractive to the commercial D-block licensee, who is also prohibited from partitioning its nationwide license to other commercial or public safety entities seeking to cover unserved areas (47 C.F.R. Sec. 27.1333). The PSBL is similarly restricted (47 C.F.R. Sec. 90.528(e)). Finally, the FCC rules require that the D-Block licensee make available to public safety users at least one handset that includes a seamlessly integrated satellite solution, do not set forth a time table for the handset's availability and do not require that the D-Block licensee incorporate support for satellite communications into the infrastructure of the shared terrestrial network.

Software Defined Radio/Cognitive Radio Capabilities

For those low density communities that fear being left behind in the broadband era (as when railroads and highways may have bypassed them in the past), cost-effective SDR/CR technologies could allow the development of compatible local public safety and commercial broadband systems which meet the robustness and reliability requirements of the nationwide broadband network in the event they are eventually integrated. While a single hybrid terrestrial/satellite device is required, the cost of this service is uncertain.

SDR/CR technologies can facilitate the use of commercial off-the-shelf (COTS) end-user devices that work on the shared national broadband network, local independent public safety networks and ad-hoc "gap-filler" networks. This is accomplished with capabilities in the infrastructure that can use multiple waveforms to accommodate legacy equipment and can use CR capabilities to recognize legacy equipment. Designing the broadband network to accommodate other users allows seamless operability and interoperability and the rapid formation of terrestrial networks where a fixed network infrastructure is damaged or unavailable. Just as existing private computer networks interoperate seamlessly with the Internet, locally financed, constructed and operated public safety IP-based 700 MHz networks using SDR/CR technology could accelerate the provision of broadband public safety service in areas where coverage from the D-Block operator is not available.

The use of SDR/CR capabilities to facilitate interoperability among a national 700 MHz network and other 700 MHz networks may require more dynamic agreements for spectrum use than are currently in place today. For example, a dynamic spectrum leasing arrangement would be particularly useful where spectrum access is needed only to fill coverage holes with temporary ad-hoc networking or where additional capacity is required for bandwidth intensive applications. Such leasing arrangements would accommodate the ability of funds-limited local public safety entities in rural communities to use CR technology to access 700 MHz broadband spectrum opportunistically only when needed and using deployable (e.g., a mobile repeater to link an out-of-coverage area to a permanent network) rather than permanent infrastructure. Alternatively, in order to get broadband service for both public safety users and its citizens, such communities may have to resort to leasing or buying spectrum from 700 MHz licensees in other blocks that are not subject to the restrictions imposed on the D-block and the public safety broadband spectrum.

3.5 Cost and Usability

Challenge 5: Meeting the technical and operational challenges for building a national broadband network should not add significant cost or detract from the usability of the subscriber equipment.

The discussion up to this point in the document suggests subscriber equipment that includes significantly greater complexity than current devices. However, forcing the user to be aware of and manage that complexity is counterproductive. For the public safety user, a simple user interface that allows the user to properly control the radio to perform the necessary functions is of overriding importance. There is no room for confusion or complication when a responder is in a life-threatening situation. From the commercial perspective, the motivation for usability of the device is somewhat different; consumers that have choices as to networks to use may be less likely to choose a system that requires significant effort to learn to use.

In addition, there are economic incentives for cost containment for both public safety users and commercial users. If the capabilities described in the preceding sections add significant cost to subscriber equipment or the cost of services, loss of customers could undermine the economic viability of the public/private partnership.

Software Defined Radio/Cognitive Radio Capabilities

With respect to the user interface issue, there are a number of capabilities of SDR/CR radios that could assist in ensuring an appropriate user interface for users. SDR-based reconfigurable radios can ensure that a first responder's radio functions as expected. SDR/CR capabilities to provide an interface between a conceptually simple user interface tailored to the user needs and a conceptually complex distributed network and spectrum resource management capability. For example, a first responder only knows that they must communicate with the dispatch center of another agency, or that they need to be on the channel designated for perimeter traffic control. The user interface should allow that information and choice to be made to the user—details as to the frequency band, specific channel assignment, priority, interference mitigation approach, and so on, are determined by the radio. CR capabilities determine the above information based on the dynamic communication and response environment, and SDR capabilities allow the radio to reconfigure as needed to execute as needed.

