# Elements of Context for Cognitive Radio Based Public Safety Communications Systems

## Document WINNF-16-P-0019

Version 1.0.1
22 May 2016

## TERMS, CONDITIONS & NOTICES

This document has been prepared by the Public Safety Special Interest Group to assist The Software Defined Radio Forum Inc. doing business as (d/b/a) The Wireless Innovation Forum (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 It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Public Safety Special Interest Group.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 move to broadband data and the attendant explosion of information available to first responders has accelerated the need to manage sensors, data collected, and networks that deliver it; but effective and efficient management of data and networks requires an understanding of the context of the data to provide present and future operational information useful to the command structure. Having needed information readily available in manageable volume and easily understood format will enhance overall performance of response teams.

Some broad trends are visible:

- An increase in the complexity of incidents
- An increase in the availability of sensors to provide more information
- An increase in the information that is flowing into the Emergency Operations Center (EOC)
- An increase in the bandwidth of the communications channels available to the first responder in the field
- The desire to catalog and manage the flood of information that is now available, often in real time
- A coupling of the incident with big-data analysis to obtain additional information that may not be directly provided by the incident, such as trend forecasting
- A need to determine and control the extent to which information can flow into and from the field
- A need to find suitable wireless and backbone network capacity to send the information to the field
- The requirement of managing several individual networks, and even aggregating networks to provide the necessary communications bandwidth
- The need to automate the setup and provisioning of equipment in the field to reduce the burden on the first responder, who would rather focus on his life-saving mission
- The need for reconfiguration of devices, networks, and their deployment as the need arises, or to forecast and continue information flow. This could be ideally done autonomously, but may need supervision, at least initially

The implications of these trends include a need to broaden the capability of the Communications Leader (COML) function, as defined in the National Incident Management System (NIMS) to include broadband communications and its integration with Land Mobile Radio (LMR).

Additionally, the need to manage the flood of information that that could hit answering services, such as the Public Safety Answering Point (PSAP) with the deployment of advanced 911 services, such as the Next Generation 9-1-1 initiative also introduce requirements for for an information manager (INFO-M) at the Emergency Operations Center (EOC) or dispatch center. This is a new position that has not been part of traditional incident command structure.

These trends, if managed properly, could have the beneficial effects of helping first responders focus on the mission at hand, rather than how to connect to the right data sources, and also enhance their personal safety. The communications network(s) will need to adapt to enable these goals.

These goals are served by the development of context aware cognitive radio and communications networks, which facilitate reconfiguration of communications parameters and networks; this reconfiguration of parameters will also assist in forecasting the need for, and bringing in, assets as needed to accomplish the mission.

This report identifies several elements of context which can be useful for public safety communications and suggests ways in which these elements can be used.

This report also recommends that the elements of information identified in this report be examined as context inputs and new concepts of operation (CONOPS) be defined as to how they can be used to enhance and continue to the mission of managing major as well as routine incidents. These CONOPS can guide the implementation of context-driven actions in the devices and networks to facilitate the work of the first responder.

A major problem that still needs to be addressed is the standardization of the presentation of context information so that it can be used by multiple context aware networks and systems. Some of the elements of context that are identified in this report could form the basis of that standardization of efforts to present and even derive context.

Additional considerations, such as network and information security, which are outside the scope of this document, must also be included in the deployment of context aware cognitive radio systems.

# Contributors

Member Representatives

| | |
|---|---|
| Ihsan Akbar | Harris Corporation |
| Daniel Devasirvatham | Idaho National Laboratory |
| James Neel | Federated Wireless |

Other Subject Matter Experts

| | |
|---|---|
| Peter Cook | Peter G. Cook Consultancy |
| Bruce Fette | DARPA |
| Fred Frantz | Engility Corporation |
| Phil Harris | Engility Corporation |
| Steven Hope | DOCOBO |
| Ken Klassen | RCMP, Canada |
| Ken Link | SHP, NC |
| Al Sadowski | State of North Carolina |

## Acknowledgements

Our thanks to Ms. Mandi Peters, Idaho National Laboratory, for her editorial insight and support.

# Elements of Context for Cognitive Radio Based Public Safety Communications Systems

## 1 Overview

### 1.1 The Landscape

As public safety communications begin to move beyond the traditional Land Mobile Radio (LMR) to broadband communications, the task of providing appropriate communications to the first responder has become ever more complex. The use of LMR systems for public safety evolved and formalized the position of the communications leader (COML) in the National Incident Management System/Incident Command System (NIMS/ICS) protocol. The COML planned frequencies and talk groups in order to maintain the most appropriate level of communications channels to meet the tasks at hand, while maintaining sufficient capacity to support emergency calls if needed when a first responder got into distress. Unlike LMR, a cellular broadband system does not require the user to perform the channel allocation function; though operational resources such as priorities and talk groups may need to be managed. It provides, instead, a suitable communications pathway using available resources. If the capacity of the system is exceeded, voice path requests could return a busy signal. Data could still be moved through, but may experience holds and delays until sufficient capacity is available to transmit the data.

