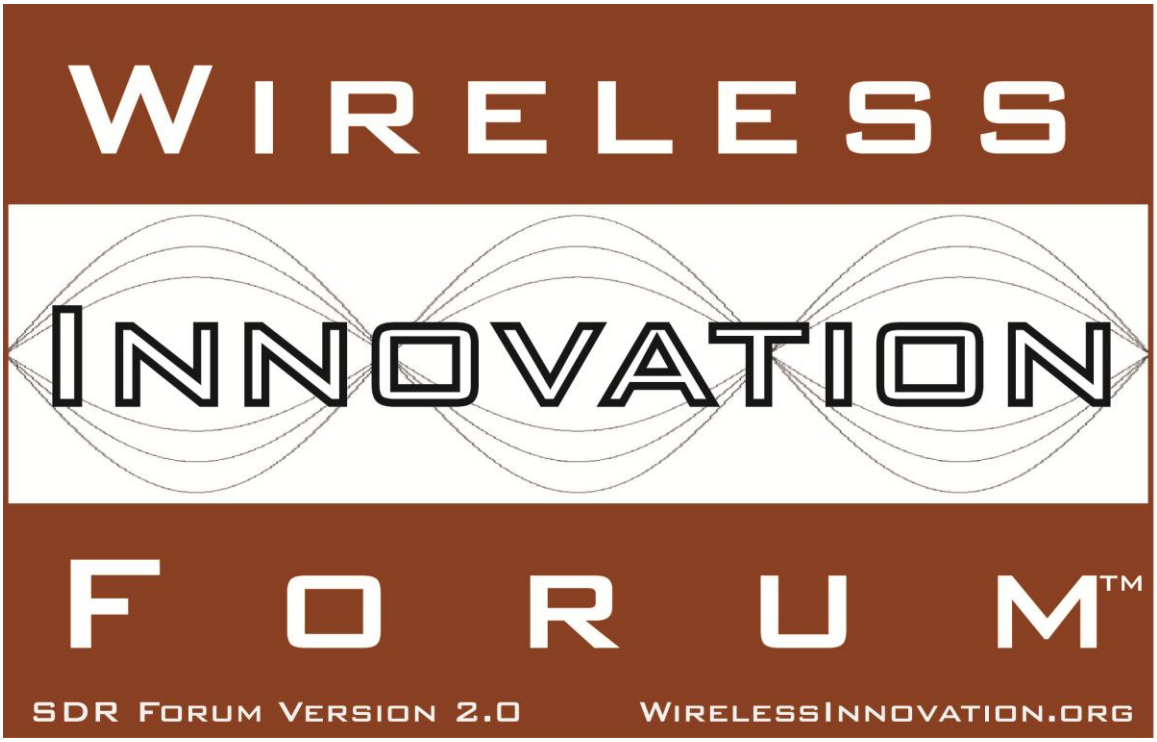

Comments on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network

Document WINNF-11-R-0017

Version V1.0.0

11 October 2011

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Public Safety Special Interest Group to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Public Safety Special Interest Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

Executive Summary

The Wireless Innovation Forum has been active for sixteen years supporting the development and deployment of advanced wireless technology, and for over seven years has specifically targeted public safety as an important domain for such technology. The Forum welcomes the progress in the United States in defining a National Public Safety Broadband Network, as enhanced digital information supports the importance of robust, reliable wireless communication is a cornerstone of effective public safety.

Many of the concepts defined in the Request for Comment (RfC) published by the National Institute of Standards and Technology (NIST) align closely with concepts and technologies that have evolved in the deliberations and publications of the Forum. Our response is intended to:

- Highlight the importance of the proposed features to public safety based on extensive scenario-based analysis;
- Identify specific capabilities and functionalities needed to realize the high-level features proposed in the RfC;
- Identify operational and regulatory considerations associated with the features;
- Identify additional capabilities that would further enhance the capabilities and utility of the National Public Safety Broadband Network.
- Provide specific references to Public Safety communication issues in publicly available publications of the Forum.

The Wireless Innovation Forum has worked to identify the potential impact of advanced wireless technologies on public safety communications. The U.S. National Public Safety Broadband Network can benefit from the concepts and capabilities identified by the Forum. Our response to this RfC provides a mapping of the Forum's work to the specific questions posed in the RfC, and provides detailed discussions of the topics and issues identified by NIST.

Comments on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network

1 Overview

The Wireless Innovation Forum has been active for sixteen years supporting the development and deployment of advanced wireless technology, and for over seven years has specifically targeted public safety as an important domain for such technology. The Forum welcomes the progress in the United States in defining a National Public Safety Broadband Network, as enhanced digital information supports the importance of robust, reliable wireless communication is a cornerstone of effective public safety.

Many of the concepts defined in the Request for Comment (RfC) published by the National Institute of Standards and Technology (NIST) align closely with concepts and technologies that have evolved in the deliberations and publications of the Forum. Our response is intended to:

- Highlight the importance of the proposed features to public safety based on extensive scenario-based analysis;
- Identify specific capabilities and functionalities needed to realize the high-level features proposed in the RfC;
- Identify operational and regulatory considerations associated with the features;
- Identify additional capabilities that would further enhance the capabilities and utility of the National Public Safety Broadband Network.
- Provide specific references to Public Safety communication issues in publicly available publications of the Forum.

The remainder of this overview presents a brief introduction to the Forum and the projects and documents relevant to the RfC. In Section 2, we provide a mapping of desirable features defined in the RfC and use cases generated by the Forum that highlight the impact and challenges of implementing those features. While we have referenced the full use case documents, we have included the specific use case write-ups as appendixes as those write ups contain the information about desired features requested in the RfC. In Section 3 we include similar mappings to "challenges" that were defined in two reports that the Forum previously published on the topic of a public/private shared network for public safety. In Section 4, we have included answers to additional questions in the RfC.

The Wireless Innovation Forum (WInnF) is an open, non-profit mutual benefit corporation dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems, with a mission to accelerate the proliferation of advanced

communications 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 technologies, to include working in liaison with other organizations to ensure that Forum recommendations are easily adapted to existing standards and evolving wireless systems
- Cooperatively addressing the global regulatory environment
- Providing a common ground to codify global developments,
- Serving as an industry meeting place

The Public Safety Special Interest Group (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 advanced communications technology within a particular domain or market area. Goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise awareness of key technologies, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the WInnF. 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, manufacturers of advanced communications technologies for military applications, software developers, researchers, and regulators.

Our response references two use case documents which the Forum published as the result of project to determine how advanced wireless technology such as software defined radio, reconfigurable radios, and cognitive radios could enhance public safety communications. In each case, a detailed scenario was analyzed with respect to the communications capabilities available to responders to determine how advanced technologies could have impacted the response. These reports include:

- **Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground**
  SDRF-07-P-0019-V1.0.0[1] (Nov. 8, 2007)
- **Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2--Chemical Plant Explosion Scenario**
  WINNF-09-P-0015-V1.0.0[2] (Jan. 26, 2010)

When the concept of a shared public/private wireless network as a basis for a nationwide public safety network was first introduced, the Forum also published two reports that highlighted the challenges in implementing such a network and the advanced technologies that could address the

[1] *available at* http://groups.winnforum.org/d/do/1565
[2] *available at* http://groups.winnforum.org/d/do/2325

challenges. While the business models currently under consideration are different, the technologies and challenges are relevant to the National Public Safety Broadband Network. The second report (the Utilization Report), built on the work of the initial report, and the challenges from the Utilization Report are included in this response as appendices.

- **Considerations and Recommendations for Software Defined Radio Technologies for the 700 MHz Public/Private Partnership**
  SDRF-07-R-0024-V1.0.0 (Recommendations Report, December 5, 2007)[3]

- **Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership**
  SDRF-08-P-0004-V1.0.0 (Utilization Report, June 18, 2008)[4]

The Modeling Language for Mobility (MLM) Work Group has developed three documents that provide relevant background to the RfC:

- **Use Cases for MLM Language in Modern Wireless Networks**
  SDRF-08-P-0009-V1.0.0 (June 1, 2002)[5]

- **Description of the Cognitive Radio Ontology**,
  WINNF-10-S-0007, Version V1.0.0 (September 30, 2010)[6]

- **Description of the Cognitive Radio Ontology**,
  WINNF-10-S-0007, Version V1.0.0, (September 30, 2010, with associated Ontology provided in OWL)[7]

The first document includes four use cases that are based on the use cases of the Public Safety SIG. The second referenced document contains the description of the ontology (called there the Cognitive Radio Ontology (CRO). The third document contains the representation of the ontology in the declarative language called the Web Ontology Language (OWL).[8]

[3] Available at http://groups.winnforum.org/d/do/1579
[4] Available at http://groups.winnforum.org/d/do/1564
[5] Available at http://groups.winnforum.org/d/do/1562
[6] Available at http://groups.winnforum.org/d/do/3370
[7] Available at http://groups.winnforum.org/d/do/4441
[8] *See also* Wireless Innovation Forum Comments to FCC in ET Docket No. 10-237, "In the Matter of Promoting More Efficient Use of Spectrum Through Dynamic Spectrum Use Technologies," (Feb. 28, 2011) *available at* http://groups.winnforum.org/d/do/4397; Wireless Innovation Forum Comments to FCC in GN Docket Nos. 09-51 and 09-157, "In the Matter of Fostering Innovation and Investment in the Wireless Communications Market; A National Broadband Plan for the Commission's Future," (Sept. 30, 2009), *available at* http://groups.winnforum.org/d/do/1575.

2 Mapping of Feature List to Use Case Documents

The RfC identifies a number of desirable features of a National Public Safety Broadband Network. In this section, we highlight work done within the Forum to assess the potential of advanced communications techniques in the context of specific scenarios. The use cases are included as an appendix to this document, and within each use case (described in Table 1) discussion, there is information specific to the following NIST questions:

- **Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network.** The importance of the feature is defined in the context of the scenario and the use case that shows how the capability could impact the first responder communications capabilities. The use cases for the Chemical Plant Scenario specifically include a section on impact.

- **Current gaps that exist preventing the realization of the full potential of the feature:** The use case discussion includes a discussion of capability shortfalls.

- **Possible research and development that could take place to close any technical gaps:** The summary of capabilities outlines what we propose as an ideal capability, and the ultimate goal of research to address the capability gaps.

- **Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:** Operational and regulatory implications are discussed in each use case.

- **Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.** The use cases do not specifically address best practices from other industries.

Metalanguage for Mobility (MLM) Use Case

The main objective of the MLM use cases was to show how the objectives of the Public Safety use cases can be achieved through use of a declarative language (MLM). MLM is based on an ontology (terminology that includes concepts, relationships and instances) and allows for expressing policies that define how a communication device should react to various types of events. Once an ontology and policies are defined, then the policies can be executed by the computing device of the communication node and thus imposing the behavior on the nodes that is specified in the policies.

To demonstrate the feasibility of using the cognitive radio ontology (CRO) and policies to control communication nodes, VIStology, Inc. and Northeastern University have developed a demonstration in which two radios, implemented on the GNU Radio platform, used the CRO and policies to exchange information about their communications environment and their internal states and use policies to react to the messages. This demonstration was presented at the 2010 Software Defined Radio Technical Conference, sponsored by the WInnF, in December of 2010. In this demonstration, two cognitive radios were shown to adaptively control their transmit power in order to improve their performance, or quality of service (QoS), defined in terms of a relation between the transmit power and the mSNR. The results of this demonstration can be found in: S. Li, J. Moskal, M. M. Kokar, and D. Brady. An implementation of collaborative adaptation of cognitive radio parameters using an ontology and policy based approach. *Analog Integrated Circuits and Signal Processing*, DOI: 10.1007/s10470-011-9681-y:1-14, 2011.

Table 1, List of Use Cases

Use Case	Description
London Bombing Scenario (see Appendix Section 6)	
1	Network Extension for Coverage and Reachback
2	Dynamically Access Additional Spectrum
3	Temporarily Reconfigure First Responder Communication Device Priorities
4	Interface to Non-First Responders
Chemical Plant Use Cases (see Appendix Section 7)	
1	Role-Based Reconfiguration
2	Resource Management in a Dedicated Public Safety Network
3	Resource Management in a Shared Public/Private Network
4	Coverage Performance Improvement
5	Reconfigurable RF Gateway Capability
6	Interface with non-first responders
7	Revert to Previous State
8	Cognitive Sensor Network
Metalanguage for Mobility	
MLM	Radio Management (**see sidebar above**)

Table 2 provides a mapping of the use cases to the desirable features listed in the NIST RfC. The actual use cases are included as an appendix.

Table 2, Mapping of Desirable Features to Use Cases

Feature	London Bombing Use Cases				Chemical Plant Scenario Use Case								
	1	2	3	4	1	2	3	4	5	6	7	8	MLM
To ensure resiliency													
Resiliency	X							X			X		X
Self-Organizing	X							X					
Meshing	X												
Adaptability	X	X			X		X						X
To ensure reliability and availability:													
Prioritization			X			X	X	X					
Quality of Service (QoS)			X			X	X						X
To enable security:													
Strong, Dynamic Access Control						X				X		X	
To ensure affordability/commercial alignment:													
Compatibility with Commercial Infrastructure				X		X	X		X			X	
Network sharing		X		X		X	X		X			X	
Multi-Modal					X							X	
Scalability		X			X	X	X						
Power Awareness								X					X
Standardized Common Interfaces					X								
Uniform, Universal Access													

3 Mapping of Feature List to Challenges

The Forum generated two reports that highlighted the challenges in implementing a national broadband wireless network a network and the advanced technologies that could address the challenges. The discussion of the challenges from the more recent report are included as an appendix to this document, and within each challenge (described in Table 3) discussion, there is information specific to the following NIST questions:

- **Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network.** The importance of the feature is defined in the context of a challenge to develop a nationwide wireless broadband network for public safety.

- **Current gaps that exist preventing the realization of the full potential of the feature:** The challenge discussion includes a discussion of capability shortfalls.

- **Possible research and development that could take place to close any technical gaps:** The challenge discussion outlines advanced wireless technologies that could address the capability shortfalls.

- **Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions:** Operational and regulatory implications are discussed for each challenge.

- **Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.** The use cases do not specifically address best practices from other industries.

Table 3, List of Challenges

Challenge	Description
Utilization Document (see Appendix Section 8)	
1	Creating a Commercially Viable Network that Meets Public Safety Needs
2	Evolving over Time
3	Supporting Unique Public Safety Requirements
4	Interoperability with other 700 MHz Networks
5	Cost and Usability

Table 4 provides a mapping of the use cases to the desirable features listed in the NIST RfC. The actual challenges are included as an appendix.

Table 4, Mapping of Desirable Features to Nationwide Broadband Challenges

Feature	Utilization Challenge				
	1	2	3	4	5
Resiliency			X		
Self-Organizing					
Meshing					
Adaptability	X	X			
Prioritization	X		X		
Quality of Service (QoS)	X		X		
Strong, Dynamic Access Control					
Compatibility with Commercial Infrastructure				X	
Network sharing					
Multi-Modal					
Scalability		X			
Power Awareness	X				
Standardized Common Interfaces					
Uniform, Universal Access					

4 Additional Questions

The RfC also included additional questions; we have listed those question for which the Forum's work provides input.

What is the importance of employing open standards for the nationwide public safety network?

- Open standards are key to achieving the other goals of commonality of functions, facilitation of a multi-vendor environment, and affordability. Proprietary functionality (not including individuals applications) that is outside the standard tends to create non-interoperable capabilities; non-standard functionality needs to be available to all developers (open source architecture)

What can be done to ensure both short- and long-term affordability of the network for all types of public safety agencies?

- The Utilization Report Challenge 5 (see Appendix Section 8.5) addresses how SDR/CR technology addresses cost and usability issues in a national broadband network.

What network features or requirements have not been identified above, the lack of which may impair the network's ability to adequately serve the needs of public safety?

- Capabilities that support role-based responder access and resource management.
  - Explicit definition of user roles within an incident response structure (see Appendix Section 7.1).
  - Electronic storage of a user's credentials.
  - Ability to authenticate a user as qualified for a specific role.

  - Definition of appropriate radio capabilities as associated with a user's role.

- Capabilities that improve dynamic spectrum management.
  - Decision making based on knowledge of the RF environment, which in turn requires that the individual radios provide some information about the RF environment at their location.
  - Geolocation.
  - Capability to release use of spectrum by public safety users as the emergency communications requirements decline.

- The ability to establish and manage network operations policies

- Ability to query radios for information including, but not be limited to, vendor, radio type, available modes, version numbers, reconfigurability, etc.

- Interface to legacy systems (LMR, paging, legacy data systems) and a transition roadmap.

- Ability to refresh technology at "commercial pace" while maintaining compatibility with all users of the system, in an environment where not all users will update simultaneously.

- Ability to restore conditions to pre-incident conditions or previously known state.

- Ability to interface to and manage data from sensors.

- Ability of subnets to communicate when disconnected from the primary system, and synchronize when connection re-established.

- Interaction of QoS, security, trust, and authentication management in a dynamic environment.

- Mission critical voice functional capabilities as defined in the National Public Safety Telecommunications Council Broadband Working Group (NPSTC BBWG) document entitled "Mission Critical Voice Communications Requirements for Public Safety"[9].

How should NIST engage public safety practitioners and technologists as part of the planned R&D projects to ensure proper prioritization of efforts and effectiveness of developed solutions?

The Forum encourages NIST to continue to solicit input from technology-oriented organizations such as the Wireless Innovation Forum to provide ideas on both short-term and long-term technology solutions to the challenges of implementing and operating the National Public Safety Broadband Network; public safety users need the most effective, reliable, and affordable communications capability that the technology community can provide.

[9] http://www.npstc.org/broadband.jsp.

5 Summary

The Wireless Innovation Forum has worked to identify the potential impact of advanced wireless technologies on public safety communications. The U.S. National Public Safety Broadband Network can benefit from the concepts and capabilities identified by the Forum. Our response to this RfC provides a mapping of the Forum's work to the specific questions posed in the RfC, and provides detailed discussions of the topics and issues identified by NIST.