CR capabilities can also be implemented to "learn" user preferences, patterns, and needs. This capability has the potential for simplifying the burden on the user (while ensuring the reliability of the equipment, the ability to override the system to support emergency communications, and so on). In general, the objective of this technology is to use the SDR/CR capabilities to provide an interface between a conceptually simple user interface tailored to the user needs and a conceptually complex distributed network and spectrum resource management capability.

One of the concerns often expressed within the public safety community regarding SDR/CR is that as radios can be reconfigured to allow interoperability with more entities and with much greater flexibility, the ability to control communications paths becomes more difficult. Allowing everyone to communicate with everyone turns interoperability into chaos. In addition, as more data can be made available to responders in the field during incident response, the prospects for information overload also increase. SDR/CR technology can help manage that process. SDR reconfigurable radios can be configured so the responder has access to the communications capabilities, and only those capabilities, that are needed. Reconfigurability and over-the-air programming can ensure that the definitions of "what capabilities are needed" can evolve as an incident evolves, as responders assume new assignments, as the incident response organization evolves, and so on. CR capabilities allow the definition of "what is needed" to evolve as a function of factors that can be sensed by the radios, including the responder's role, the type of communications, location, RF environment, and so on.

SDR/CR can also provide some cost savings, particularly in terms of life cycle cost. For example, there is a significant potential for cost savings for over the air reprogramming. Excluding the time required to determine and validate new versions of software, there are costs associated with the technician time required to perform the installation, and the officer / customer time necessary to bring each radio or device into a radio shop for the reprogramming. Cost estimates for those activities can range from $120-$150 per radio, so the execution of a reprogramming exercise for a large sized department maintaining several thousand radios (including both mobile and portable devices) or a network with millions of subscribers can

become a significant budgetary item. Thus there are economic benefits as well as timeliness benefits to incorporating the flexibility of SDR technology to allow over the air upgrading, reprogramming, and reconfiguration capabilities in the network.

4 Evaluation and Certification Issues

A secondary impact of the introduction of the SDR/CR capabilities described in the preceding sections is the need to enhance evaluation and certification techniques. Many of the identified capabilities include the ability to reconfigure or reprogram radios in ways that are not accommodated by current regulations and type acceptance procedures, and will require new approaches to evaluation and certification.

The PSST Bid Document defers the responsibility for testing to the commercial partner, with an expectation of an accelerated process on the part of the commercial partner.[19] This approach is consistent with the objectives of leveraging commercial products and leveraging existing commercial certification processes such as the WiMAX Forum. It also avoids the expense and governance challenges that have been experienced by projects such as the Joint Tactical Radio System (JTRS) in setting up the Joint Test & Evaluation Laboratory, and P25 in setting up the P25 Compliance Assessment Program.

The introduction of reconfigurable and cognitive radios will require certification approaches that go beyond the certification done today to ensure that devices meet a particular standard. For example, for policy-based devices such as those described in Section 3.3.3, it is necessary to ensure that a policy is consistent, that a policy received by a device is legitimate, and that the policy can be executed on the device properly. Currently To provide guidance on how to effectively test such devices, the IEEE P1900 project is looking at the issues of evaluation and certification of cognitive radios. Specifically, the IEEE P1900.3 Working Group has begun work on developing Recommended Practice for Conformance Evaluation of Software Defined Radio (SDR) Software Modules. To date this Working Group has begun to analyze the tests necessary to ensure the proper operation of software defined and cognitive radios.