6 Appendix: London Bombing Use Cases

A number of potential cognitive use cases have been identified based on the scenario timeline as described in the preceding section. In this section, each use case is discussed in much greater detail. The use cases are ordered in descending priority based on operational relevance and feasibility as provided by the public safety practitioners who provided input to and feedback on the report.

6.1 Use Case 1: Network Extension for Coverage and Reachback

Cognitive radio capabilities could be used to automatically reconfigure radios to include a repeater capability to extend network coverage to areas where radios are otherwise cut off from their infrastructure, particularly during initial response to an incident prior to additional communications resources being deployed.

6.1.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** Bombs exploded on three London Underground trains inside tunnels with varying distances to the nearest station. Some passengers were severely wounded. There was no light. The only escape was by walking through the tunnel to the nearest station. Responders had to walk to the scene through the tunnel.

   A number of different agencies, including Metropolitan Police, British Transport Police, the London Fire Brigade, and London Ambulance responded to the emergency by entering tunnels through the nearest station.

2. **Network**: Once police and fire responders went into the tunnels, their radios lost connectivity to the above-ground infrastructure. The only means for responders to communicate back to their respective command centers and any above ground personnel was to walk to the nearest station and position themselves at the entrance to the Metro system. Individual radios were not capable of exploiting peer-to-peer capabilities to provide network extension to connect isolated nodes to the network.

3. **Procedural**: Responders had adequate authority to communicate on their own networks, but as noted under Network were unable to do so. Procedures were established to maintain some flow of information by having responders communicate to (above ground) command centers from the entrance to the tunnels, but that process required responders to walk from the scene to the entrance, which took as long as 15 minutes in some cases.

4. **Regulatory:** No regulatory issues were involved as the situation reflected an inability to communicate on licensed frequencies due to physical constraints.

5. **Chronological:** Prior planning had been performed, but infrastructure damage precluded the use of some communications capabilities that were in place and part of the plan.

The other critical chronological consideration is the amount of time (as much as 15 minutes) required to move information from the scene of the accident underground to the command centers.

6.1.2 Description of Use Case

Cognitive radio technology could be implemented to reconfigure responders' radios to create an extension to the existing network. This network extension 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 would be positioned where it could maintain connectivity with the above-ground infrastructure (such as at an opening to the tunnel) and function as a repeater to bridge between the otherwise disconnected radios and the infrastructure. Depending on distribution of radios in the tunnels, additional radios could also be automatically reconfigured to act as repeaters among the disconnected radios.

The concept is illustrated in Figure 6-1. As shown, communications is enabled between personnel at the opening of the tunnel to dispatch and emergency management centers, but not from responders at the scene of the explosion in the tunnels. The concept of the network extension capability is reflected in the additional links that could be established automatically among responders otherwise cut off from communication with the above-ground system. This provides immediate restoration of communications for all users without requiring additional equipment at the scene.

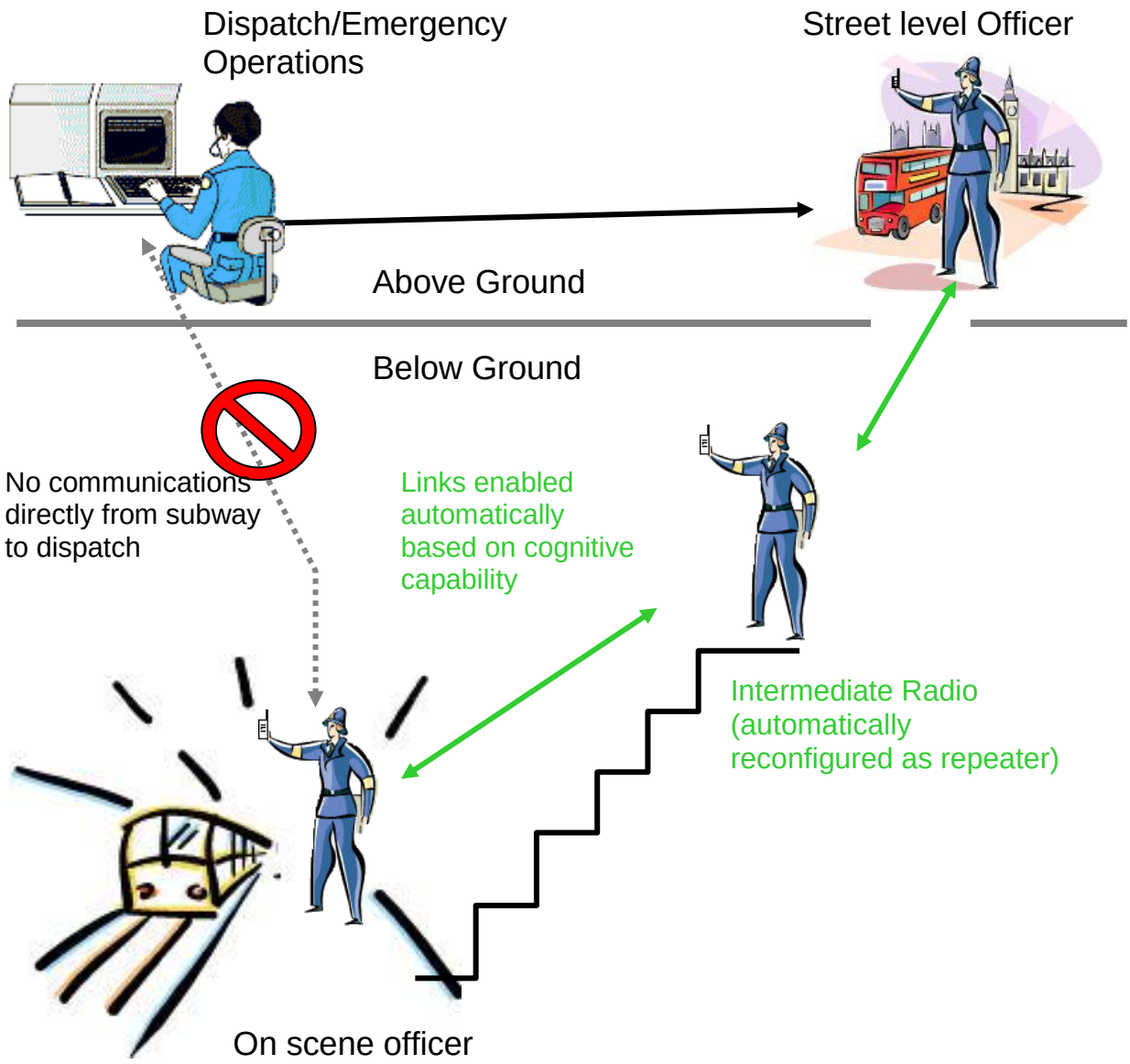

Figure 6-1. Network Coverage Extension Use Case Example

The impact of these capabilities is that on-scene responders would have direct communications to command centers without leaving the incident scene or resorting to runners that delayed communications by as much as 15 minutes. With respect to the specific aspects of the scenario situation noted in Section 4.3.1.1, this use case would result in the following:

1. **Physical**: No change from the physical situation described above.
2. **Network**: Responders would maintain connectivity with their network at all times regardless of where they were located. (Note that it would be possible to achieve the same effect by deploying repeaters at strategic locations to create the necessary extension. However, the cognitive capability has significant advantages that justify this use case:

a. Cognitive capabilities and the ability to reconfigure radios would provide the network extension immediately, rather than after the period of time necessary to deploy repeaters.

b. Cognitive capabilities would automatically determine appropriate network configuration. Repeaters would require manual determination of the repeater location, frequencies, and so on.

c. Cognitive capabilities would allow the network extension to accommodate the dynamics of the response, as users arrive and leave, as the physical location of the responders changes, and so on.

3. **Procedural**: In general the procedures normally used for communications among responders and between the responders and the above ground command centers would be followed in this situation. Additional procedures would be followed to position radios as needed to function as repeaters to ensure connectivity. However, unless the radios acting as repeaters have a full duplex capability, the responders must allow for a variable time lag for their message to be received and stored and then re-transmitted at each repeater and for an appropriate response back from the other party(ies) involved in the communications.

4. **Regulatory**: No significant regulatory change would be required as this capability assumes operation on existing licensed frequencies, however regulatory approval of operating mode changes would be required. See Section 4.3.1.4.

5. **Chronological**: The pre-planning would still be effective as network connectivity would be maintained despite infrastructure damage or the response by responders whose radio system was not normally extended into the tunnels. In addition, the timelines to move information from the scene to the command centers could be reduced from as much 15 minutes to a few seconds.

6.1.3 Functional Capabilities

There are a number of functional capabilities assumed by this cognitive use case. First, the radios must be capable of being reconfigured to function as a network extension (e.g., the radios can operate on appropriate spectrum; the radios have reconfiguration algorithms, and so on). Second, there must be some level of cognitive capability for a collection of radios to "understand" that they have lost their ability to communicate with the system infrastructure. More specifically, radios must be capable of:

- Determining that they are disconnected from the system infrastructure;
- Finding and identifying peer radios;
- Identifying and authenticating reconfigurable compatible radios;
- Determining which radio/radios is/are within coverage of the infrastructure and which radios are not within the coverage of the infrastructure;
- Forming a satisfactory network extension route to the infrastructure from each affected radio using non-interfering frequencies for each "hop";

- Adjusting the network as responders arrive and depart from the area where coverage is unavailable; and
- Preserving the level of security of the baseline network in the network extensions.
- Providing either full duplex (simultaneous receive and transmit) operation or including a "store and forward" capability for user voice and/or data communications.

There are a number of approaches that could be utilized to achieve the network extension, such as ad hoc or mesh networks. The feasibility of existing protocols to accomplish this is a relevant research topic.

6.1.4 Regulatory Implications

The proposed capability would rely on existing peer-to-peer modes of operation for which regulatory rules are already in place. Thus no major regulatory changes are required (although air interface could change from being used in simplex mode to semi-duplex or duplex mode.) However, it is possible that the spectrum and protocols required to implement such a capability would require the ability to utilize spectrum not routinely licensed to such users under current regulatory rules. Thus it may be necessary to consider allowing use of spectrum for such purposes. Part of the cognitive capability of identifying the disconnection from system infrastructure could be to ensure that spectrum used for peer-to-peer communication would not interfere with other users. In the case of the tunnel bombing, such interference would be unlikely because the area in question is generally cut off from most above-ground infrastructure. However, to generalize this use case to other situations in addition to the tunnel scenario, channel assignments should be made on approved frequencies.

6.1.5 Policy Implications

As noted above, the objective of this use case is to seamlessly restore lost connectivity of responders who have already been authorized and authenticated to use the network. Ideally responders would be unaware of the reconfiguration of radios, although an audio or visual alert should be included to indicate that the radio is following the network extension protocols. Policies governing use of the network (e.g., who may use the network, radio protocols, use of channel) would be the same for the network extension as when the radio is within range of the infrastructure.

Some procedures will need to be modified or added to reflect that some radio behavior, such as the rebroadcast of voice transmissions, may be evident to the responders because of response delays. Training will be generated to be appropriate so that users will be familiar with the differences in radio performance and behavior. In addition, training will be established for responders to understand the impact of physical location and how best to deploy, particularly if they were going to carry a radio that can be reconfigured as a repeater. Consideration should also be given to allowing individual first responders the option of excluding their radio from participating in the network (see discussion in Section 5.2).

Network management policies (e.g., machine readable policies) that govern the manner in which radios are reconfigured to achieve network extension will need to be implemented in advance to facilitate such operations. However the impact on usage behavior should be minimal.

Some training will also be needed to fully exploit such capabilities. For example, responders would need to understand how the radios respond when outside network coverage. Users should be familiar with performance aspects of the radios such as changes in delay times, capabilities and performance of the radio when acting as a repeater, the impact of physical location of the radios on network performance, and similar information.

Policies and procedures will need to be established for operation of radios that end up being used as repeaters. For example, a responder whose radio is used as a repeater may need to stay in a specific physical location and "man" the position to maintain the communication link, and may not be able to participate in other functions of the response. Agencies will need to consider the tradeoffs of how to allocate responders accordingly. Procedures may also be established for responders "dropping off" radios as needed to allow the network extension to function (here again the issue is how best to allocate resources, with the radio and the responder being considered separate resources). Given the proposed capabilities of the radios, spare or cache radios which can be rapidly delivered to the scene may also be part of an incident response strategy.

6.2 Use Case 2: Dynamically Access Additional Spectrum

At several points in the scenario there were communications difficulties because of the sheer volume of calls on the voice communications networks. Dynamic spectrum access, or the ability for cognitive radios to identify unused or underutilized spectrum, could be a solution in this scenario and provide a means for expanding capacity when needed.

We understand that there are significant technical issues associated with implementation of this use case that are dependent on the technology used in the system infrastructure. The focus of this discussion is the overall desirability and benefit to public safety of being able to expand capacity in emergency situations in a timely manner.

Note, however, that most dynamic spectrum access approaches assume that the user is operating as a secondary user, and able to relocate to other spectrum as needed if a primary user utilizes the spectrum. This use case in this scenario would be significantly different—in an emergency situation, dynamic spectrum access for responders would be as a primary user—to specifically appropriate spectrum that is not being used, or can be appropriated for emergency use.

6.2.1.1 Summary of Scenario Situation

In terms of the aspects of public safety communications:

1. **Physical:** In the process of responding to the situation, the density of radios and access attempts overloaded some infrastructure elements in a specific geographic area. Key considerations include that the scenario took place in a densely populated urban area during a workday. In addition, multiple incident locations created demand for services that impacted the system as a whole.

2. **Network:** Based on the demand exceeding capacity, access control mechanisms (ACCOLC) were invoked in the area around Aldgate East to block access for some users, including first responders that did not have priority access.
3. **Procedural:** A significant decision process was executed to determine whether or not to invoke Access Overload Control (ACCOLC)[10] when the mobile phone system could not handle the number of attempted calls. Part of the decision process was assessment of the impact of ACCOLC on responders who were supporting the response but whose radios did not have priority.
4. **Regulatory:** No regulatory procedures existed for dynamic allocation and use of spectrum outside the previously licensed frequencies.
5. **Chronological:** The ACCOLC decision process occurred as the response to the bombing events was unfolding.

6.2.2 Description of the Use Case

This use case involves identifying and utilizing spectrum not normally utilized by the system—in this case the mobile phone system.

There are three different approaches that can be considered to realize this use case, as outlined (underlined) below:

Pre-defined agreement among organizations: One approach to dynamic spectrum access, taking advantage of reconfigurable radios/cell phones, is to establish agreements among organizations that would allow a non-licensed authorized user to utilize additional spectrum under defined circumstances and by mutual agreement. Implementation of this cognitive capability may be limited to the ability to identify the channel loading limits that would require accessing additional spectrum. The cognitive capability may also be used to manage network and subscriber reconfiguration to enhance the utilization of the allocated spectrum. There is a broad range of potential types of agreements under which spectrum could be dynamically accessed. The following is by no means conclusive but serves to provide a range of possibilities:

- Dynamic spectrum access that is triggered by a pre-defined event, such as reaching a capacity limit;
- Dynamic spectrum access that occurs when one organization requests access and the licensed organization grants it (e.g., spectrum mutual aid).
- Dynamic spectrum access granted to another user (spectrum leasing) or to a secondary user on a non-interfering basis.

Emergency declaration: Another approach to dynamic spectrum access, again requiring the ability to reconfigure radios/cell phones is to establish rules by which some spectrum (licensed

[10] We recognize that the increasing deployment of Airwave (a dedicated public safety communications system) into the police and fire services is reducing the use of public networks by first responders, and therefore reducing the chances of a recurrence of the specific circumstances under which ACCOLC was invoked in this scenario. Nevertheless, this scenario highlights the general challenge of obtaining adequate capacity for first responder communications in an escalating event, for which dynamic spectrum access is an important use case for cognitive radio capabilities.

for other services) is accessed for emergency response under a governmental declaration. Here again the cognitive capability may be limited to identifying the load circumstances under which access of additional spectrum is appropriate, or may be used to manage network and subscriber reconfiguration to enhance spectrum utilization.

Identify unused or underutilized spectrum not licensed to the network: Another approach to dynamic spectrum access is to monitor spectrum utilization in frequencies not licensed to the network, identify spectrum which is unused or underutilized ("white space"), and reconfigure the network and subscriber equipment to utilize that spectrum. Clearly this type of dynamic spectrum access would be limited to emergency situations and only be allowed under clearly defined circumstances (such as a governmental declaration). Cognitive capabilities would be required to identify available spectrum and to reconfigure the network and subscribers accordingly.

1. **Physical**: No change from the physical situation described above.
2. **Network:** In this scenario, the network congestion would be relieved by providing more spectrum for use by all network users including first responders. If the infrastructure has a cellular architecture, it may be possible to dynamically reallocate the channel distribution to create additional capacity in the afflicted cells. Alternately, there may be a place in nearby spectrum where some other service can be pre-empted to satisfy the demand.
3. **Procedural:** There are a number of procedural decisions involved in implementing this use case. Key procedures include determining at what point to invoke dynamic spectrum access procedures, procedures for identifying spectrum that can be utilized, and when to release the bandwidth. The specific procedural implications are a function of the implementation approach. For example, this use case could be based on a fully automated determination of the need for additional spectrum and the spectrum to be utilized; in other implementations there may be a human in the decision loop, in which case the procedures for making such a decision must be defined. Also, different procedures may be appropriate depending on whether the additional spectrum is based on a pre-defined procedure or agreement, or whether additional spectrum is identified in real-time during the course of an incident.
4. **Regulatory:** The regulatory implications of dynamically accessing spectrum depend on the approach (as outlined above) that is used. Some pre-defined agreements among organizations may be feasible under existing regulatory rules, particularly if the spectrum is allocated under the same service rules or if the rules explicitly provide for secondary spectrum usage. Rules may require modification if the dynamically allocated spectrum is normally allocated under different service rules, or if there is no explicit allowance for such agreements to be put in place. In general the approach that allows spectrum to be accessed for emergency response is not embodied in existing regulations and would need to be added to allow this approach. Likewise, the ability to identify and access unused or underutilized spectrum not licensed to the network is not generally part of existing regulations. We recognize that these regulatory changes can involve sweeping changes to how spectrum is utilized in emergency situations, and that crafting rules which balance the needs of emergency response and other legitimate uses of spectrum during emergencies will require extensive research, development, and public discussion.