The SDR Forum, also recognizes that development of techniques to evaluate such devices for acceptance purposes will be an important aspect of introducing these capabilities into the market, and is taking proactive steps in these areas. The Forum recently held a workshop in April 2008 in Rome, Italy that included discussions of certification of various types of SDR devices. As evidenced by papers presented at this workshop, the military is the predominate driver of SDR certification processes at present, but can serve as a starting point for developing certification processes for the SDR/CR capabilities described in this report. In one paper[20], an SDR certification process was discussed by the European Defense Agency (EDA) with the goal of maximizing interoperability and code portability between SDR devices. In another paper[21], the European Joint Research Center (JRC) discussed a certification process with the goal to "Provide reference and independent Test and Evaluation capabilities of technologies, including certification aspects, for ensuring the availability of efficient communications systems for security applications." Still another paper[22] discussed general European initiatives to certify

[19] Public Safety Spectrum Trust, *Public/Private Partnership Bidder Information Document,* Version 2.0, 30 November 2007, Public Safety System Trust, Section 3.7.1.

[20] Gari, M., "European approach for SDR Certification", *SDR Forum Workshop on SCA Test, Evaluation and Certification,* April 2007, Rome, Italy.

[21] Oliveri, F., "Systematic Approach to Requirements Collection and Analysis in the Area of Reliable Telecommunication Systems for Security Forces, *SDR Forum Workshop on SCA Test, Evaluation and Certification,* April 2007, Rome, Italy.

[22] Heijster, R. "European Software Radio Architecture", *SDR Forum Workshop on SCA Test, Evaluation and Certification,* April 2007, Rome, Italy.

"portability, interoperability and reliability". A paper from NATO[23] recognized the need for a certification process for certifying Software Communications Architecture (SCA) and interoperability compliance across SDR radios from all NATO countries and their partners. In addition, certification techniques proposed and/or being implemented by France, Finland, Italy, and India were discussed. In the United States, SCA compliance is certified via the Department of Defense's Joint Test and Evaluation Laboratory (JTEL) compliance testing.

In considering the JTRS JTEL, and consider an analogous compliance testing program for public safety land mobile radios (the P25 Compliance Assessment Program), we can draw some ideas about what may be required to support compliance testing for the national broadband network. One common theme among both programs is that compliance testing is a multi-layered approach. Joint Tactical Radio System (JTRS), which is the Department of Defense's program for developing new tactical radios, relies on SDR technology to facilitate the deployment of several waveforms on different radio architectures. A key component of the JTRS is the Software Communications Architecture, which provides a set of rules and protocols that characterize a standard operating environment and application program interface. The SCA facilitates porting of waveforms from one radio to another assuming the waveforms are compliant with the standard. components of compliance are required for JTRS radios: compliance of a radio to meet the requirements defined in the JTRS Operational Requirements Document; waveform porting compliance; and SCA compliance.

P25 is the interoperable standard for public safety land mobile radios, and is actually a suite of standards that define the interfaces between components of a land mobile radio network. Unlike the SCA, P25 does not include an standard interface among components within an individual radio; there is no definition comparable to the SCA in the JTRS. Compliance testing within P25 requires three types of tests:

- Performance
    - Do radios A and B meet specifications?
- Interoperability
    - Does radio A work with radio B?
- Conformance
    - Radio A and B work together, but do they both comply with the standard?[24]

While the specifics of compliance testing for the national broadband network will be determined through the Network Sharing Agreement between the D-Block winner and the PSST, it is likely that compliance testing will need to be approached in a similar multi-layered approach. Note that different aspects of compliance testing may be conducted in different ways. One model is the Common Criteria Recognition Arrangement (CCRA), whose purpose "is to advance those objectives by bringing about a situation in which IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluation."[25]

.
[23]Barfoot, R., *SDR Forum Workshop on SCA Test, Evaluation and Certification*, April 2007, Rome, Italy.
[24] Nelson, E., "Project 25 Compliance Testing Program," presentation at the January 2006 NPSTC meeting, available at www.npstc.org/meetings.
[25] www.commoncriteriaportal.org.

The CCRA provides a profile which addresses the security aspect of IT products; such products may be subject to other compliance testing based on the specific application for which the product is intended. Similarly, devices for the national broadband network may have several profiles to address various aspects of performance (e.g., security, protocols, dynamic spectrum access), perhaps with different organizations providing the test and evaluation infrastructure.

The capabilities suggested throughout Section 3 can provide significant benefit to users and operators of the proposed national broadband network, but assurance that the network and the devices that operate on the network function properly with increasingly sophisticated functionality is critical. This issue must be addressed from a regulatory perspective, a standards perspective, and a technical perspective. While the commercial model of certification called for by the PSST needs to meet the objectives of the shared partnership, we encourage the leveraging of the ongoing developments in certification approaches to fully realize the capabilities that SDR/cognitive radio technology provides.

5 Relevant Activities of the SDR Forum

The SDR Forum is engaged in a number of activities to further the development and deployment of the SDR and CR capabilities identified in the preceding section. The SDR Forum is an open, non-profit corporation dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems, with a mission to accelerate the proliferation of SDR/CR technologies in wireless networks to support the needs of civil, commercial, and military market sectors. Activities focus on:

- Developing requirements and/or standards for SDR and CR technologies, including working in liaison with other organizations to ensure that Forum recommendations are easily adapted to existing and evolving wireless systems;
- Cooperatively addressing the global regulatory environment;
- Providing a common ground to codify global developments;
- Serving as an industry meeting place.

With the SDR Forum, key issues relating to the development and deployment of SDR and CR technology in public safety are addressed in the Public Safety Special Interest Group (SIG). The Public Safety SIG is one of several special interest groups within the Forum that bring together developers, users, regulators, and educators to address issues specific to the application of SDR technology to a particular domain or market area. The goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise awareness of SDR, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the SDR Forum. The Public Safety SIG also interacts with other committees and working groups within the Forum to provide the public safety community's inputs into the publications and initiatives undertaken by the Forum.

The Public Safety SIG is a unique venue, because participation in the SIG has historically included public safety organizations, land mobile radio vendors, advanced technology developers, service providers, manufacturers of SDR for military applications, software developers, researchers, and regulators.

Technical work within the SDR Forum is performed by the Technical Committee, which includes a number of Working Groups. Working Groups addressing specific issues relevant to the topics described in this paper include the following:

- Cognitive Radio Working Group—developing definitions, nomenclature, and conceptual models of cognitive radio to help categorize and clarify the relationships of cognitive and SDR functions.
- Metalanguage for Mobility Working Group—developing a metalanguage standard for CR applications that will enable automated SDR software installation, compatibility, and maintenance; the metalanguage standard will lead to languages for specification of policies for cognitive radios across various applications domains (e.g., commercial and public safety).
- Research and Development Working Group—identifying and describing technologies and development topics, significant for SDR/cognitive radio in terms of need, technological

challenge and maturity by creating white papers, recommendations, and summary reports, and advancing those technologies in the industry.

- Security Working Group—producing a security framework that can be applied to various uses of SDR to address security issues that arise from the introduction of SDR technology.
- Smart Antenna Working Group—developing a specification for a Smart Antenna Application Program Interface.
- Test & Measurement Working Group – Identify gaps in the existing capabilities of the test & measurement tools to facilitate development/manufacture/deployment/operation of SDR/CR enabled systems and come up with test methodolgies to meet these needs

(Other Working Groups include a Design Process & Tools Working Group, Software Communications Architecture (SCA) Working Group, System Interface Working Group, Space Working Group, and Education Working Group.)

Key technical issues associated with the deployment of SDR and CR technology outlined in Section 3 can be addressed within this Working Group structure.

The SDR Forum also has a Regulatory Committee which provides an industry perspective on regulatory issues relating to SDR and cognitive radios.

Finally, the SDR Forum has initiated a Smart Radio Challenge, in which challenge problems are defined, and university teams compete to develop demonstrated solutions to the problems.