5. **Chronological:** This kind of Spectrum Sharing would require a significant amount of advanced detailed planning. Plans can have varying degrees of dynamic range. Switching from one fixed plan to another is easier than dynamic cognitive problem solving in real time, but more likely would result in less efficient spectrum utilization. Also note that relinquishing spectrum that has been utilized to facilitate emergency response must be done in a timely manner to have value greater than present systems.

6.2.3 Functional Capabilities

Dynamic spectrum access implies a number of functional capabilities, as described below.

- The network must be able to identify capacity loading that meets whatever criteria are in place to initiate the dynamic spectrum access.
- The network must be capable of identifying spectrum resources that can be utilized to offload some calls. There are two possible approaches to identifying additional spectrum.
    - First, there may be established agreements in place that under certain circumstances spectrum normally used for one purpose is made available to support communications networks being utilized in an emergency. Such identification could be based on established agreements among spectrum "owners" or based on allocation of spectrum for emergency use in the event of a certain level of emergency.
    - Alternatively, cognitive capabilities to search for underutilized spectrum ("white space") that could be dynamically accessed. Note that in this case a scheme must be implemented to manage the hidden node problem. Also, the network must be able to support the ability to deconflict the situation if multiple users attempt to access the same available spectrum "white space".
- The network infrastructure must be able to reconfigure to use the new spectrum. If the system is a trunked system, the network must be able to incorporate additional frequency options into the system. Network transmitters and receivers must be able to be reconfigured to utilize the additional spectrum. If the additional spectrum is based on a pre-defined agreement, frequencies may be pre-programmed, in which case only an execution command is required to access the additional spectrum.
- Subscriber equipment must be able to reconfigure to use the new spectrum, i.e., must be able to transmit and receive on the additional frequencies.
- Reconfiguration information must be communicated among the radios and the network infrastructure to coordinate the utilization of additional spectrum.
- Dynamic access of spectrum must be consistent with the regulatory requirements of that spectrum (e.g., in terms of bandwidth, out of band emissions, power management, location based rules) to ensure that other users in that service are not adversely impacted by use of a specific frequency.

6.2.4 Regulatory Implications

The regulatory implications of this use case depend largely on the manner in which spectrum is dynamically accessed.

Approaches based on pre-defined agreements among organizations that allow users to utilize spectrum in emergency situations may require regulatory approval to allow secondary use (secondary markets, leased spectrum, etc.) of spectrum by non-licensed users.

One potential regulatory change is to allocate spectrum for first responder use that is otherwise allocated for other non-public safety use during normal conditions (e.g., executive declaration of an emergency automatically dynamically allocates certain commercial use spectrum for emergency responder utilization).

Use of licensed spectrum without pre-arrangements is generally not allowed and would require changes to existing regulations. Use of unlicensed spectrum is generally allowable, although regulatory changes could recognize public safety priority use of unlicensed spectrum in emergency situations (just as drivers yield the right of way to emergency vehicles with lights and sirens).

6.2.5 Policy Implications

There are a number of policy implications for this use case. Key questions include:

- What are the circumstances under which spectrum can be allocated as described above?
- Who has the authority under which a decision to utilize non-licensed spectrum is made?
- What is the interaction of priority services and dynamically allocated spectrum?
- When and how is dynamically allocated spectrum released?

6.3 Use Case 3: Temporarily Reconfigure First Responder Communication Device Priorities

Cognitive radios (in this case, referring to cell phones) might be able to be temporarily reconfigured with higher priorities based on the circumstances of the emergency responder.

6.3.1 Summary of Scenario Situation

In terms of the aspects of public safety communications:

1. **Physical:** In the process of responding to the situation, the density of radios and access attempts overloaded some infrastructure elements in a specific geographic area.
2. **Network:** Mobile phone network resources were being utilized by public users as well as first responders.
3. **Procedural:** A significant decision process was executed to determine whether or not to invoke Access Overload Control (ACCOLC) when the mobile phone system could not handle the number of attempted calls. Part of the decision process was assessment of the

impact of ACCOLC on responders who were supporting the response but whose radios did not have priority.

4. **Regulatory:** No regulatory issues were involved.
5. **Chronological:** The ACCOLC decision process occurred as the response to the bombing events was unfolding.

6.3.2 Description of the Use Case

The dynamic prioritization use case exploits cognitive capabilities to adjust the priorities of responders based on the ongoing communications activity as well as the dynamics of incident response. Priority schemes are implemented in today's public safety and commercial cellular systems. The application of cognitive capabilities provides the opportunity to adjust those priorities to accommodate unanticipated priorities or to manage priority access in real-time.

One of the sources of motivation for this use case comes from one of the major issues that arose in the London bombing scenario. The high demand for cellular calls motivated the Gold Coordinating Group to consider activating the Access Overload Control (ACCOLC) to deny access to the system for any device that did not have the required priority access. One of the considerations in the decision of the Gold Coordinating Group not to invoke ACCOLC was concern that the key responders might not be carrying phones that would allow access were ACCOLC to be invoked.

While the after action reports cited issues surrounding the deliberation to invoke ACCOLC on the day of the bombing, our analysis led to consideration of another use for cognitive capabilities: dynamic priorities. In a crisis situation, as demands for system resources rise, it may become necessary to manage access to the system based on the relative importance of the user and the communication being transmitted. The concept of the use case is to be able to change those priorities in real-time as an event unfolds. In the case of emergency responders using a commercial cell phone network, priority access may be public safety users getting priority access over commercial users in the event of emergency situations. For example, in land mobile radio systems, "man down" alarms get priority over other communications.

While there are differences in typical use of cell phones for incident response between the United Kingdom and locations in other regions such as the United States, this use case is still generally applicable. It is not uncommon for first responders and incident command staff to use cell phones for non-mission critical communications. While not mission-critical, there may still be significant benefit in managing the priorities of such users. Furthermore, although not the focus of this particular discussion, the entire concept of dynamic prioritization based on responder role can be applied to land mobile radio systems as well. Trunking systems today have prioritization capabilities, but they are statically defined.

The role of cognitive capabilities here is in the ability to adjust in real time those priorities based on the unfolding events of the incident, communications resources demands and availability, and the changing roles of individual responders over the course of an event. In the case of the London bombing scenario, a capability that would have enabled responders who did not have ACCOLC-enabled devices (cell phones) would be to have devices reconfigured over-the-air and in real time. This could have eliminated the risk of responders being denied access to the system

in the event that ACCOLC was invoked. These cognitive capabilities could provide more sophisticated and dynamic access management for radio/cellular systems.

The scenario situation would be described as follows:

1. **Physical**: No change from the physical situation described above.
2. **Network:** First responders would be assigned a priority based on their role in support of the response. Priority modifications would be downloaded to the first responders' mobile phones as needed. In addition, cognitive capabilities in the network management would recognize the increasing load level and congestion levels and block access to lower priority calls as needed. User mobile phones would 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.
3. **Procedural:** As discussed in Section 4.3.2.3, there are several approaches to deploying this cognitive use case. Appropriate procedures will be needed, and depend on what particular approach is followed. For example, if individual responders are allowed to change (or request to change) their priority, policies and procedures need to be defined to govern the circumstances and steps to be followed by responders. Likewise, policies and procedures for any request approvals or assignment of priorities as described in the following section will be required.
4. **Regulatory:** Mechanisms for over the air reprovisioning of mobile phones may require regulatory modifications.
5. **Chronological:** Policy and procedures would need to be addressed as part of system planning. During an incident, invocation of access controls would take place upon activation of a set of trigger conditions. When demand no longer exceeds capacity, then the access control mechanisms can be removed, although the normal feedback loop stability criteria must be observed to avoid an on-off-on-off pathology.

6.3.3 Functional Capabilities

A number of capabilities must be available in order to realize this cognitive use case. First, there must be a mechanism to determine those first responders who have a legitimate need to have priority access to the communications network. Access to the network itself has already been established, i.e., the network has already recognized and authenticated the first responder's cell phone (responder's device). The required capability is to establish that the circumstances of that particular user warrant a level of priority greater than the priority level currently granted to the responder's device.

The definition and assignment of priorities can incorporate a number of different elements of incident response and management. For example, priority assignments could be based on:

- The roles within the response that have been assigned to the individual responder's device;
- Physical location of the responder's device;
- Service of the responder's device (e.g., EMS priority over law enforcement);

- Type of data being communicated;
- Role of the user in the communications process.

There is a potentially broad range of complexity and sophistication of the cognitive capabilities implied by this use case. At the simplest level, assuming that priorities can be dynamically modified, radios could be reconfigured either by the individual responder or manually by a network operator without utilizing any cognitive capability. However, manually determining priorities for individual radios is not very practical for large scale incidents. Relatively simple cognitive capabilities[11] could be implemented to associate priorities with responder assignments, physical location, and/or service. More sophisticated cognitive capabilities could assign priorities automatically based on a variety of parameters associated with the communications of the response, or even in a predictive mode to anticipate, rather than react to, the dynamic needs of the responders.

The advantage of role based priorities (supplemented by other ad hoc assignable methods) is that preplanning can determine the appropriate priorities for each role in a variety of situations of varying complexity. Cognitive capabilities might be able to assess the level of complexity involved and select a suitable priority. All of this is supplemented by the user controlled methods delineated as follows.

One approach to considering the different functional capabilities for handling priority assignments is to consider that there are three possibilities for requesting changes in priority—the responder, some central authority (e.g., incident command, incident communications leader), and the communication network itself. Note that in the case of the communications network, the actual functionality could be distributed between the subscriber unit and the network infrastructure, but the request or the authorization is made automatically without human initiative. Each of these entities may also authorize the requested priority change. This leads to nine possible approaches to priority assignment as shown in Table 5.

[11] Relatively simple in this context refers to the notion that the complexity of an algorithm to assign higher priorities to responders in a defined location is low; we recognize that the ability to reconfigure cell phones or other communications devices dynamically is a challenging issue.

Table 5. Possible Dynamic Prioritization Approaches

Requested by \ Authorized by	Individual Responder	Central Authority	Network
Individual Responder	Priority is controlled by individual responder	Individual requests are granted "manually" by central authority, would not require cognitive capabilities.	Cognitive capability to respond to individual request.
Central Authority	Priority changes are initiated by central authority and "accepted" by individual responder.	Central authority makes unilateral decisions regarding individual responder priorities.	Cognitive capabilities in the communications network evaluate requests initiated by central authority
Network	Cognitive capabilities in network "recommend" priority change to individual responder who must "accept" the change.	Cognitive capabilities in network "recommend" priority changes to central authority who must "accept" the change.	Fully automated capability for priority management with no human in the decision loop.

While any of the above approaches is possible, we recognize that not all approaches will be appropriate for all situations, and user requirements for a specific system may well dictate that only one of the above approaches be implemented in a particular system. In addition, we recognize that a investment may be required to maintain information on responder credentials and to establish general policies as well as specific priorities associated with roles assigned to individual responders. Also note that there are ongoing and planned efforts in developing responder credential infrastructure to support incident management that can be leveraged to support this use case.

The other significant functional capability is the capability to reconfigure such a responder's device. In this situation involving a GSM-based cellular network[12], when ACCOLC is invoked, only cell phones with a SIM with priority authorization can access the system; other devices are blocked. The proposed cognitive use case assumes that either the SIM can be provisioned over the air for properly authenticated users, such that the phone would function with priority access. Alternatively, the system could determine that the user was a priority user based on the device ID (as opposed to the priority access code in the SIM) and allow access that way as well; however, the system computational effort to determine whether a call is being initiated by a priority user may involve substantial computational requirements.

We recognize that assignment of priorities presents challenges in making the determination of what communications are more important than others. Part of the ACCOLC decision criteria is

[12] Note that concept of this use case would apply for other types of networks but reconfiguration would be implemented in ways other than over-the-air provisioning of SIMs.

the understanding that implementing ACCOLC would deny access to the network for responders (or for victims and observers who are providing critical information or notifying others). The ability to prioritize communications as proposed in this use case does not guarantee that all critical or important calls are made—there are physical limitations to the capacity of any system. However, this use case provides the opportunity to utilize cognitive radio capabilities to implement the best decisions that can be made with the available information.

In addition to the changes to dynamically modify user priority, it is also important to be able to restore default conditions, such as when the user no longer requires priority access. Different mechanisms for restoration may be implemented but could be similar to the same mechanisms used to implement dynamic prioritization. Restoration could be executed based on a variety of mechanisms, for example user request, incident command direction, and location if the user moves out of the incident area. (see Section 5.4).

6.3.4 Regulatory Implications

The ability to define priorities and block access to the system for certain types of priorities is part of the GSM specification.[13] Since this use case does not change the basic mechanism of ACCOLC, the regulatory changes are limited to only those that may be necessary to allow reprovisioning of SIMs over-the-air to change priorities.

6.3.5 Policy Implications

There are a number of policy changes implicit in this use case.

- Policies for determining the circumstances under which an emergency responder would be eligible to "upgrade" priority?
- What information is required to authenticate the eligibility of the user to operate with higher priority?
- What procedure is followed if a user requests priority? Is there any human in that decision loop?
- Under what circumstances does the device's priority revert to original level? Could reversion be automatic based on responder location, or time frame? Could incident command generate a broad directive (e.g., priority communications no longer required for a particular sector/unit/area) that cognitive capabilities could then execute to restore default priorities for all users?
- While not necessarily applicable in the case of ACCOLC, a more general capability to manage user priorities in real-time could also allow reducing default priorities of responders if their role in the response is less critical. Under what circumstances would a responder's priority be reduced?

[13] Siemens Insight Consulting, "Communicating in a crisis – which technologies can be relied on?" 22 September 2006, available at http://www.continuitycentral.com/feature0394.htm

6.4 Use Case 4: Interface to Non-First Responders

Cognitive radios could allow non-first responders communications access to first responders in specific situations in which the non-first responders are actively participating in the response, while ensuring that mission critical public safety networks are not impacted.

6.4.1 Summary of Scenario Situation

In terms of the aspects of public safety communications:

1. **Physical**: A fourth bomb was detonated aboard a bus near Tavistock Square. A group of doctors were within walking distance of the explosion and the injured people. The doctors arrived on the scene more quickly than first responders and therefore had more timely information than the first responders. No specific prior planning had taken place to apply these physicians as emergency response resources.
2. **Network**: The doctors did not have radios on any Public Safety net, but they did have cell phones and landlines were available in the building. However, no dispatch organization knew of doctors' availability, and thus had no ability to initiate contact with them. Any communication from the doctors had to come from 999 calls to dispatch, with information then relayed to command centers.
3. **Procedural**: Since they were not part of a first responder organization, the doctors had no authority to communicate on the first responder network.
4. **Regulatory**: Communication used established facilities.
5. **Chronological**: No prior planning had been done for the specific incident, but medical personnel are aware of the legal implications of what they do in an emergency situation.

6.4.2 Description of the Use Case

In a mass casualty emergency there is a possibility that there are civilians that have the ability to provide added benefit to the responses that are taking place by the public safety community. In some cases these may be the only response available for an extended period of time. Thus it would be advantageous to leverage this capability and to provide direction to the efforts being put forth. This situation arose in this scenario when the bomb went off in a bus near Tavistock Square, as there was a group of medical doctors meeting in a nearby building. Thus there were a number of qualified medical personnel who were immediately available but were not tied into the incident command communications. These trained medical personnel were not associated with an EMS provider but were on the scene and able to provide qualified medical information regarding casualties. While this was in many respects a fortunate coincidence, a well meaning "good Samaritan" can also do more damage than good if they are unaware of the full situation. Thus the challenge is to establish effective communications with non-first responders without negatively impacting the incident command communications system and capabilities.

In today's communication environment the average person carries as a minimum a basic cell phone with the possibility of text messaging, photo and video capture and transmission. This cognitive use case is an example of how communications capabilities could be adapted to most

effectively take advantage of situations in which non-first responder personnel are positioned to play a role in the response.

We recognize that current concepts of operation and existing procedures do not generally include linking first responder communications networks to non-first responder personnel (regardless of their potential role in a response), and any change to such procedures cannot compromise first responder communications.

Also note that the ability to appropriately link first responder communications with non-first responder personnel can also apply where some first responders are only equipped with commercial equipment. In Europe, for example, volunteers (such as a volunteer fire service) that are part of the response may be equipped with commercial handsets rather than radios that access public safety networks. In such cases, the capability to link them into a first responder network is a vitally important capability.

A cognitive radio capability could allow them to link appropriately (upon proper authentication) to coordinate their activities with public safety professionals as needed. The following provides a view of how this scenario with cognitive radio could unfold:

1. **Physical**: No change from the physical situation described above.
2. **Network:** The initial doctor(s) on the scene would call 999 to report the explosion, and identify themselves as doctors qualified to provide information on the medical status of casualties. Dispatch, upon satisfaction that the caller could provide relevant information, reconfigures the network (infrastructure, portable, or both) to allow the caller to communicate directly with the appropriate emergency management medical coordinator, incident command, and so on as dictated by policy. Once the doctor no longer needs to be connected (i.e., first responder personnel arrive on the scene, the doctor begins performing other functions, or all relevant information has been communicated), the network reconfigurations are rescinded.
3. **Procedural:** Appropriate procedures would be in place to verify that the doctor was qualified to provide the information. This could be accomplished by having medical personnel pre-registered in some manner so that a dispatcher could authenticate the caller (e.g., password, biometric, etc.) and ensure that the individual's credentials already existed in a registry. The doctor(s) would have communications capability as needed to the appropriate organizations within the incident command structure. Procedures would also be in place to establish voice communications channels that would not disrupt mission critical incident command channels.