6 Conclusions

The public/private partnership to utilize new 700 MHz spectrum is an innovative attempt to provide public safety with a needed nationwide broadband network funded by sharing resources with commercial users. This is clearly uncharted territory for public safety and presents a number of challenges. Emerging SDR and CR technologies provide near-term and longer-term solutions to meet these challenges. It is paramount that the stakeholders in the 700 MHz Public/Private Partnership plan for the benefits that can be gained by these technologies at several points in the development and deployment process:

- in the system design and implementation,
- in negotiation of agreements among the PSBL and the D-block awardee, and
- in the governance structures that are developed for use of the national broadband network.

Otherwise, the options for providing an economically viable network that meets both public safety and commercial user requirements will be unnecessarily, and significantly, curtailed.

A Technical Background

A.1 Technical Details on CR/SDR Mechanisms to Improve Coverage

For this discussion, "coverage" is characterized by the maximum distance d at which communications can occur in environments with and without interfering signals while achieving a required quality of service; the higher d is, the larger the area that can be covered at a given confidence level. Quality of service is related here to a maximum bit error rate for the received signal, above which the data integrity is deemed unacceptable.

Equation 1, which is derived in Appendix A.2 assuming line of sight communications paths[26], relates the coverage distance to various parameters.

$$d = M \sqrt{\frac{KP_t}{R[N_0 + \sum_{j=1}^{N} (ACPR_j \frac{K_j P_j}{Bd_j^{\,2}})]}} \qquad (1)$$

where

N = number of interference sources

R = data rate of the desired signal in bits per second

P_t = transmit power (watts) for the desired signal's transmitter

P_j = transmit power (watts) for undesired (interference) transmitter j

d= distance of the receiver from the desired signal's transmitter

d_j= distance of the receiver from the undesired (interference) transmitter j (if interference is present)

K = fixed constant which includes many of the desired signal transmitter/receiver design parameters (inversely proportional to the required signal to noise ratio for achieving the coverage criterion)

K_j = fixed constant which includes many of the undesired signal's transmitter design parameters

N_0 = receiver noise spectral density (fixed parameter)

B= receiver noise bandwidth

ACPRj= attenuation of the interference signal j due to receive filtering

M = margin factor (less than 1) to account for fading and required confidence level of the estimate

[26] Line of sight is assumed without loss of generality to simplify the discussion. The conclusions to be drawn are valid for non line of sight communications as well.

If no interference is present,

$$Pi = 0 \quad (2)$$

and equation 1 simplifies to

$$d = M\sqrt{\frac{KP_t}{RN_0}} \quad (3)$$

The margin factor M is extremely important for accounting for inevitable uncertainties in the estimate of *d* due to fading and other factors as well as to increase the confidence that the actual coverage range will be at least equal to the estimate. *M* varies between 0 and 1, with low values indicating high fading and/or high required confidence in the estimate.

ACPR is discussed extensively in TIA document TSB-88[27], and is a key parameter in TSB-88's suggested methodology for estimating the effects of interference on a public safety radio link. Numerous tables are provided therein that give values of ACPR for various types of modulations used by public safety (e.g., P25, analog-FM, Tetra, and numerous manufacturer proprietary modulations used today in existing public safety systems). As would be expected, the tables show that ACPR decreases (i.e, the interference is attenuated more) with

- increased frequency separation of the interference from the desired signal (various frequency offsets are shown in TSB-88's tables)
- increased receive filter selectivity, specified in terms of 3 dB bandwidth and various types of filter models (e.g,, root raised cosine with different falloff rates, butterworth, etc)
- decreased spectral bandwidth and sidelobes of the interference modulation

Figure 2 illustrates how interference "leakage" into the desired signal is affected by the above parameters.

[27] Reference TSB-88

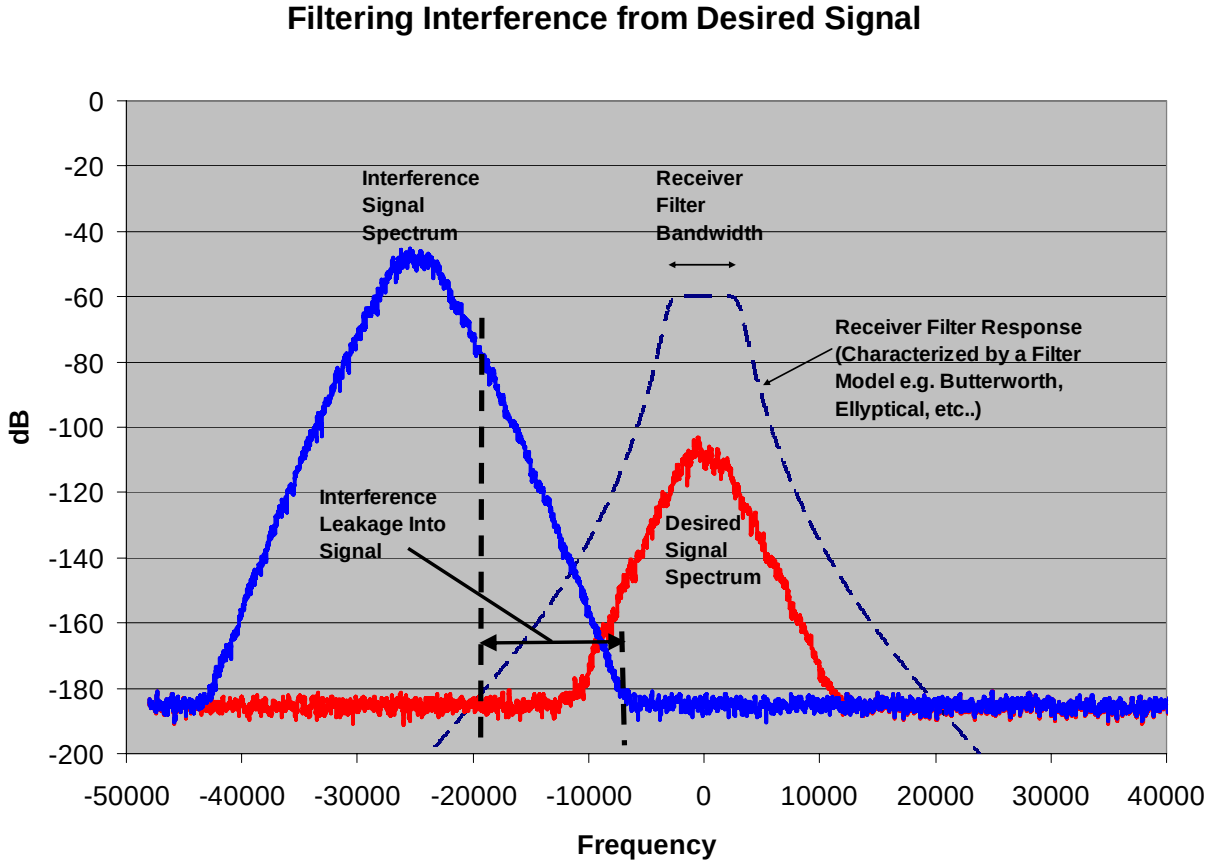

Figure 2, Interference of a Desired Signal by a Signal on a Different Frequency

If these factors can be controlled by the CR system to reduce the ACPR (i.e., increase the interference attenuation), Equation 1 indicates that the coverage distance can be increased in the presence of interference.

The parameters embodied in K and K_i are documented in Appendix A.1. For the purposes of this discussion, these and N_0 are considered fixed constants that are not practically controllable by a cognitive radio system. All other variables can be adjusted by a cognitive radio system as environments, geometries, and system loadings change to maximize d for mission critical communications paths.