   Given the presence of pre-registered individuals, an additional capability to be leveraged is the ability to push information from dispatch or incident command (using some type of notification system) out to pre-registered users requesting that they make appropriate contact with the incident command staff for allocation and assignment. Location-aware cognitive radios could also provide information to incident command to refine a notification procedure. For example, upon indication of a problem at Tavistock Square, the medical coordinator in dispatch would look at a map that indicates current deployment of medical resources. The concentration of doctors would show up immediately.

From a detailed roster of doctors near the bus, the dispatcher would select an appropriate number, and would send a short message to their mobiles asking if they can respond to a bomb emergency in Tavistock Square. Doctors would be selected based on their qualifications and specialties. The Cognitive element in the network would establish an ad-hoc response network. Each doctor who responds affirmatively would receive network identification information (i.e., callsign).

4. **Regulatory:** Appropriate regulations would be in place to allow non-first responders to communicate over the designated channels in emergency circumstances. Depending on the communications capabilities used, this may or may not require regulatory changes.
5. **Chronological:** This use case would require that some pre-planning takes place that allows doctors to establish the means by which they can be identified as such during an event (i.e., registration).

The above use case postulates that the communications is initiated by the doctors. A variation of this use case considers a situation in which any interface with the first responder networks is initiated by incident command. In this case we assume that a qualified medical person is not pre-registered but has arrived on the scene of the incident. The individual calls 999; dispatch relays the information through normal channels to incident command. The incident commander or appropriate authority within the incident command structure determines that direct communications with the individual is desirable, in which case the appropriate reconfigurations are executed. The scenario situation would be described as follows:

1. **Physical**: No change from the physical situation described above.
2. **Network:** No change from the network situation described above.
3. **Procedural:** A doctor arrives on the scene of the explosion and calls 999. The doctor explains the situation and his/her qualifications to provide more detailed assessment of the medical condition of the victims to the call taker. The call taker obtains contact information for the doctor and relays the information to incident command. Incident command determines that direct contact is beneficial—the cognitive radio capabilities then establish the appropriate communications network linkage between radios within the incident command/first responder units and the doctor at the scene. Note that additional non-first responders can be added to the network through the same process as needed and appropriate.
4. **Regulatory:** Rules are required to describe exactly how such an ad-hoc network is to perform and what channels they use.
5. **Chronological:** This use case would require that some pre-planning takes place that allows doctors to establish the means by which they can be identified as such during an event (i.e., registration). Registration would also cover responsibilities and liabilities that are assumed by the individual to perform such functions in an emergency. At time of notification of the event, each Doctor would have the option of responding, or opting out. If they respond affirmatively, they would become an on-site resource for incident command.

6.4.3 Functional Capabilities

The specific functional capabilities involved in this use case depend on the approach used to implement it. If the implementation involves reconfiguring non-first responder radios to provide them with a capability to communicate with the incident command/first responders, then the functional capabilities include the ability to download a waveform and the ability for the non-first responders' radios to be reconfigured accordingly. If the implementation is based on infrastructure linking in a non-responder radio, then there must be a means for the non-first responder radio to upload information about the radio type.

A key element of this use, although not considered part of the cognitive capabilities, is ensuring that any user who is linked to the first responders has a legitimate need for such communications, and has a device that will not adversely impact first responder communications. Establishing that a user has a legitimate need for such communications involves a number of issues:

- Is the person someone appropriate for working with first responders? One approach used currently for interaction between first responders and civilians is to utilize some pre-registration process for translators, ministers, physicians, hazard experts, etc. Background checks were performed on all individuals prior to use.
- How is the identity of the user verified? Is the user who he/she claims to be?
- How is information provided by a user verified? In the scenario, assuming a doctor notified dispatch of the existence of casualties, how can that information be verified to a level of confidence necessary to modify communications? (Note that dispatch call-takers routinely evaluate the information provided in incoming calls.)
- How is the potential role of a non-first responder verified?

In addition, the role of such responders would need to be incorporated into the incident management (e.g., NIMS) as appropriate. Note that it is common for existing dispatch centers to have a capability to patch a phone line to a radio channel. This cognitive use case extends that concept to include establishing links between first responder communications channels and non-first responder wireless devices/radios.

6.4.4 Regulatory Implications

Regulatory implications may also depend on implementation approach. Reconfiguring a non-first responder radio to be able to have some type of access to a public safety network would require changes to the manner in which radios are currently type accepted. The alternative implementation, in which the non-first responder communicates on their existing frequencies which is patched to a public safety network frequency or channel is done with current technology and would not generally require regulatory changes.

6.4.5 Policy Implications

Policy implications are dependent on the extent to which "non-first responders" are currently incorporated into emergency response/incident management. In locations such as the United

Kingdom, where volunteer responders are incorporated into the response team, the only policy change would potentially involve:

- Guidance on the circumstances under which the cognitive capabilities would be exercised to establish access for non-first responders (including policy on authentication, security, and procedures);
- Guidance on what communications are appropriate under such circumstances; and
- Guidance on when and how non-first responders are disassociated with the network.

For agencies that typically do not utilize direct communications with non-first responders, such as those in the U.S., any implementation of this cognitive capability would involve much broader policies.

7 Appendix: Chemical Plant Explosion Scenario Use Cases

7.1 Use Case 1: Role-Based Reconfiguration

There are a number of events in the scenario in which the first responders from multiple agencies are arriving to support the incident response. Given the scope of the incident, these responders are not from jurisdictions within which the incident is occurring, but are from outside areas for which there are no standing mutual aid agreements and pre-planned communications interoperability capabilities. This means that upon arrival to the incident their radios are not interoperable with local communications systems in use for incident response. The concept of this use case is that arriving radios can be reconfigured specifically to facilitate capabilities that the responder requires, based on the arriving responders role within the incident response structure.

The capability that the arriving radio should provide is a function of the role that the responder user is performing—for example, supervisors in the incident command structure may need more capabilities than other users. This approach provides greater control of communications resources and ensures that interoperability does not result in "everyone talking to everyone." Once a radio is reconfigured, test messages should be sent to ensure that the reconfiguration was successfully executed.

As with any of the use cases that involve reconfiguration of the radio, it is also necessary to be able to rollback reconfigurations to a previous state, and to the pre-incident state on incident completion. This rollback capability is addressed as a separate use case (see Section 5.7).

The impact of this use case can be greatly enhanced by the use of over-the-air reconfiguration/reprogramming. In the described scenario, an assumption is made that arriving radios can be reconfigured while responders are either en route to the incident, or in the field, as needed as responders are reassigned. However, the use case for role-based reprogramming can also be applied even without over-the-air reconfiguration; in this case cognitive capabilities can still provide reconfiguration information even thought the radios must be physically connected to a computer (i.e., "tethered") to be reconfigured. Thus for the discussion in Section 5.1, we focus on the use case to link radio configuration to the roles of a first responders, and make no assumptions about the process by which the radio is reconfigured—specifically, this use case could be realized using current methods of reprogramming the radio by physical connection to computer.

7.1.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are numerous first responders who are arriving to support the incident response. They either report to a staging area, or (in conjunction with Use Case 2) register with incident command while enroute to the incident. They are then physically re-located within the RF coverage footprint of the network(s) supporting incident response communications.
2. **Network**: The first responders have radios which are not pre-configured to interoperate with the network(s) supporting incident response communications, or limited access to nationwide interoperability frequencies. Thus, initially, they have no radio connectivity with the incident response team.
3. **Procedural**: There are several possible procedures based on the technology used to provide interoperability. If cache radios are handed out, there are procedures defining the use and responsibility for the cache radios. If some type of gateway is used to patch channels/frequencies of the arriving first responders and the existing network, there are procedures defining authorization of use of the patch as well as responsibilities and use of the channels/frequencies. There are also defined procedures that define roles and responsibilities of an incident command structure. (In the United States, for example, the procedures are defined as part of the National Incident Management System, or NIMS.)
4. **Regulatory**: All channels/frequencies used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case.
5. **Chronological:** Either a patch or gateway device must be activated to bridge frequencies, a task taking anywhere from a few minutes to an hour or more (see Use Case 3 for a more detailed discussion of gateway capabilities). Reprogramming a radio to operate on the network(s) supporting incident response communications can take as little as take a few minutes (assuming permissions are in place).

7.1.2 Capability Shortfall

Current systems provide limited and static capability to configure radios based on the roles and responsibilities of the radio user. Some agencies have “supervisor” radios which are configured to provide different capabilities than radios given to other personnel, but these capabilities are often built into the radio and cannot be changed. Some radios can also be reconfigured to include needed channel/frequency assignments and functions, but this is a manual process. In addition, such program templates are typically predefined and not modified during the course of an incident.

As a result, responders generally have identical capabilities in their radios. In the event of a major incident, in which responders arrive from outside the jurisdiction where the incident is occurring, incompatible arriving radios need to be reprogrammed to support the incident response. Because of the general static nature of radio configuration templates and the “one-size-fits-all” approach, responders’ radios are programmed generically. The challenge is that either a very limited number of functions and channels are provided, which may limit the responders’ capabilities, or the maximum capability is provided, an option which opens the door for the chaos of “everyone talking to everyone.”

Note that this use case assumes that radio interoperability is achieved by reconfiguring the arriving responders' radios to operate within the local network(s) supporting incident response communications, as opposed to configuring the network (by activating a patch or gateway capability).

While most of the above discussion is based on providing capabilities to users based on their role, this use case also includes managing capabilities for all network users based on emergency status, responder role, and optimizing use of network-wide resources. For example, an issue recently observed on regionally trunked radio systems, is unintended consequences of public safety personnel/responders who are not actively involved in a response remotely monitoring response activities via the trunked system talk-groups. For example: an off-duty responder monitoring over the network from a location (home) that is a significant distance from the incident site (using network capacity to transport the incident communications (audio) to a remotely connected location away from the incident). This activity may be well-intentioned and often legitimate from the perspective of first responders who are rotated in and out of the incident and want to maintain situational awareness before returning to the incident. This may also occur from the perspective of lending agency dispatch centers who want to monitor activities of mutual assistance activities to which local resources are deployed. This can impact local radio system resource availability on network segments that may be capacity limited, invisibly consuming local over the air resources needed to ensure continuity of local services outside the area and unrelated to the monitored incident. (For instance, during the recent bridge collapse in Minnesota, network resources on the city system met the needs of incident responders, but network segments on the periphery of the regional system were capacity limited. Remotely monitoring the incident impacted the ability to dispatch ongoing non-incident related calls.) Reconfiguring user radios and prioritizing the network resources appropriately can ensure that the communications channels are used for the highest priority needs, for both the incident as well as ensuring resource availability required for continuity of ongoing operations away from the incident.

7.1.3 Description of Use Case

The concept of this use case is to use cognitive capabilities to create the appropriate radio programming template for the radio, based on the radio user's role within the incident response. In addition, this capability would be dynamic so that as the responder's role changes, the radio is reprogrammed/reconfigured to provide the necessary supporting capabilities.

With respect to the specific aspects of the scenario situation noted in Section 5.1.1, this use case would result in the following:

1. **Physical:** There is no change in the physical deployment of assets.
2. **Network**: Reconfiguration of the radios provides role-based connectivity to the network(s) supporting incident response communications.
3. **Procedural**: The primary procedural change in this use case is explicit definition of responder roles in an incident, and explicit definition of the communications capabilities and operating procedures associated with those roles. (Note that definition of roles and communications capabilities must be done as part of pre-incident planning.)

4. **Regulatory**: All channels/frequencies to be used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case.
5. **Chronological:** This use case does materially change the timelines involved in reconfiguring radios for responders' use in an incident. Radios that are not operable with the network(s) supporting incident response communications must be reprogrammed.

7.1.3.1 Functional Capabilities

Cognitive radio functions required to realize this use case include the following:

- Explicit definition of user roles within an incident response structure. The appropriate (based on the incident command procedures in place for the jurisdiction or region) framework for identifying responder roles should be used as a baseline. One of the technical challenges is the cognitive system's ability to react to the adaptations and tailoring of an overall framework that is required to meet the user requirements within a specific incident.
    - User roles could be organized in a hierarchical (or other) structure. For example, roles could be defined for fire, law enforcement, medical, etc. Then within each of these categories there could be appropriate subcategories, (e.g. EMT, doctor) and ending with a specific role such as on-site triage.
- Electronic storage of a user's credentials (e.g., an RFID chip). Credentials could contain digital certificates and a listing of all roles that the individual is qualified to fulfill within an incident response. Such a function would allow the user to authenticate his credentials using any radio capable of querying the network, and to inform the network of their presence and qualified roles. Command authorities could then make an informed decision as to how the individual could best function in support of the incident response. An enabling code would then be transmitted from the network back to the user radio (and the user) which, when accepted by the user, configures the radio in a proper state to support that user's role. The user would then follow up with command to find out specific details of their actual tasking within the incident.
- Ability to authenticate a user's qualifications, in support of a specific incident need.
- Ability to query user radios for information including, but not be limited to, manufacturer, radio type, available modes, software/hardware version numbers, reconfigurability, etc. The format/protocols for such information must be vendor neutral and standardized. This capability is particularly important when a mix of radio types are being used and not all devices can be pre-programmed.
- Definition of appropriate radio capabilities in context of its user's role. Note this can range from manually defined, pre-planned assignments (which is completed, to a limited extent, within current device capabilities) to a more cognitive-based, dynamic function which operates in conjunction with network management resource allocation (see Use Cases 2 and 3) to dynamically determine and provide appropriate radio capabilities needed to support a user as the incident evolves.
- Ability to associate users, radios, and user roles.

- Ability to reconfigure the radio based on the user's role. There are several approaches to reconfiguration that can provide this capability. The simplest approach is to reprogram the personality of the radio, which includes frequencies, channels, talk group assignments, and so on. This capability is a typical feature of public safety radio systems available today.
    - An additional level of control on radio use could be achieved by also using downloadable executable policies. These policies would define constraints and implement restrictions on the use of the radio based on the responder's role. Use of policies could ensure that the use of the radios stays within regulatory constraints, and also provides additional controls to avoid the challenges of "everybody talking to everybody".
    - Radio capabilities constrain radio reconfigurability. For example, a radio that does not have a P25 data capability is not likely to be able to be "reconfigured" to handle P25 data, given the current generation of P25 radios, without a complete software download or hardware upgrade. However, it may be possible to have capabilities pre-programmed into their radios but selected capabilities disabled for use until reconfiguration activates them. Then, when the radio is deployed in a situation described above, specific required capabilities could then be enabled (turned on) and any that are not required could be disabled.
- For over the air reconfiguration, a standards-based over the air programming capability is needed, to include the software tools and a radio "meeting point" (with standardized modulation, bandwidth, frequency, and protocols) to obtain configuration data for radios to be reprogrammed over the air.
- Sufficient security must be included to ensure integrity of the over the air reconfiguration process.[14]
- An ability to restore a radio to a previous configuration, including a default configuration and the re-configuration of the radio to its state prior to the incident; this function is addressed separately in the Revert/Rollback Use Case discussed in Section 5.8.)

7.1.3.2 Regulatory Implications

All channels/frequencies to be used are licensed public safety frequencies. Therefore there are no regulatory implications of this use case for radio use by public safety personnel.

However, the licensee of a given radio may not be licensed for channels which are available and for which a pre-existing mutual agreement is not in place, precluding legal use. Regulatory changes could facilitate this process; for example, use of downloadable executable policies covering frequency usage that reflect regulatory policies could allow more dynamic application of regulatory constraints.

Some regulatory support may be required for implementing the "meeting point" function described in Section 5.1.3.1 for standardized over the air reconfiguration.

[14] The SDR Forum Security Working Group is currently addressing this topic and is preparing a report entitled "Securing Software Reconfigurable Communications Devices" for subsequent release.

However, this use case also facilitates the ability of non-first responders, particularly if they are acting as liaisons to public safety personnel within an incident command framework, to have a role defined such that their radio include public safety frequencies. This aspect of the use case may require some regulatory changes to be realized. (See the Interface with Non-First Responders Use Case discussion in Section 5.6 for a use case discussion specific to the communications interface between first responder and non-first responder personnel.)

7.1.3.3 Policy Implications

The major policy implication of this use case is definition, in much greater detail, of the relationship between radio capabilities and responder roles than is currently available. Note that these policies and procedures will likely vary from jurisdiction to jurisdiction unless national standards are established and followed. One advantage of this use case is that it allows individual agencies to define policies and procedures for incident response, and ensure that responders with whom they have previously trained or worked with can follow those polices since they are programmed into their radios.

Procedures must also be defined to:

- Describe responders' roles;
- Authenticate the users and their assigned roles; and
- Test the radio by sending/receiving a set of test transmissions to ensure that the reconfiguration was properly executed.

Users will need to be trained in the reconfiguration process and changes in radio behavior that may result.

A standard definition of radio capabilities and the protocols used for query/response transmissions must be defined to allow the network to query radio capabilities to determine how the radio can be reconfigured to support the defined role.

7.1.4 Summary of Impact of Use Case

One of the major concerns expressed by the public safety community about interoperability is that providing interoperable communications can devolve into chaos if everyone can talk to everyone. Aside from extensive training and user discipline, one way of managing this issue is to provide responders with the only the communications capabilities that they need without providing them capabilities that they do not need. "Need" is based on the responder's role in the incident response. Thus role-based reconfiguration of radios provides agencies with much greater control of their communications resources and reduces the risk of inefficient use of those communications resources, and eliminating confusion resulting from establishment of links and resources that are not needed or appropriate. Furthermore, individual agencies can define agency specific policies and procedures, in terms of radio configuration, so that responders who typically do not use the network(s) supporting an incident response can operate within these defined policies without significant additional training.

The other significant impact is that role-based reconfiguration provides must greater ability to evolve communications capabilities to meet the changing demands of an evolving incident. One of the challenges in incident management is that incidents are unpredictable and dynamic—no amount of pre-planning can account for all possibilities, and user training is focused on

providing an overall framework that can be adjusted as needed. This use case provides tools that allow user communications capabilities to be dynamic, and adjusted as needed to meet incident communications requirements.

7.2 Use Case 2: Resource Management in a Dedicated Public Safety Network

There are several points in the scenario in which real-time management of network resources becomes critical. While network resource management is always an important component of communications support, several events in the scenario (16, 18, 25, 29) highlight specific situations in which incident communications requirements exceed the system capacity, creating a need for greater network resource management tools than are available today.

For example, as the incident progresses the shared broadband network capacity reaches its technological throughput limit. The network moves into its next level of QoS parameters and begins to throttle some types of traffic throughput, particularly for data intensive applications. Applications respond to the throttling by reducing their throughput requirements while still delivering an acceptable product. Traffic cameras sense the reduction in available throughput and reduce the quality of the frame rate of the video. AVL and other sensor data reduce their beacon rate. The commanders notice the reduction and begin to force some sensor applications to send updates more frequently. The applications respond by resetting their beacon rate to a more acceptable level, other less critical sensors, intern, reduce their beacon rate further to compensate.

As the broadband network reaches capacity, the voice network does also. In response to incident needs IC directs FDMA users to use (repeated) conventional national interoperability channels, allowing the trunked system to handle more TDMA users, effectively providing more capacity. Simultaneously a frequency sharing agreement is invoked with Metropolis. The Central City 700MHz trunked system communicates with the Metropolis trunked radio system, to dynamically allocate additional frequencies, as needed, to the Central City system. This agreement allows an extra 5 channels or 10 TDMA talk paths to be temporarily added to the Central City system.

Another potential aspect network resource management involves a concept which we refer to as spectrum mutual aid. In much the same manner that agencies share manpower and equipment resources during major incidents, the ability to reconfigure communications resources could allow agencies to share spectrum resources. Agencies could establish sharing agreements that, by mutual consent, disable use of a particular frequency by one agency (for which it is licensed), and then allow another agency to utilize (borrow) that frequency during a major incident. As noted below, this concept requires some regulatory and procedural changes, and would require appropriate frequency coordination prior to deploying equipment and establishing such a mutual aid pact.

Network resource management may be helpful in adjusting talk groups or other network links as the incident evolves in geographic scope and/or number of users. For example, a traffic perimeter control net may need to be sub-divided into multiple nets as the incident perimeter expands, as voice traffic on the designated channel/talk group approaches capacity, or the geographic extent of the perimeter expands. Monitoring evolving geographic extent of communications is required for an incident and critical to ensure that users stay within the coverage area of the communications channel being used, and that incident transmissions are not disrupting other

mission-critical communications at the "edges" of the evolving incident. The proposed cognitive capability described in this case is use of information about the location of the radios, traffic loading, role information (see Section 5.1) and the RF environment (see Section 5.4) to determine optimum allocation of frequency resources, and modification of talk groups, and so on. The most likely implementation approach would involve cognitive capabilities able to recognize (or anticipate[15]) a situation in which communications are likely to degrade, and then recommend solutions to a network operator or comm. unit leader for execution.

Network resource management can also be implemented on a more localized scale; for example, using technology such as adaptive antennas and/or adaptive power output can be used by individual radios, or coordinated among multiple radios in a network to mitigate the effects of RF interference. This topic treated as a separate use case (see Section 5.4).

7.2.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** The extent of the damage caused in the chemical plant explosion requires marking and recording each location that involved casualties, fire, evidence, incident parameters, etc. The affected area, where information must be collected, can extend over a large geographical area encompassing both hazardous and non-hazardous zones. In addition, there are a significant number of first responders located within the immediate vicinity of the chemical plant.
2. **Network**: Network loading approaches the capacity of available network resources. Presently geolocation information is exchanged, via a narrowband channel, on the land mobile radio network (if the feature is available) and the resulting information is not conveniently available to the Incident Commander or Comm Unit Leader. In current trunked radio systems, queuing times for calls can be collected, but this information is not mapped to the location of the communications assets to provide an overall "picture" of the RF environment. Network management data that is (sometimes) communicated in a standard way from public safety subscriber devices to the network, for network management use (such as channel occupancy) is insufficient to support the scope of network resource allocation envisioned in this use case. In addition, there is no overall control of spectrum requirements for data transmissions that could be varied as a function of priority, resolution, and so on.

   The exchange of geolocation and RF information by network entities will depend on the degree of interoperability deployed to promote and support the seamless transfer of data. Interoperability enhances operations and saves time; conversely, lack of such interoperability results in inefficiencies which can translate into lost time and affect safety of first responders.
3. **Procedural**: Current procedures provide limited options for network resource management. Talk groups, priorities, and QoS controls can often be modified, but generally they are not because of the difficulties of doing so. This must be done manually, and without all of the supporting data required to do so effectively. Procedures

[15] For example, a cognitive capability with information on radio locations, channel frequency, and terrain/land use could run coarse propagation models to anticipate when radios may exit the coverage footprint of a network.

to allow spectrum mutual aid generally do not exist other than for certain pre-established shared channels

4. **Regulatory:** There are several aspects of network resource management which are bound by current regulations.
   a. Reallocation of frequencies: only frequencies licensed to the system user can be reallocated, and only within the licensed footprint of that channel. There is currently no regulatory provision for allocating/loaning licensed frequencies to another user (the spectrum mutual aid concept).
   b. Frequency coordination is often based on defined contours; changes to the contours by adaptive antennas are not allowed under current rules. Using frequencies that are licensed by a user at a specific location, at another location, will often fall outside licensed contours. Regulatory implications become more involved when those contours are in the vicinity of international borders. (Conversely, use of adaptive antennas might also be used to ensure licensed contours are not exceeded).
   c. Geolocation signaling is covered under existing rules for public safety communications.
5. **Chronological:** Network resource management options are limited and generally not automated. When an incident starts, network resource allocation is critical, but it is impossible to predict how the incident will evolve over time, and therefore current capabilities tend toward static network configurations that are increasingly inefficient over the course of the incident. Manual changes to the network, to better allocate resources, require minutes or hours for implementation.

7.2.2 Capability Shortfall

Current (trunked) public safety systems have some limited capability for reconfiguration to accommodate network resource management. Implementing network changes through the use of these capabilities effectively in real time is limited, due to:

- Lack of data (such as locations of user radios and information about the RF environment) that can be used to better configure network resources;
  - Present day public safety geolocation capabilities utilize custom alert messages that the radio can send containing pre-determined events (such as Unit Emergency Alert) or more typically, an IP Service where radios can be polled and then respond with location data (either with a onetime response or a periodic response until time expires and/ or # responses is sent). The PSSIG is not aware of any LMR Air Interface that sends GPS location data embedded with a voice call (i.e. embedded in the header data and therefore capable of being sent regularly all the time, with any voice stream).
  - RF information is not available for analysis or for network resource management decisions, and there are currently no capabilities in place to adjust spectrum demands or to arbitrate among competing communications requirements.
- Limitations in reconfiguring radios to automatically take advantage of changes in the network structure/topology.

- Limitations in network reconfiguration capabilities.
- Lack of effective tools to monitor, anticipate, and identify situations in which network resources should be reconfigured.
- Limitations in automating the network reconfiguration process.

7.2.3 Description of Use Case

As the incident unfolds a cognitive capability within the network monitors the geolocation of the radios on the net, the traffic loading on the channels, and the RF environment as reported by the individual radios. The cognitive capability monitors trends, for example; geospatial distribution of radio users on certain radio nets that remain in the same general area (e.g., users located within the immediate area of the chemical plant) or radios supporting users on other nets (such as those assigned to coordinate evacuations) that cover larger, and shifting, geographic areas. Users on some nets provide a relatively constant level of traffic, while traffic from users on other nets require significant increases in capacity as the incident evolves. The network cognitive capability monitors these ongoing situations, and determines at various points in time that network resources need to be reallocated to ensure coverage (see Section 5.4) for all radio users that are on a particular net/channel, and to ensure that there is sufficient capacity by dynamically re-allocating frequencies, or adding frequencies in support of incident communications, or by changing user priorities (or QoS parameters) ensuring that the most important transmissions have the highest probability of success. These tasks must be completed without causing interference to other networks.

A survey of the explosion area is conducted by LE, Fire, and EMS personnel to mark and record geolocation data of casualties, fires, evidence, the incident perimeter, etc. This information is available to the IC as a GIS overlay on a map of the explosion area. Network operational information (location and operating parameters of radios, detected signal strength information, spectrum sensing data) is also provided to the COML.

The impact of these capabilities is such that information can be collected, analyzed, and disseminated to those with need. The network cognitive capability would provide recommendations for action and also enable RF environment and geolocation information to be transmitted to the Comm Unit Leader. The Comm Unit Leader uses the information provided to optimize, modify, and then execute recommended network changes, reallocating network resources (power output, talk group assignment, frequency reuse) as needed. With respect to the specific aspects of the scenario situation described in Section 5.2.11, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets. The cognitive-enabled reconfigurable device is deployed in the same manner as current devices.
2. **Network**: Connectivity (e.g., who can talk to whom) would not change. How the network implements connectivity may change, including network aspects such as the allocation of frequencies, user priorities, and QoS parameters. The cognitive capability would be integrated with geolocation information to optimize radio transmit power output, talk group assignment, and frequency reuse.
3. **Procedural**: There are a number of procedural implications that must be addressed in order to realize this use case:

- COML (or network operator) procedures (and training) would be changed to provide the expertise to effectively manage the network resource management options that would be available.
- Dynamic allocation of frequencies; before frequencies licensed to agencies are made available (loaned) to other agencies via "spectrum mutual aid" agreements, pre-coordination (via frequency coordinators) will be required to ensure that these operations do not impact third party agencies.

4. **Regulatory**: Some regulatory changes would be required to permit the dynamic allocation of frequencies by non-licensed users per agreements with licensed users. The other aspects of this use case, such as modifying talk groups, cross-programming within subscriber radio units, reassigning channels, and so on are capabilities that are allowed today, but are not generally performed automatically. There are not likely any regulatory changes required to accommodate those capabilities.
5. **Chronological**: Enabling this cognitive capability would increase efficiencies in responding to situations that arise and then subsequently dealing with network changes in support of the response. Native cognitive capabilities would be seamlessly handled. Network reconfigurations that require manual activation are likely to require minutes or hours; cognitive capabilities that can provide recommendations can cut this time to seconds.

7.2.3.1 Functional Capabilities

There are a number of functions that need to be implemented to realize this use case, they are listed below.

- **RF Environment Sensing:** This cognitive capability described assumes a decision process based on knowledge of the RF environment which, in turn, requires that the individual radios provide some information about the RF environment at their location. The specific type of information to be collected may vary based on the algorithms for monitoring, anticipating, and identifying network resource allocation issues (see paragraph below). In general, this would include the received signal strength of the network transmit site, signal-to-noise and/or signal-to-interference ratios, for both the frequencies currently being used by the device and information about other frequencies accessible by the radio. In addition to an ability within the radio to collect this information, there must be a standard method of transmitting this information back into the network for analysis.
- **Geolocation:** The cognitive capability to use geolocation data is implemented in one of two ways: autonomously and manually. Autonomous geolocation capability is made possible using radios that have this cognitive capability incorporated into the radio devices, infrastructure, and command and control interfaces. This geolocation functionality executes in the background providing information to the network; information that includes user identification data, location data, and radio operational statistics under normal conditions. When the system senses an increase in activity, the network cognitive function will adjust resources to accommodate traffic loading changes and the nature of priority of calls. If a user connects a peripheral device such as a camera, oxygen, or chemical sensor, etc, to their cognitive radio it will automatically

begin integrating the new data into the infosphere. On the dispatch or command and control end, the system infrastructure and computer aided dispatch services will incorporate this new information into the network external sensor data pool.

The second approach to incorporation cognitive geolocation capability is through an interoperability device that cross-patches information between disparate radio systems. Once the system has been manually activated, the device will automatically sense the type of radio networks that are being bridged and information about associated network subscriber equipment, from which it will extract available geolocation information. If interoperability plan data is available in advance, the interoperability device will utilize that information when cross-patching the disparate system. Manual intervention is needed to terminate the use of the manually operated initiation of the interoperability device to utilize geolocation information.

If this geolocation feature is enabled, when a visiting subscriber device is added to the network, the network will automatically incorporate it in a manner analogous to adding a peripheral device to a personal computer. Device features could be added by downloading device drivers automatically and then to adding data received from the vesting device to the dispatch console. If a specific feature is not supported, the information will be logged or archived for post processing.

- **Algorithms for monitoring, anticipating, and identifying network resource allocation issues:** Core cognitive capabilities include an ability to monitor data from the evolving incident, then establishing trends and trigger points for network changes, anticipation of the need for network reconfiguration, and then identifying available options for COML use. Trend analysis is important to distinguish between network events; e.g., simple short-term spikes in network traffic versus a temporary geographic relocation of network users for which resources must be quickly adapted, or by quantifying longer term trends associated with incident evolution.

7.2.3.2 Regulatory Implications

Some regulatory changes would also be required to permit the dynamic allocation and sharing of licensed frequencies, by other users, per pre-established agreements with licensed users (this is similar to the regulatory considerations described in Section 5.1.3.2). Other aspects of this use case, such as modifying talk groups, reassigning channels, cross programming of frequencies etc, occur within the rules today, but these network changes are not generally performed automatically. There are not likely any regulatory changes required to accommodate those capabilities.

For network based cross-patching or transcoding of information between disparate (licensed) systems, regulatory requirements should not be an issue because current the over-the-air regulations currently governing these operations would be in force. Non-network based over-the-air transactions would be subject to regulations governing public safety LMR communications.

7.2.3.3 Policy Implications

A major policy implication involves a significant change in the role that the COML, or network operations manager, has in terms of real-time network control. Current systems generally rely on

extensive pre-planning and network management generally ensures that the network stays operational within a mostly static network plan. This cognitive use case envisions that a much wider range of options for dynamic network resource management will be available to the COML, or network operations manager. Options supported by data and analytical capabilities that are not available today. Note also that policies may need to be established or modified as to the conditions under which data that could continuously track the location of responders is collected, maintained, and disseminated.

7.2.4 Summary of Impact of Use Case

By collecting RF and geolocation information from individual radios, a COML or network manager would have access to data necessary to more effectively manage communications resources. Management of current network technology relies on static, pre-defined allocation of resources that are difficult to enhance as incident response requirements change. With access to geolocation data, the COML would be able to monitor, plan, and react to changes in the environment and the incident response requirements to utilize communications resources more effectively.

7.3 Use Case 3: Resource Management in a Shared Public/Private Network

The network management use case described above, in Section 5.2, focuses on management of resources assuming a dedicated public safety network. However, one of the elements of the scenario is the existence of a shared public/private broadband network. While there are many similarities in the capabilities needed for network resource management for both the dedicated public safety network and the shared public/private network, we analyze this case as a separate use case because there are significantly different regulatory and procedural considerations (which should be transparent to the first responders).

The motivation for this aspect of the scenario is based on the ongoing activities regarding the 700 MHz spectrum in the United States. Although the final rules governing use of that spectrum were undetermined at the time of this report, the concept of establishing a shared network using common spectrum and common network resources to support both public safety and commercial users is still a potential outcome. A shared network is one that can benefit from both software defined radio and cognitive radio technologies.[16] For the purposes of this use case, we assume that there is a shared network, in which spectrum resources are licensed for both commercial and public safety use.[17] There is a network sharing agreement between the public safety and commercial entities accommodates commercial use of the spectrum during routine conditions, and prioritizes public safety use of the spectrum during emergency situations. Other aspects of the partnership (regional or national, whether the public safety license holder is the local agency or a national license holder, and so on) are immaterial to the use case.

Event 15 requires the network sharing agreement emergency provisions to activate in the system. The current demands of broadband data to incident command have exceeded the negotiated

[16] See SDR Forum Reports "Considerations and Recommendations for Software Defined Radio Technologies for the 700 MHz Public/Private Partnership," Report No. SDRF-07-R-0024-V1.0.0, and "Utilization of Software Defined Radio (SDR) Technology for the 700 MHz Public/Private Partnership," Report No. SDRF-08-P-0004-V1.0.0, both available at www.sdrforum.org.

[17] Note that this could be established in a manner along the lines of the FCC's original concept for Block D of the 700 MHz spectrum, or through an allocation of spectrum specifically designed for shared use.

threshold. The network agreement must mandate automatically reconfiguration of resources to accommodate the bandwidth requirements of public safety users through any way possible. Note that Use Case 2 addresses network resource allocation and network management in general. This use case extends that concept to look specifically at the use case in the context of a shared public/private system.

Based on governance and resource sharing rules, when activated, the cognitive network immediately activates its emergency service plan and places public safety data at the top of the QoS prioritization list. The cognitive network begins to plan for other ways to accommodate user throughput needs, by increasing modulation complexity and/or channel bandwidth. The network must automatically sense the most efficient modulation format available, based on the location of the responders. The network must identify the towers through which the responders and command are communicating. The network may then reconfigure the carriers' frequency reuse plan to increase channel bandwidth on some towers, which may also include disabling some network resources for the duration of the emergency. As responders move, the network automatically optimizes its configuration, as required, to adapt to user needs.

As noted in Event 15 of the scenario, the network resources include terrestrial and satellite communications. Cognitive capabilities can also provide intelligent routing to sustain connectivity when communications links cannot be supported by land-based network segments, because of network capacity constraints, or because user nodes move beyond the RF coverage area of the network.