Cognitive Radio's Methods to Optimize the Coverage Range d

Technology exists today to introduce "intelligence" into a system for adaptive, real time optimization of the variable parameters of Equation 1 with the goal of achieving the desired coverage range *d* for each mission critical communications link in a system. For example, suppose there is a potential for interference occurring for a critical data transfer between a transmitter and receiver at range *d* from one or more same-system interference sources. Equation 1 indicates that coverage for that communication will be improved by optimizing the following adjustments either by themselves or in a multi-dimensional optimized combination.

1. ***Increasing Frequency Separation for Interferers with Small d_i .*** It is not a major challenge for a CR system to keep track of the spatial separation distances of all of its

radios using GPS or other means.[28] A CR system can perform intelligent system-wide transmission frequency control to reduce the probability of time overlap of communications from an interfering transmitter that is too close in proximity and frequency to the receiver. Such control could be based on lookup from a ACPR table, much like those in TSB-88, in conjunction with equation 1. An estimate of the necessary ACPR can be made, and then the required frequency separation determined from the ACPR table for achieving that ACPR. Interferers with large d_i would be allowed to use frequencies closer together (higher ACPR).

2. ***Increasing the ratio of P_t to P_j when interference is present.*** Power control is already implemented in many commercial data systems with the purpose of lowering power levels when higher levels are not needed for maintaining the requisite quality of service. These techniques in essence minimize the P_i for potential interference paths as well as increasing battery life. Such power control techniques are generally controlled at the radio based on measurements of received signal to noise ratio and assuming reciprocity of the inbound and outbound communications paths. A cognitive radio system can accomplish this through knowledge of the locations of its radios, and furthermore more accurately determine the potential interference paths than could be done with a radio-centric algorithm, perhaps enabling higher power and thus quality of service on the links where there is no potential interference. Also, an intelligent CR system, using estimates from equation 1 or a variant, will have information not available in a traditional system as to when power control by itself needs to be augmented by other control adjustments listed here to establish the communications path. Furthermore, a top-priority data transmission can be assigned, by the CR system, a P_t value higher than for lower priority calls to increase the probability of successful data transfer.

3. Reducing Data Rate R. A CR system can estimate the maximum communicable data rate R either given a known communications path length d or through bit error rate measurements. Since higher data rates generally require more transmit spectrum, this determination also results in more efficient spectral utilization relative to blindly trying to transmit the highest data rate everywhere.

4. Reducing ACPR when interference is present. Adjustment 1 discussed one method of reducing ACPR by increasing frequency separation between the same-system potential interference sources. Other methods that could be controlled by a CR system for reducing ACPR and increasing coverage when the CR system determines a potential interference situation are as follows

- ***Flexible, Mode-Dependent Receiver Filtering***. The filters used in a receiver influence both the sensitivity and the tolerance of the receiver to interference. The filter choice must seek to achieve the best balance between these factors to meet system-level requirements, and will be generally different for every modulation type that is used. The modulation of desired signal can be adjusted to reduce signal bandwidth and allow more selective receive filtering (lower bandwidths, steeper frequency falloff). Alternately, the receive filter bandwidth can be reduced without a corresponding reduction in the signal bandwidth if the

[28] Even measurements of received average signal to noise ratios could be used to roughly estimate separation distances.

CR system estimates that the degradation of the desired signal caused by the reduced filter bandwidth is outweighed by the reduction of received interference. Furthermore, due to different system level requirements for public safety and commercial users, the filter may be different between the two types of systems even if the modulation is the same. SDR/CR affords the potential for dynamically reconfiguring filters in real time to enhance filter optimizations for disparate services.

- ***Lower spectral sidelobes*** of the interference transmit spectrum. Since an intelligent system can estimate which transmitters might cause interference, it can lower the data rate for those transmissions to reduce the spectral bandwidth and thus lower the ACPR and increase the coverage over the desired path.