7.3.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

- **Physical:** There are a number of first responders located in the same area as non-first responders (e.g., victims, people trying to evacuate the area, people stuck in a traffic jam caused by the vehicular accident, and so on)
- **Network**: Both first responders and non-first responders are accessing the shared network resources per the existing network sharing agreement.
- **Procedural**: The network sharing agreement specifies that under certain emergency conditions, the ratio of network resources allocated to first responder communications and those allocated to non-first responders can be changed, effectively increasing the allocation used by public safety.
- **Regulatory**: This resource re-allocation is based on a pre-negotiated agreement within the existing regulatory framework.
- **Chronological:** The need to re-allocate resources is determined and executed over a matter of seconds.

7.3.2 Capability Shortfall

The concept of a public/private partnership in which spectrum allocation can change based on need and an emergency circumstance does not exist to the extent that is envisioned in this use case. There are examples of trunked systems in which public safety and other non-public safety governmental functions co-exist, and there are examples in which public safety users utilize commercial data systems, but neither of these examples reflect the challenges inherent in a

network shared between commercial users and public safety users in which network resources are reallocated based on emergency conditions.

7.3.3 Description of Use Case

This use case specifically describes cognitive capability to automatically implement network resource allocation procedures defined in a network sharing agreement between a commercial carrier and a public safety agency.

With respect to the specific aspects of the scenario situation noted in Section 5.7.1, this use case would result in the following:

1. **Physical**: The physical location of the public safety and commercial users does not change in this use case.
2. **Network**: Connectivity remains the same in this use case; public safety and commercial users continue to access the network. However, the resource allocations change as a function of public safety network user needs, establishing a lower priority for commercial user bandwidth needs during incident response, resulting in greater blockage of lower priority commercial traffic during the incident. This condition is a transitory state that will automatically revert as the incident response dissolves, and commercial customers would purchase services based on prior knowledge that commercial network resources are managed in this way[18].
3. **Procedural**: The procedures for network resource allocation are defined in detail in the network sharing agreement between the public safety license holder and the commercial entity.
4. **Regulatory**: The regulatory regime provides explicit support for shared spectrum use.
5. **Chronological**: The procedures for network resource allocation are defined prior to an incident. Execution of the procedures occurs in real time.

7.3.3.1 Functional Capabilities

Functional capabilities required to realize this use case include the following:

- A capability to adjust network resource utilization based on the terms of the network sharing agreement. The core cognitive capability is to provide a greater portion of available network resources to public safety when they are needed by public safety. The specific implementation of this capability would be driven by network sharing agreement terms. For example, an agreement would typically provide for public safety use of a pre-defined portion of shared network capacity on an as needed basis for day-to day operations, requiring some simple prioritization of traffic such that commercial access is on an as-available basis. The network sharing agreement would also have terms by which public safety could utilize all available network capacity, pre-empting all commercial use. If this "trigger condition" is based on a public safety utilization threshold, or some alert condition, then some network load monitoring capability would be required to monitor these conditions and activate network priority changes. If the network sharing

[18] Conversely, since the shared network would be build to hardened public safety specifications, commercial customers would likely gain in the context of enhanced day-to-day network reliability.

agreement relies on some external declaration "trigger" condition(s) have been met, it may still be helpful for relevant data to be collected by the network. It may also help overall network resource management if agreement "trigger" conditions can be anticipated or predicted.

- The capability to revert from public safety network priority use is required as the emergency communications requirements decline below the trigger thresholds. This capability is the inverse of the above capability, and relies on the same network operations monitoring and incident management as the capability to increase the spectrum allocated to public safety. We identify it separately because the ramp down of network operations often tends to not receive the same level of interest as the ramp up process, and because the economic viability of such networks is likely to depend on the rapid restoration of commercial services (consistent with ensuring that public safety operations are not compromised).
- In addition to identifying the key conditions for network sharing, the other function required to realize this use case is the ability to allocate additional spectrum in the most effective manner.

7.3.3.2 Regulatory Implications

The assumption in this use case that "the regulatory regime provides explicit support for shared spectrum use" has not been broadly adopted at this time. In the United States, there has been a lengthy proceeding relating to this concept and the related auction of spectrum in the 800 MHz frequency band. While much of the proceeding dealt with auction rules and licensing (which we do not address here), the regulatory framework of a network sharing agreement between public safety spectrum and commercial spectrum licensees has also been debated in great detail. Rather than repeat that extensive discussion, we note here that currently regulations do not generally support the level of spectrum sharing envisioned in this use case, and thus significant regulatory changes would be required.

7.3.3.3 Policy Implications

There are a number of policy implications related to this use case. The heart of the policy considerations is the proposed network sharing agreement. Such an agreement would codify the policies of spectrum sharing.

For the individual users, however, there would be little policy change required, as the use case involves dynamic allocation of network resources (capacity) for public safety use, most likely in a network built using shared commercial and public safety spectrum. Thus the only impact to the end user should be improved performance, unless incident conditions cause commercial traffic to be completely pre-empted on the network; a known potential condition, established in commercial end-user service agreements.

7.3.4 Summary of Impact of Use Case

The major impact of this use case is enhanced performance and capacity for public safety users during an incident response. By sharing spectrum resources, public safety users have access to more network resources when needed to support incident response communications, allowing more data to be moved more effectively and quickly, with greater robustness.

7.4 Use Case 4: Coverage Performance Improvement

Event 19 captures the notion of the presence of interference and the ability of the cognitive network and cognitive subscriber units to adjust operating parameters as necessary to mitigate the effects of RF interference as well as improve noise-limited performance. In event 19, RF interference is caused by increased traffic occupying nearby frequencies that are close enough (in frequency and/or location) to public safety user communication channels to cause blockage and/or interference residue via leakage through the radio's filters.

7.4.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of subscriber units that must communicate when responding to the hazardous situation, but communications is hindered and even prevented by interference and network signal levels are weak for some users, which causes noticeable degradation in voice quality.
2. **Network**: The network is a typical public safety trunked radio system, consisting of one or more sites where base stations/repeaters are located, network backhaul data links from the sites, networking switching/routing to route radio communications from the source to destination communications devices (subscriber units, dispatch centers, etc.), and all network control and database peripherals. Base stations typically can sense when there is an excessive interference source and disable those channels (a brute force solution that reduces overall system capacity).
3. **Procedural**: The procedure for dealing with interference and poor voice quality due to weak signal is subscriber- and/or base station-centric. If a user's transmissions are not understandable, the user repeats the transmission and/or moves in the hope of getting better coverage. When base stations sense when there is an excessive interference source and disable those channels, this is typically transparent to the end user if other channels are available but it also affects access capacity and latency times. Roaming algorithms are also employed in radios so that the radio can "automatically" try communicating on alternate trunked sites if the received signal falls below a threshold and/or the received BER is excessive. For voice quality to improve, obviously there needs to be coverage overlap between network sites with robust link margins. A more "brute force" technique than roaming is for the radio operator to manually force his radio to use a different site, system, or even frequency band (rarely happens) in the hope that voice quality will improve.
4. **Regulatory:** The frequencies and waveforms that the subscribers and infrastructure are authorized to use in a given area are dictated by licensing.
5. **Chronological:** Depending on the severity of the interference, the trunked system response time can collapse into a gridlock condition since every repeated transmission represents additional traffic and additional traffic, in turn, further delays response time.

7.4.2 Capability Shortfall

In regards to interference-limited communications, today's trunked public safety base stations typically employ limited interference avoidance on the control channel, using a technique that is often termed "carrier detection". The carrier detection technique discriminates between wanted

and unwanted receive signals in the base station control channel receiver using the time domain characteristics of the signal envelope. Desired receive control channel signals originating from radios wishing to communicate with the station will be in short bursts (i.e., on for a short time, then off). If the base station receiver detects that a received signal does not exhibit this characteristic (e.g., it is long duration) and of sufficient level to interfere, it will shut down that channel and the control channel will revert (direct subscribers) to the next available channel.

Roaming algorithms, manually forcing an end users radio to access a different site, or even frequency band changes, as described in the Procedural entry in Section 5.4.1, do not provide high assurance that a weak signal power condition will be corrected. Roaming algorithms can have many thresholds that are often specific to the environment in which the radio operates, and these thresholds must be fine-tuned. Also, a radio operator who manually changes systems during deep fading situations may find that the signal "comes and goes" even after making his alternative signal source selection. As a result, he may find himself having to repeatedly change controls on his radio, thus causing distraction from his life-critical mission.

The current brute force, manual, and subscriber-centric methods of dealing with interference and weak signals are cumbersome, time consuming, spectrally inefficient to say the least, and they can even cause system instability and/or breakdown in severe cases. "Smarter", network-based solutions can improve spectral efficiency via intelligent, optimal, algorithms that can be automated.

7.4.3 Description of Use Case

The interference mitigation and link margin improvement techniques for Event 19 use the known location of both the subscriber units and interference sources, the subscriber units' desired data rate needs (e.g., voice, slow speed data, or high speed data), the subscriber units' priorities, and analytical prediction of the RF coverage to choose the following parameters for each subscriber based on a multi-dimensional coverage, priority, and traffic optimization:

- Transmit power
- Waveform (various bandwidths corresponding to different data rates)
- Frequency channel(s)
- Sites and systems
- Antenna parameters and/or configuration

The information is sent by the network via a control link to each radio and site. Each radio, in turn, adjusts its transmit and receive filters commensurate with optimality for the particular waveform, its power output is configured to be "just enough" for communications at the desired quality of service, its operating frequency set to be far enough away from other radios' communications channels to enable enhanced cancellation by its receiver filters, and its site and/or system if improved coverage is predicted with this alternate selection. Also, if adaptive and/or reconfigurable site and/or terminal antennas are employed, the parameters of such antennas may be changed or adaptively enabled to form a beam in the direction of the desired communications path and/or set a null on the direction of arrival of (a) received interference signals(s). The network also controls network access of each subscriber based on its priority relative to other subscribers.

If the location, bandwidth, power, and frequency of the interference is unknown this substantially increases the complexity of the multi-dimensional optimization, but techniques such as game theory may be applicable to help ensure desirable network behavior in light of the distributed control.[19]

Candidate techniques that can be prescribed by the network when dealing with interference include the following:

- Frequency agility—move the communications channels away from the frequencies where the effects of the interference are being observed
- Burn through—increase the power output of the subscriber units and/or use waveforms that can better tolerate the interference
- Coverage extension—set up an ad hoc network to reduce the ratio of communications range to interferer range, which achieves better signal to interference ratio.
- Subscriber receiver parameter modification—mitigate the effects of the interference by changing subscriber receiver parameters; if the interference is causing a blockage due to overload of the radio receiver, sometimes insertion of additional receiver attenuation will improve the signal to interference ratio.
- Antenna nulling—use site and/or terminal antennas that can place a null in the direction of the interfering signal, either adaptively or via external control.

Candidate techniques that can be prescribed by the network to deal with weak signals include the following:

- Power increase—increase the power output of the subscriber units (for terminal to base station limited situations)
- Waveform design—use waveforms that can better tolerate weak signals
- Coverage extension—set up an ad hoc network to "relay" the signal among closer spaced radios
- Subscriber receiver parameter modification—the optimum receiver configuration in noise-limited situations is typically not the same as for interference limited situations, so in noise-limited cases where adjacent channel interference is not a concern, some improvement in link margin can be afforded with a filter change. Also, even RF front end components of the subscriber radio could be controlled to enable more effective radio sensitivity at the expense of higher interference susceptibility.
- Antenna gain—use site and/or terminal antennas that can optimize gain in the desired direction of communication, either adaptively or via external control.

All of the techniques described in the above lists can be performed today, but require extensive human (manual) analysis. Cognitive radio capabilities can automate significant parts of the process, shortening the time required to execute performance improvement actions and reducing the burden on the humans in the loop. That is, much less time required for operators to react to

[19] James O. Neel: "Analysis and Design Of Cognitive Radio and Distributed Radio Resource Management Algorithms PHD Dissertation Virginia Tech September 2006

the situation; operating parameters could be optimized automatically; and automated monitoring of performance over time allows parameters to be adjusted automatically as well. With respect to the specific aspects of the scenario situation noted in Section 5.4.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets, except for potentially a more capable network processor to accommodate the network-based application that performs the processing algorithms.
2. **Network**: The existing network will be augmented with an application that implements interference mitigation and/or link margin improvement algorithm(s), and may require additional control interfaces from/to the subscriber units.
3. **Procedural**: Manual operations required with current technology would be replaced by reviewing (and approving as necessary) the reconfiguration steps taken by the cognitive-enabled network.
4. **Regulatory**: Radios are licensed to operate with more waveforms that have more varying bandwidths and data rates. Radios are also licensed to utilize frequencies allocated to other services under specified conditions.
5. **Chronological**: The time required to respond to interference and/or weak signals is reduced significantly.

7.4.3.1 Functional Capabilities

The functional capabilities required to realize this use case include the following

1. GPS in all subscriber units and communication of the position coordinates of each subscriber unit to the network application.
2. The ability of each subscriber unit to specify, to the network application, the subscriber units' data rate needs for its next transmission or message sequence.
3. The ability of each subscriber unit to rapidly change transmit power, waveforms, frequencies, filtering, and receiver attenuation based on commands sent over the network.
4. A network application that includes
    a. A coverage and interference model that can predict signal and interference levels at every potential end-user location.
    b. A CR algorithm that optimizes the following variables based on predicted signal and interference levels for all subscribers:
        - Transmit power
        - Waveform for communication (various bandwidths corresponding to different data rates)
        - Frequency channel(s) for communication
    c. Dynamically controllable access priority per subscriber unit

5. The ability to set up an ad hoc network[20]
6. Optional adaptive and/or externally controllable antennas for the sites and/or terminals that can place additional gain in the direction of the desired communications and/or nulls in the direction of interference sources.

7.4.3.2 Regulatory Implications

To enable the most "hooks" for improving performance, radios will likely have to be licensed to operate with the flexibility of using multiple waveforms that have more varying bandwidths and data rates. Also, if the cognitive algorithm is extended to "borrow" frequencies from other services this, of course, impacts regulatory procedures/certifications.

7.4.3.3 Policy Implications

The additional functionality of a cognitive network may allow some changes to existing policies and procedures to expedite the deployment of such devices in emergency situations.

7.4.4 Summary of Impact of Use Case

"Smarter", network-based solutions improve spectral efficiency via automated, intelligent, and more optimal algorithms.

7.5 Use Case 5: Reconfigurable RF Gateway Capability

In events 13 and 14 of the scenario, a situation arises in which it becomes necessary to establish a voice communications link between first responders and personnel that do not have access to first responder equipment. For example, tow truck operators need to coordinate their activities with incident command staff and to obtain personal protective equipment (PPE) so that they can go into a hot zone to remove vehicles that are blocking traffic routes that are needed by emergency vehicles.

In this use case, a reconfigurable repeater is deployed to link a frequency used by tow truck operators with a frequency used by the first responders. For ease of reference we refer to such a device as a Mode Agile Gateway Network Enabled Technology (MAGNET) in subsequent use case discussions.

7.5.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of tow truck operators whose activities must be coordinated within several elements of the response; they must be directed to locations to receive PPE; they must then be directed where to go to remove vehicles, etc. The area from which vehicles must be removed is within a hazardous material plume. The geographic area covered by the responders who need to be connected is generally the immediate area of the incident—an area of approximately 1 mile radius, requiring voice radio links back to the EOC.

[20] See Use Case 1, Section 4.3.1., "Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 1: Review of the 7 July Bombing of the London Underground," Report No. SDRF-07-P-0019-V1.0.0, 7 November 2007, available at www.sdrforum.org.

2. **Network**: The tow truck operators have legacy equipment that does not operate on public safety frequencies; thus they have no means for direct voice communication with first responders. With current technology, it is possible to deploy a programmable gateway device that could be used to establish the necessary communications link via channel audio bridging.
3. **Procedural**: Assuming the use of a programmable gateway device, the current procedures are for a Communications Unit Leader or other qualified individual to set up the device, determine the parameters of the channels to be connected, and establish the connection.
4. **Regulatory**: Two or more mobile or portable radio units are typically interconnected via an audio gateway bridging device, and these radio units actually provide access to RF channels. The regulations that apply to such radios are in force.
5. **Chronological:** The time required to set up and properly configure a programmable gateway device varies with the complexity of the RF environment, characteristics of the interconnected radio networks, and the experience of the gateway operator. While it is possible to set up and connect two radios in a matter of minutes, experience has indicated that it can take much longer to adjust parameters to ensure adequate quality in the communications.

7.5.2 Capability Shortfall

Using current technology, the typical approach to providing this gateway capability is to deploy a programmable gateway device that patches audio from a radio tuned to a communications frequency used by the tow trucks with audio from a radio tuned to frequency used by the first responders. The gateway manages all radio push to talk controls. There are several different products and approaches that are currently available, including:

- Mobile or fixed-site repeaters that simply retransmit incoming calls on a different outgoing channel.
- Dispatch console patches or audio linking devices (including IP-internetworking devices) that link channels of different radio systems. Such patches are generally permanent capabilities of the network infrastructure rather than capabilities that can be deployed at an incident.
- Intelligent gateway devices that allow a user to define which channels are to be linked together, and can support multiple simultaneous "conversations" through the device.

All of these approaches are characterized by the fact that a radio transmission on one channel must be rebroadcast on each other channel that is linked through the repeater/patch/gateway device.[21]

[21] We also recognize that with current technology it is also possible that an emergency management coordinator could contact individual tow trucks via commercial cell phone. While that is a feasible approach, it is difficult to broadcast information to all tow truck operators simultaneously, or for individual operators to be aware of what other trucks are doing, etc.

While such devices are employed extensively today and provide needed communications interoperability, field experience has indicated a number of challenges with the current technology:

- Such devices require personnel with extensive training to operate effectively.
- While set up can occur quickly, there are typically a number of parameters which must be adjusted to ensure effective operation at the time of activation. Determining the optimum parameters and adjusting them can be time-consuming, labor intensive, and potentially tie up valuable communications channels.
- Improperly deployed devices can have a severe detrimental effect on overall communications, and on resources associated with all interconnected networks.
- Mobile devices and supporting networks are susceptible to "parallel" links and loops if more than one gateway is active in an incident.
- All programming is manual; thus if changes need to be made to the gateway device to accommodate changing communications requirements, or changes in RF environment, the device parameters must be manually adjusted.

7.5.3 Description of Use Case

The concept of this use is a gateway device that functions much like current gateway devices, with three notable exceptions: (1) rather than plug existing radios into the device (as required by most current devices), the device has front end reconfigurable transceivers (radios) that can configure to the required frequencies, protocols, and other operating parameters, potentially eliminating the need to bridge at an audio level by bridging at a digital level or at an intermediate frequency ; (2) cognitive capabilities can determine how the radios need to be configured, and (3) the device can monitor ongoing communications to adjust operating parameters to maintain optimum quality of the communications links.

With respect to the specific aspects of the scenario situation noted in Section 5.5.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets. The cognitive-enabled reconfigurable device is deployed in the same manner as current devices.
2. **Network**: There is no change to the network. The cognitive-enabled reconfigurable device established the same network connectivity and the same users are connected as with current devices.
3. **Procedural**: Because of the greater capabilities of the cognitive-enabled device, some changes in the procedures are appropriate. In particular, manual operations required with current technology would be replaced by reviewing (and approving as necessary) the reconfiguration steps taken by the cognitive-enabled device.
4. **Regulatory**: The actual use of the communications channels does not change, so no regulatory changes are required for that aspect of the use case. However, the replacement of separate radios with a reconfigurable transmit/receive capability that is an integral part of the device would typically require that the device undergo the certification required of

other radios. This use case assumes that all use of communications frequencies falls within the bounds defined in the licenses for use of that frequency.

5. **Chronological**: The time required to properly deploy the gateway device is reduced significantly (from as long as several hours to a few minutes).

7.5.3.1 Functional capabilities

The functions required to realize this use case include the following:

1. Cognitive capabilities to identify operating parameters of communications links to be connected. Such operating parameters include, but are not limited to, frequency, bandwidth, PL tone, repeater hang time, repeater squelch tail, transmit power, etc.
2. Reconfigurable multiband radio modules that are components of the gateway device. Reconfigurable parameters include those listed above.
3. Elimination of the need to bridge at a baseband audio level by bridging at a digital level or at an intermediate frequency. Encrypted digital signals can be bridged without compromising transmission security at within the bridge, potentially allowing end-to-end encryption between compatible systems.
4. Cognitive capability to identify the degradation of performance, "ping pong effects" when bridging conventional repeaters, or situations in which a channel is "locked up" due to improper parameter setting, etc.
5. The ability to pass authentication and credential information from one system to another through the gateway. Note that procedures are defined in the P25 ISSI to accomplish this, but gateways linking non-P25 systems, and gateways which convert transmission to audio baseband do not have this capability.

There are a range of architectures for a MAGNET device. The majority of devices currently commercially available use an architecture in which radios are connected to the device, and generally switch audio at the baseband level, with some modifiable parameters to control some aspects of the transmit/receive functions. The cognitive functionality for such a device would monitor performance and modify these parameters. Alternative architectures can incorporate reconfigurable transceivers in the MAGNET itself, in which case the cognitive capabilities can control parameters in both the transceivers and the switching mechanism. Regardless of the architecture, the key required functions determine what reconfiguration options are available (whether they involve reconfiguring a radio connected to the device or a programmable transceiver embedded in the device) and what changes are appropriate to improve performance.

7.5.3.2 Regulatory Implications

A reconfigurable gateway device would include reconfigurable radios, designed to operate with specified parameters but able to be reconfigured as needed to replicate different capabilities. Thus the key regulatory issue is how the reconfigurable radio capabilities are certified.

7.5.3.3 Policy Implications

Most agencies have established, or are establishing, policies and procedures governing the use of gateway devices. Some policies may cover guidelines or rules defining the authority and circumstances under which such devices can be deployed, establishing rules for coordination

when such devices are to be deployed, and establishing the qualifications of device operators. Such policies and procedures would still be appropriate in this use case. The additional functionality of a cognitive-enabled reconfigurable gateway device may allow some changes to existing policies and procedures to expedite the deployment of such devices in emergency situations.

Also note that reconfigurable gateways are intended to provide communications capability among users that do not typically communicate with each other. It is important to ensure that where possible, users are trained in best communications practices (e.g., plain English) needed for efficient communication of information. In cases where disparate user groups must communicate in emergency situations for which they have not trained, a short list of guidelines should be available and quickly communicated to all users of a linked channel. For example, it is important for non-public safety personnel in such a situation to practice good radio discipline to avoid straining system capacity. Ensuring the ability for disparate user groups to communicate is not only a technical issue but also a training and operations issue.

Policies and procedures must also be established for authenticating users who are on a system that is linked via the MAGNET.

7.5.4 Summary of Impact of Use Case

The positive results of realizing this use case are as follows:

1. Such devices could be deployed with much less time required for the operator to interact with the device relative to current technology.
2. Operating parameters could be optimized automatically if device receive frequencies are known, in addition to the ability to identify transmit frequencies (i.e., the FCC Part 90VHF band does not use paired channels).
3. Automated monitoring of performance over time allows parameters to be adjusted automatically as well. Optimized operation would ensure that the communication link problems such as repeater interference problems, channel "lock ups", and interference, can be addressed in real-time rather than requiring manual intervention.

7.6 Use Case 6: Interface with non-first responders

In event 27 of the scenario, additional specialty agencies begin to arrive and their radios must be integrated into the networks. Of particular concern are the industrial firefighters brought in from outside the area (and for which there are no pre-existing aid agreements) to assist in controlling and extinguishing the fire. Audio patches (such as a reconfigurable gateway as described in Section 5.5) are configured for use by environmental health and safety agency personnel. We assume that the industrial firefighters' radios are state of the art and are automatically reconfigured to operate on Central City's network. The COML authorizes the additional agencies to access the Incident Area Network (IAN). The IAN automatically reconfigures its operation to accept the additional client units. Reconfiguration occurs in two ways;

- Reconfiguration of industrial firefighter radios that can be authenticated into the network. For radios that can be reconfigured to operate on the public safety network, those radios are reconfigured in accordance with the roles for which the firefighters are assigned; this

situation is similar to that described in Use Case 1 (Section 5.1), with the exception that the personnel in this case are not part of a first responder agency.

- Second, for health and safety agency personnel that cannot be directly authenticated to the network, and/or have radios that cannot be reconfigured to operate on the network, a MAGNET (see Section 5.5) is deployed to provide a gateway interconnecting those firefighters radios and the public safety radio system.

In both situations, the technical aspects of this use case are similar to Use Cases 1 and 5; however, the procedural and regulatory implications of this use case are different. In addition, since the industrial firefighters and health and safety personnel are not first responders, it is also critical that the network connections that allow them direct communications with first responders do not adversely impact the remainder of the communications capabilities being used by other incident response personnel.

7.6.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** There are a number of responders (Industrial Firefighters, Environmental Health, and Worker Safety) that must communicate on the IAN as they work in proximity to the incident area.
2. **Network**: Though the Industrial Firefighters are equipped with compatible public safety radios, they must work through the COML to be authorized on the system. Health and Safety personnel have legacy radios that do not have access to the public safety frequencies and thus have no direct access to First Responders. The COML authorizes use of the MAGNET system to allow Health and Safety personnel to be bridged onto the network.
3. **Procedural**: Two procedures are involved in this instance. First, for the Industrial Firefighters and the Health/Safety Personnel; assuming that the Industrial Firefighters have compatible radios, the process will be for the COML to get information on these radios so they can be authorized on the Central City Network. Assuming theses radios are standards based OTAP capable, the COML will load these radios with the correct template and the radios can be immediately used. Second, in the case of the health/safety personnel, the procedure is much like for the tow-truck; the COML will authorize the MAGNET system to configure itself to accommodate bridging in the Health/Safety personnel into appropriate talk groups as per ICS On-Scene Commander guidance.
4. **Regulatory:** The frequencies and waveforms that the subscribers and infrastructure are authorized to use in a given area are dictated by licensing. Non first responders cannot access public safety systems.
5. **Chronological:** Two separate timelines are involved. The first is the time required to set up and properly configure a MAGNET unit; the required time varies with the complexity of the RF environment and the experience of the operator. While it is possible to set up and bridge two radio systems in a matter of minutes, experience has indicated that it can take much longer to adjust parameters to ensure adequate quality in the communications. The alternative, in which non-first responders such as the Industrial Firefighters have radios that are compatible with public safety systems, is that the interface between first

responders and non-first responders could be accomplished with over the air programming once such action is authorized. In this case the reconfiguration timeline is on the order of a few minutes. (Note that in the latter case there is additional time required to add such users as authorized users to the system.)

7.6.2 Capability Shortfall

The capability shortfalls for this use case are identical to the shortfalls listed in Section 5.1.2 and Section 5.5.2.

7.6.3 Description of Use Case

The concept of this use case is twofold. The first is using OTAP to reconfigure the compatible (Industrial Firefighter) radios. The second is to utilize the previously mentioned MAGNET unit which: (1) rather than plug existing radios into the device, the device has front end reconfigurable radios that can configure to the required frequencies, protocols, and other operating parameters; and (2) cognitive capabilities to determine how the radios need to be configured.

7.6.3.1 Functional Capabilities

The functional capabilities required to realize this use case are those listed in Sections 5.1.3.1 and 5.5.3.1.

7.6.3.2 Regulatory Implications

The most significant regulatory implication is that this use case assumes that non-first responders will be transmitting on frequencies allocated for public safety service. While regulations may allow such communications in emergency situations, they may need to be modified to explicitly define the circumstances and appropriate authorizations that should be in place to ensure that such communications is available when needed while not adversely impacting other first responder communications.

7.6.3.3 Policy Implications

Policies and procedures may need to be defined to outline agency rules on the circumstances under which non-first responders can communicate on first responder networks, policies and procedures for authorization and authentication, and policies and procedures for how agency communications assets may be configured to accommodate interface to non-first responders.

7.6.4 Summary of Impact of Use Case

In certain circumstances, such as the ones outlined in the scenario, direct communications between first responders and non-first responders provides more efficient and effective communications. Relaying messages through dispatchers, as an alternative, is subject to errors, takes valuable time, and involves the time and attention of another person (the dispatcher). Other alternatives (such as assigning a liaison officer to work with the non-first responders) require additional personnel for relaying messages rather than performing a more direct incident response task. While the public safety community justifiably is wary of untrained non-first responder use of valuable first responder communications assets, under the appropriate circumstances this use case can provide critical, timely communication that maximizes the support provided by non-first responders.

7.7 Use Case 7: Revert to Previous State

Radio users reconfigure their radios to return to their default home template. As the loading on the voice network lessens, the voice network releases channels back to Metropolis and restrictions on FDMA users are removed from the radio system. The IAN continues to reconfigure itself as responders stand down, units move and leave the network, until there are no more units left to communicate. The broadband network continues to automatically reconfigure itself until utilization drops below specified thresholds. Once below the threshold the network returns to normal operation. A conventional repeater is on site which is able to receive and transmit on multiple frequencies at the same time. The repeater automatically senses the RF environment and allows the COML to create groups of uses through that repeater.

This cognitive capability could reside with the infrastructure, within the radio, or both. If in the infrastructure then the radio would have to be capable of providing this data to the network before it is reprogrammed. If a part of the radio the user might have to tell or configure the radio to save its current state and programming so that it can be restored later.

7.7.1 Summary of Scenario Situation

In terms of the aspects of the public safety communications environment:

1. **Physical:** As first responders arrive at the incident (and throughout the course of the incident), their radios are reconfigured to meet incident needs. The first responders are physically distributed throughout the incident area, including evacuation areas and perimeter control areas removed from the actual chemical plant where the initial explosion occurs. Two potential rollback applications: at some point in the scenario, a reconfiguration of the system (network and subscriber radios) results in a degraded communications capability, therefore these configurations must be restored to their previous state (Use Case 7a). Later, when the first responders are released from the incident, prior to departing for their home jurisdictions, which may be hundreds of miles from the incident, their radios should be normalized , or “rolled back” to a pre- incident, or “home” configuration (Use Case 7b).
2. **Network**: The first responders are linked to the network as needed to support the incident response. At one point the network and subscriber radios are reconfigured, and the result is a degradation of communications capabilities. To resolve this condition, the previous configuration must be restored. Later, some first responders are released from the incident and as they depart their radios are disconnected from the network.
3. **Procedural**: At some point in the scenario the procedure for reconfiguring some element of the communication system (network and subscriber devices) is executed. The result is that communications are degraded.
4. **Regulatory:** The regulations that govern commands for reconfiguration (see Section 5.1.1) apply to this use case.
5. **Chronological:** Current capabilities do not provide simple approaches to systemically roll back changes to configurations. Thus the timeline requires manual review of the communications situation and execution of reconfiguration commands to restore a previous configuration.

7.7.2 Capability Shortfall

For the situation in which a reconfiguration needs to be rolled back, networks and subscriber devices may maintain a configuration history which allows previous configurations to be restored. However, rolling back a configuration change that involves the network and subscriber equipment is not typically automated in current systems. Thus changes which turn out to have a negative impact on communication can only be reversed by manually resetting software configurations installed in the network and in subscriber equipment.

In the case of restoring default or home agency configurations as a responder is released from an incident, the most significant shortfall is associated with radios which cannot be reconfigured over the air. Reprogramming radios that must be tethered to programming hardware can take a significant amount of time (days or weeks) due to the logistics of transporting radios to where they can be reprogrammed. Radio security is not discussed here, but some LMR manufacturers require use of special hardware or software keys prior to accessing radio configuration functions.

7.7.3 Description of Use Case

With respect to the specific aspects of the scenario situation noted in Section 5.7.1, this use case would result in the following:

1. **Physical**: There is no change to the physical deployment of assets.
2. **Network**: Once a network operator or COML issues the appropriate command, the network automatically restores the previous, or home, configuration of the network and the subscriber radios.
3. **Procedural**: A procedure must be in place to determine when a reconfiguration results in degraded communication. This could be an automated process but would logically include some human oversight to avoid unnecessary configuration changes. For visiting users providing mutual aid, the "home configuration" must be stored in the network or on the radio unit itself, for later recall and activation, prior to departing the incident scene. This "image" could be encrypted prior to storage to protect the integrity of the home network, making it unreadable by incident personnel, or to provide a capability to bypass home network security keys. This will also provide significant cost savings for home network personnel.
4. **Regulatory**: No specific regulatory changes are needed to implement the concept of reverting back to a previous state. Some standardization of appropriate messages may be necessary to maintain interoperability in a multi-vendor or multi-model environment.
5. **Chronological**: The time required to reconfigure network equipment, or to rollback a reconfiguration, can be significant if the process is not automated. It can also be a time consuming process to restore subscriber equipment to default or home jurisdiction configurations after the radios have been reconfigured to support an incident response outside of the agency's home jurisdiction. Much of the time in this situation is based on tethering radios physically to programming hardware, a process that can be eliminated with over the air reconfiguration.

7.7.3.1 Functional Capabilities

The functions required to realize this use case include the following:

1. The ability to recognize when a reconfiguration process results in a degraded communications condition. Note that the process of determining that such a condition exists could be entirely manual (i.e., strictly based on the reaction of users or observations of a network operator or COML staff). However, given a capability in which subscribers can report RF information to the network (see Section 5.4), it is also possible that a cognitive capability within the network could monitor RF information and configuration changes to correlate changes in system capabilities and effectiveness of configuration changes. Such information could be analyzed over time to develop more effective configuration options (a "learning" capability) or at least alert a human operator if communications capabilities degrade following a configuration change.
2. The ability to retrieve and securely store prior configuration information.
3. The ability to restore a configuration.
4. The protocols and algorithms to ensure that all radios rollback the correct known and valid prior configuration.
5. The ability to securely return network equipment to a default configuration, via over the air command or reprogramming.

7.7.3.2 Regulatory Implications

No specific regulatory changes are needed to implement the concept of reverting back to a previous state. Some standardization of appropriate reconfiguration messages may be necessary to maintain interoperability in a multi-vendor or multi-model environment.

7.7.3.3 Policy Implications

There are a number of policies and procedures that are required to realize this use case. This use case assumes some level of human oversight into execution of reconfiguration and rollback commands, so the policies and procedures must be put in place to address the following:

- Under what circumstances is a rollback decision made?
- Who has the authority to order a roll back to previous state?

7.7.4 Summary of Impact

Many of the use cases discussed in this document involve reconfiguration of the network and/or reconfiguration of subscriber devices. While thorough analysis, careful implementation, and rigorous testing are mandatory prior to any deployment of such capabilities, the unpredictable nature of real-time incident response means that it is necessary to have contingencies in place, should the outcome of network equipment and/or system reconfiguration not provide the desired or expected results. In such cases it is necessary to return the equipment and/or system back to a known working state as quickly as possible. Current systems do not provide the tools to systematically reverse a sequence of reconfigurations among network and subscriber devices. This use case simplifies this process by providing capabilities to restore a previous configuration as needed.

7.8 Use Case 8: Cognitive Sensor Network

Discussion of sensor input arises in events 6 and 26 of the scenario. Consideration is also given to vehicular traffic in events 13 and 14.

The primary legacy source of automated sensor data is in the personal protective equipment (PPE) worn by firefighters entering the hazardous area. Other related information is typically relayed over voice channels. In exploring the benefits of cognitive capabilities to more effectively respond to this type of situation, we will address additional sources of sensor data, consider how information from them is delivered to IC, and how it is used in the response.