A.2 Derivation of Coverage Range Equation

From Proakis[29], the power received P_r from a transmitter at distance d with a line of sight path between the transmitter and receiver, assuming free space propagation, is as follows:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2} \quad (1)$$

Where

P_t = transmit power

G_t = transmit antenna gain

G_r = receive antenna gain

λ = wavelength of signal

d= distance between transmitter and receiver

The carrier to noise ratio C/N is the received power P_r divided by the noise in the receiver, ie

$$C/N = \frac{P_r}{N_0 B + I} = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 (N_0 B + I)} \quad (3)$$

where N_0 is the noise power spectral density, B is the receiver bandwidth, and I is the interference power (if interference is present) in the receiver after the receive filtering.

"Coverage" requires that the receive power C/N be greater than a minimum criterion related to the quality of service. For voice systems, the quality of service is specified in terms of DAQ (1.0= lowest voice quality; 4.0 = highest). For data systems, the coverage criterion is usually

[29] Proakis, "Digital Communications", McGraw Hill, 2001, p316

specified in terms of a maximum bit error rate requirement[30]. TSB-88[31] gives minimum values of C/N for achieving various DAQ voice quality criteria as well as bit error rate.

Data rate dependence is introduced into equation 3 by writing the C/N in terms of the data rate R (bits per second) and the commonly used parameter E_b/N_0 that is a fundamental constant for the type of modulation and required bit error rate.

$$C/N = (E_b/N_0)(R/B) \quad (4)$$

Substituting equation (4) into (3) and solving for d gives

$$d = \sqrt{\frac{KP_t}{R(N_0 + I/B)}} \quad (5)$$

Where

$$K = \frac{G_t G_r \lambda^2}{(4\pi)^2 (E_b/N_0)} \quad (6)$$

In cases where there are several interference sources transmitting simultaneously with the desired signal, the interference I in equation 4 is the power summation of all sources as follows:

$$I = \sum_{j=1}^{N} I_j \quad (7)$$

Where

N= total number of interference sources

I_j = Interference received from the jth interference source

TSB-88[32] defines a variable ACPR that represents the attenuation, by the filtering performed in the receiver, of the total interference power that is received. ACPR is dependent on the modulation of the interference, frequency offset of the interference from the desired signal, and the characteristics of the receiver filtering. Also, this reference discusses a methodology for estimating the effect of the interference on the desired signal. In essence, the methodology relates the interference power received by the radio to the total interference power at the receiver input P_i and the ACPR value. Using equation 1 to estimate the received signal from the interference, we have:

[30] Bit error rate is the probability of misinterpreting a one as a zero or vice versa. It is also related to C/N in that it decreases as C/N increases.
[31] Reference for TSB-88
[32] TSB-88 reference

$$I_j = ACPR_j \frac{K_j P_j}{d_j^2} \quad (8)$$

Where

$$K_j = \frac{G_j G_r \lambda^2}{(4\pi)^2} \quad (9)$$

And

$ACPR_j$ = adjacent channel power ratio for interference source j

G_j= Transmit antenna gain for interference j

P_j= Transmit power for interference j

d_j = distance between the receiver and the interference source j transmitter

Substituting equations (8) and (7) into (5) and introducing a margin (i.e., confidence) factor M gives

$$d = M \sqrt{\frac{KP_t}{R[N_0 + \sum_{j=1}^{N} (ACPR_j \frac{K_j P_j}{B d_j^2})]}} \quad (10)$$

M = margin factor (less than 1) to account for fading and required confidence level of the estimate

where

d= distance of the receiver from the desired transmitter

di= distance of the receiver from the undesired (interference) transmitter

K and K_j = fixed system constants for the desired signal transmitter/receiver and the interference signal respectively (K is inversely proportional to the required signal to noise ratio for achieving the coverage criterion)

N_0 = receiver noise spectral density (fixed)

Pt = transmit power for the desired signal transmitter

Pj= transmit power for the undesired (interference) transmitter

B= receiver bandwidth

$ACPR_j$=adjacent channel power ratio for interference source j (the amount of energy spillover from the carrier into the adjacent channel)