7.8.1 Summary of Scenario Situation

1. **Physical:** A facility with substantial quantities of flammable and potentially toxic chemicals has experienced an explosion and fire, and the situation is out of control. There are two categories of hazards at the site. The first set is associated with physical hazards to personnel entering the area to deal with the fire. The other hazard is presented by a toxic plume emanating from the scene that threatens the nearby population and facilities. Some aspects of these problems can be determined by observation, but others, such as carbon monoxide are invisible, and require sensors to ascertain the level of toxicity. In the described scenario, the primary source of sensor data is from sensors in the protective equipment worn by firefighters. That data relates primarily to the onsite problem, and does not deal adequately with the larger toxic plume that extends beyond the plant location.
2. **Network**: Part of the gear carried into the fire consists of radio equipment providing communications support between IC and other first responders via the trunked radio network. The sensors also generate traffic that requires bandwidth on the IAN for delivery to incident command. Each data radio connects directly to a common central unit. As more firefighters are deployed, sensor traffic increases creating a congestion problem both from the quantity of data generated and the loss of effective bandwidth due to contention for channel time.
3. **Procedural**: Firefighters control when they transmit on voice channels, and can respond to congestion by reducing the number of transmissions and their length. Autonomous uncoordinated sensors, however, are not directly controlled, and lead to channel congestion, with some information that is ultimately redundant.
4. **Regulatory:** Spectrum is assigned to public safety operations, but additional channel capacity may be required to handle the increasing volume of data and voice traffic. There are no unresolved regulatory issues.
5. **Chronological:** During the initial phases of the incident, any issues with hazardous conditions are unknown. Initial notification of a specific hazard is critically important, but repeated messages reporting no change in the situation are redundant, and wasteful of bandwidth. Once existence of a hazard is known, then changes in its intensity or location become relevant.

7.8.2 Capability Shortfall

There are three significant areas of shortfall that can be alleviated by improved system design and application of enhanced information technology. One is inadequacy, or lack of, of available

sensor information. Legacy operations depend largely on facilities that responders bring to the scene, and do not take full advantage of supplementary information sources.

Another shortfall is congestion in the communication systems, caused by delivery of information by individual sensors operating independently, and without a coordinated priority structure. This problem can be alleviated by coordination between on-scene CR terminals that cooperate at the data source to avoid data transmission that is irrelevant or redundant.

The third shortfall is onsite information overload on the part of the response team. Both the processing and presentation of available sensor data should provide all needed information in a form that is easy to understand. For example, an on-screen map of the factory, with color-coded symbols to display the hazard level in different areas, is more readily assimilated than a printed list of coordinated and raw sensor data.

7.8.2.1 Supplementary Sources of Sensor Data

The following are additional sources of sensor data that have potential to be processed to enhance overall situational awareness.

A. **Personal Protective Equipment Mounted Supplemental Sensors.** Existing PPE resources provide data from sensors, including life signs data about the wearer and information about ambient conditions, such as air temperature and carbon monoxide levels. To supplement sensors mounted directly on individuals, devices called "pebbles" or "motes" can be placed in the environment. These small radio-equipped devices are dropped at various locations along the path of response both to provide extra sensor data and also augment the communications network.

B. Building Mechanical and Emergency Systems. Buildings are equipped with systems to provide heating and cooling. Those systems have sensor networks with sensors located throughout the building, and the resulting data is used to control building air flow and temperature. The buildings also have emergency system sensors that detect over-temperature conditions, sound alarms, close fire doors, and activate sprinklers. All of these facilities are normally managed via a sensor management or telemetry system centrally within the building, but this control function can often be redirected to external facilities during the emergency[22]. Sensor power is normally provided via the building power system, but critical sensors can be equipped with battery backup. Data from these sensors can be redirected from the building management system to incident management and/or individual first responders by cable or a local RF network.

C. Environmental Measurement Facilities. The US Weather Service has an extensive network of devices that provide meteorological data on a continuous basis. It also provides current weather data summaries and forecasts to predict future weather conditions. The service tracks frontal movement, information that could be used to predict wind shifts that will affect smoke and toxic plume clouds around the scene of an emergency. Additional environmental information is available from other local sources, such as airports and sewage treatment facilities.

[22] See Alan Vinh, Computer-based Monitoring for Decision Support Systems and Disaster Preparedness in Buildings, IMETI Proceedings, June 2008, Orlando, FL

D. Video Cameras. Video from privately owned and municipal cameras can be used to enhance situational awareness. Due to the amount of information available, video feeds would be recorded at the Emergency Operations Center (EOC), a permanent central site, and edited to select the most relevant footage. The resulting clips are made available to units on the scene when relevant or on demand. Edited and tailored time-lapse information about a plume is an example of preparing video information for maximum effectiveness.

E. Commercial Digital TV. With conversion to Digital TV, commercial stations have a 20 MB pipe, more capacity than is needed to deliver their primary program material. With high-powered licensed transmitters these stations have excellent coverage. In an effort to provide additional services, the TV broadcast industry is looking for business cases where a revenue stream can be derived from broadcast of data. Transmission of video content or advertising directly to cell phones, based on geolocation, is a commercial version of this capability.

For Public Safety, this data stream can supplement dedicated channels for delivery of information from government agencies and other sources. Local municipal or remote FEMA command posts, for example, might use such a channel to download lower-priority but relevant data that might overload busy lower-capacity dedicated channels.

Commercial TV stations are also generating video relevant to certain types of disasters for use in their news broadcasting, via feeds from cameras located in news helicopters, for example. Their broadcast data sub-channel is a potential way that information, supplementing the video feeds mentioned in D. above, could be delivered.

F. Cellular System Traffic Information. The incident generates variations from the normal call traffic patterns as indicated by call volume data and the pattern of hand-offs between cell sites. Geolocation data can be obtained via mobile phones equipped with GPS capability or by triangulation from network base station antennas. This information is used to determine where people with active cell phones are located and to derive traffic patterns in the vicinity of the incident.

G. Intelligent Traffic Systems. ITS Cognitive Radios in vehicles, and infrastructure associated with highway automation systems serve as sensors for traffic flow information used by Incident Management personnel, including routing of emergency vehicles to the scene. Conversely, information from the incident is used by the highway system to warn drivers and to divert traffic around congested or dangerous roadways.[23]

7.8.2.2 Information overload

When a small number of sensors are active in a given area, routine network query and sensor response data volumes will be small, and channel contention will not present a problem. Both sensor network message volume and network contention will increase issues as data collected

[23] This is an interesting example of system interaction. Two independent systems, developed without a requirement to coordinate, link up and work together to satisfy needs of both DOT for highway management and PS in responding to the incident. Upon conclusion of the event they will disconnect and resume independent operation.

from sensors and sensor query activity levels increase while network resources remain constant, significantly more so if conditions trigger transmission of asynchronous alarm data.

In a simple implementation, sensors will repeatedly transmit their current readings to the central system, asynchronously or in response to a system query. A large number of messages with negative reports may not represent useful data. When some pre-defined level of a sensed parameter is detected, that change in status becomes useful information. For example, if a significant number of individual sensors mounted in responder PPE which are located are in close proximity to each other, they may all contend for channel capacity to transmit redundant information, all reporting the same condition.

The solution lies in coordinating information delivery to minimize channel contention. It is also useful to vary reporting intervals to minimize redundant information, while reporting often enough to establish that connectivity has not been lost.

7.8.3 Description of Use Case

This Use Case involves both inclusion of additional sensors as supplementary sources of data, and management of the resulting information. Networks, communication facilities, and operating procedures are modified to encompass the seven sources of information described in Section 5.8.2.1. Activities in the Central City EOC are brought into the scenario.

This Use Case treats the two components of "Cognitive Radio" independently. Cognition is composed of information processing, decision making, and policy execution delegated to the system. Radio is delivery of data of all kinds over wireless links. The Use Case does not confine itself to cognitive functionality implemented in the same box as the RF components: that functionality can be accomplished anywhere in the system. With efficient communication links, data can be processed locally, or sent to remote sites and the results returned with minimal delay.

The following aspects of the scenario situation noted in Section 5.8.1 describe this Use Case:

1. **Physical**: The physical aspect of the scenario is essentially the same as described is 1.1.1., with the addition of traffic sensing as indicated in items F. and G. Some additional equipment, including additional radios and the pebbles, is added. Activities, particularly handling video information, in the Central City EOC result in its inclusion in facilities involved.

   It is of particular interest that significant improvements in capability and performance are realized by the addition of CR functionality with minor physical modifications.

2. **Network**: Network changes to implement enhanced sensor capability are as follows.

   A. Sensor communication facilities in individual PPE equipment interact to form an ad hoc network. This net reduces contention, and improves connectivity. In addition, the pebbles dropped by firefighters on their path into the scene contain radios that enhance network connectivity and also provide additional sensors.

   B. Building HVAC systems are designed to accommodate an interface with emergency services. A building control diagram is maintained in the municipal emergency information database, and the building network can be accessed for emergency control of

the facility. Primary connection to the building network is IP through the commercial service provider data facility, with local wireless backup via unlicensed spectrum.

Individual sensors in the facility connect with the building control room through a wireless local net. Security information needed to access that network is also available to the emergency crew so that sensors can be read out even though the central site is not functional due to the emergency.

C. Meteorological data is important is cases where wind velocity and air temperature influence the plume emitted from the site. The US Weather Service offers a special service for Public Safety use where local weather conditions and forecasts are available for specific locations. The specific location for which information is needed can be obtained from the emergency database, or read from an onsite GPS receiver. In this scenario, the wind shift in Event 32 is forecast. Delivery of this weather information to IC occurs over a DTV data sub-channel from a local TV station.

D. Central City has a number of video cameras available throughout the city. During an emergency these cameras can be controlled from the City EOC to provide relevant incident information, such as information to IC for traffic congestion and plume tracking. Due to the vast amount of footage generated, the video streams are all digitally recorded for computer storage. A feed directly to IC can be provided. Alternately, EOC personnel are trained in both interpreting pictures and editing time-lapse clips which are then transmitted to the IC location.

E. As previously mentioned, commercial TV stations can provide data sub-channels on a contractual basis for emergency use. They also frequently have video feeds transmitted from remote units and helicopters. These feeds are relayed to the EOC to supplement broadcast reporting with additional footage.

F. Commercial Service Providers operate the familiar cellular Telephone service. The structure of their protocols provides geolocation from base station sector directionality, or in some cases, by GPS coordinates derived within the call phone or mobile units. As highway coverage is an important revenue source, the cellular providers have good coverage in high-density traffic areas. The resulting data has a characteristic pattern of sector utilization and hand-off that changes when traffic disruption occurs. When traffic is congested or blocked, the resulting data can be analyzed and overlaid on local GIS data to assist in dealing with the vehicular congestion described in Event 13. Delivery of that information is over the carrier's existing data service connection.

G. Connection between the city EOC and ITS will be by landline. Relevant data is then forwarded to the incident command post by their RF link. Intelligent Transportation System (ITS) support data for emergency vehicles in movement is transmitted direct between the vehicle and the ITS infrastructure; emergency vehicle priority in the ITS system supplements Code 3 operation.

3. **Procedural**: Procedures for incident management vary significantly as incident commanders tailor response to local conditions. As additional sensor output is provided, there is danger of data overload both in terms of overwhelming the communications resources and in overloading the human decision makers. Data processing facilities in IC, supplemented by those in EOC, reduce the data load by eliminating redundant or

unchanging information reports, and by well-designed data presentation on computer displays. Training in display management for IC personnel is needed to optimize decision-making.

The sensor data stream is in parallel with voice communication. Legacy operating procedures may need to be extended to ensure that all personnel have the same context for understanding full implications of information derived from sensors.

With access to data transmitted from sensors located in responder PPE, and facility mechanical systems, commanders can warn firefighters where toxic or over-temperature conditions occur. For example building fan controls can be used to reduce oxygen delivery or control air pressure within parts of a structure.

Availability of significant amounts of visual information from video footage enhances understanding of the scene, but also presents a problem of viewing time required. The addition of video backup and storage in the better-equipped and environmentally controlled city EOC partially addresses the need to immediately analyze real-time video with a high information density. It does introduce the need for on-scene personnel to request images of specific areas or events. Protocols must be established for its delivery to the scene with the video, plus contextual and interpretive information so there is no confusion about what the images are showing.

4. **Regulatory**: Regulatory agencies are sensitive to the needs of PS agencies, and a number of actions are being proposed and implemented. Priority access to commercial capacity can be required to accommodate emergency response traffic. 700 MHz or 4.9GHz FCC licenses in the US can provide needed bandwidth and useful air interfaces with appropriate priority structures. Unlicensed operation in Whitespace TV spectrum can also support a number of applications for emergency response.
5. **Chronological**: Availability of sensor data might help reduce the need for a change in evacuation in Event 32. Otherwise, the timeline is not changed.

1.1.1.1 Functional Capabilities

Functions include the following:

- Enhancement of cognitive radio functionality to improve PS systems and within systems that are sources of data to automate handling of the significantly increased traffic volume.
- Enhancement of PPE sensors, ad-hoc networking, pebble technology supplementing the incident area network, monitoring software in IC with cognitive tools to provide an effective display of current conditions and generate appropriate alarms.
- Prior planning with building personnel to establish details of connection to the building management and mechanical systems, and provisions for taking control.
- Process to monitor weather information continually in the city EOC, and procedures/standards that specify information format when it is relayed to IC.
- Video feed from traffic control center to EOC. Training for personnel to determine procedures/standards that specify what images & video information are needed, and what format is used when it is relayed to IC.

7.8.3.1 Regulatory Implications

Most of the communications described in this Use Case will involve use of spectrum that is already licensed. Permission may be needed for TV band use. Regulatory action may be needed to provide additional spectrum to construct networks with adequate bandwidth.

7.8.3.2 Policy Implications

In some cases PS planning is completed with the assumption that every resource utilized is brought to the scene by first responders, and controlled by them. Some of the items described above, in *5.8.3.1, Functional Capabilities*, may require changes in policies and procedures. For example, this use case would require:

- Accepted agreement with TV stations as to what services will be provided, technical details of channels to be used, and integration of that information into incident response equipment, procedures, and training.
- Accepted agreement with cellular service providers as to exactly what call traffic data can be made available, and in what format. Capture of that real-time data is a function of cognitive functionality within the cellular infrastructure. Provisions for protection of data, ensuring the privacy of individual callers must be addressed.
- Agreement must be reached between PS and DOT authorities as to what ITS traffic information will be exchanged and the formats to be used. Incorporation of CR capability in both systems to automate as much as possible of the information exchange process, and to define policies for its use. Training for control of the two systems when they are connected and procedures for disconnecting the systems.

7.8.4 Summary of Impact of Use Case

This Use Case describes a number of opportunities to enhance sensor information available during an incident. These capabilities are relatively independent; application of any of them has potential to improve operations. The case also identifies potential problems that may arise as a result of the sheer volume of data available. Cognitive Radios, and cognitive functionality in other areas of the system, can be of great assistance in reducing the volume of information transferred over the network and also increase its relevance for recipients.

An important consideration is how much of the decision space can be stated as policy, and delegated to cognitive functionality for execution. Insufficient delegation leads to individual overload, while too much delegation can result in inadequate control under unusual circumstances. Another consideration is the human-machine interface. Users must be able to vary the level of control they want to retain, and the information they want to see must be in a form to facilitate decisions to be made.

Facilities such as we have described can provide better projections, and reduce the likelihood of unexpected developments. That, in turn, permits first responders and commanders to be more proactive and less reactive.

8 Appendix: Utilization Challenges

8.1 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 Spectrum Trust (PSST) for the broadband network define a higher tolerance to network downtime than have traditionally been engineered into commercial systems.[24] 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

[24] 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.

progressively higher levels of efficiency and capacity as user requirements are progressively relaxed. This relationship is highlighted in Figure 1.

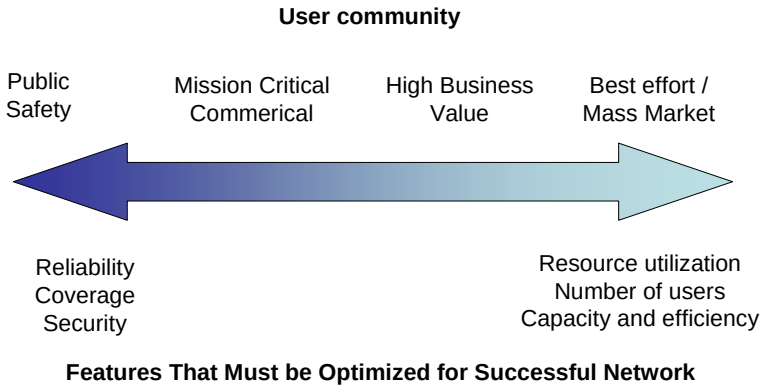

Figure 2. Divergent Requirements on a Public/Private Shared Network

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[25] 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.

[25] 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.

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 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.[26]

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

[26] 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.)[27]

Table 6, 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[28]
	Intelligent transmit power control
	Adaptive beamforming
Link Budget Improvement	Flexible mode-dependent receiver filtering
	Reconfigurable radios to support coverage extension [29]
	Dynamically adaptable modulation
	CR-based mesh networks for coverage extension[30]
	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.

[27] 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.

[28] including avoidance of "near-far" interference situations

[29] SDR enables radio reconfiguration to mesh

[30] 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.[31] 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

[31] 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[32] 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 uses predominately "one-to-many" (i.e. group) calls that would require forming several simultaneous beams.

[32] 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.

8.2 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."[33] 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

[33] 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.

8.3 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."

8.3.1 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.

8.3.2 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[34] 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 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 adaptive 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:

[34] 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.[35] 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.

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

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[36], dynamic prioritization 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[37] provides more detail on different approaches that could be followed for the assignment and management of the role-based priority assignments.

8.3.3 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

[36] 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.
[37] 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.

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."

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 policy.
5. Existing radio system talk groups and licensed channels.
6. Prioritization of use. Policies 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.

8.3.4 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,[38] 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 systems 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.

[38] 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.

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 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.

8.4 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.

8.5 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.