The user, today, sees his terminal less and less as part of a specific system, but more as an information gateway. It does not really matter to the user what mechanisms were used to transport the data; the underlying detail and complexity are of little or no interest to the user. However, there are a number of circumstances which could still overload the network–need for bandwidth intensive data such as high definition video for remote triage or ordnance disposal; large numbers of users in a compact response area; competing priorities, and data requests. This will be compounded by undisciplined use. Hence, avoiding or minimizing service degradation will require an expansion in the role of the COML to manage the information flow in the field network and to keep the quality of service and response acceptable, prioritizing those needs across multiple users, disciplines, functions, networks, etc.. The name COM-B, or COMB, has been proposed for a communications leader with broadband training.  While it may be important to distinguish training for operational purposes, this report will continue to refer to a COML to denote a communications leader with the appropriate training for operating with LMR or broadband, as appropriate. In addition, discipline of use and integration of resources, i.e., concepts of operation (CONOPS), need to evolve to make maximum use of available resources and meet the task at hand. This is similar to Standard Operating Procedures (SOP) and Memoranda of Understanding (MOU) in the LMR world.

It is also expected that the complexity of the first responder’s mission will continue to grow as the potential information available explodes with the availability of broadband, sensors and applications. The first responder still needs to execute traditional tasks, such as fighting fires, apprehending suspects, rescuing the stranded, etc.[1], without being overloaded by data. Hence, the information presented to the first responder needs to be managed and offered in a form that is easily comprehended and usable in the field within the press of the moment. This approach also calls for strong and appropriate human-machine interfaces (HMI) in the field. Additionally, a new role for information management, an INFO-M, may need to be added to the incidence response team, at the emergency operations center, to take care of this broadband information management function.

As first responders focus more on their life saving tasks and less on the details of the communications, and as the intelligence and capabilities of the network improves, it is now also thought that the network, itself, could assist the first responders and communications managers by either suggesting or taking care of some details of network setup, configuration, and future resource planning as the mission evolves. This automated assistance forms the link to cognitive capabilities of the network.

Finally, some of these functions could evolve as networks evolve. Deployment of the technology could be costly. However, it is thought that the savings in operational costs and the benefits of more effective performance could be significant.

## 1.2 The Role of FirstNet

In order to meet or stimulate new broadband uses for public safety, the U.S. Congress created the First Responder Network Authority (FirstNet) to deploy a national public safety broadband network (NPSBN). The charter for FirstNet is found in Title 6 of the Middle Class Tax Relief Act of 2012. Congress also allocated spectrum for this purpose in Band Class 14 in the 700 MHz band. While the architecture of the network is still evolving, the mandates and requirements of the act place heavy demands on FirstNet. Hence, as part of its evolving strategy, FirstNet, using a Statement of Objectives (SOO) based RFP released in January 2016, seeks to contract with an entity to provide the national Long Term Evolution (LTE) core and statewide Radio Access Networks (RAN). Commercial LTE operators are also being engaged to provide support for public safety communications in their networks. In the U.S., the deployment of FirstNet and dedicated broadband channels for public safety are expected to enable high data rate applications to the public safety community utilizing LTE, especially where there is coverage in its own dedicated band. Keeping in mind the demands from public safety and requirements set forth by the Department of Commerce (DoC), which oversees FirstNet, commercial LTE operators have started working to support public safety communications through the FirstNet initiative by considering co-locating Band 14 RAN equipment in their towers. FirstNet is also expected to depend on commercial coverage, where needed, throughout its life cycle. This dependency gives rise to interesting use-cases on how public safety would be accommodated on these networks, since public safety has much stricter requirements including spectrum availability, reliability, latency, resiliency, hardening, etc., as well as the need for priority and pre-emption.

FirstNet also requires LTE to support Device-to-Device or User-Equipment-to-User-Equipment (D2D or UE2UE) communications not only while in-network but also out-of-network coverage. The resource allocation for in-network coverage, bandwidth in a high traffic situation, and out-of-network coverage needs to be planned on-the-fly. Allocation also requires several contextual components that need to be evaluated in order to provide reliable service to the public safety personnel while minimizing the degradation of the service overall. Prioritizing public safety communications is a challenging task, and it is expected that these tools/techniques can help resolve this issue.

LTE's D2D communications specifically address public safety needs through applications such as Proximity Services (ProSe) and Group Communications System Enabler (GCSE). ProSe-enabled LTE devices can also serve as fallback for public safety networks that must function when cellular networks are not available or fail. In the public safety context, D2D must function even without RAN support, making it behave more like a mobile ad-hoc network or MANET. Introducing D2D poses many challenges and risks to the base station(s) driven cellular architecture. Furthermore, out-of-coverage public safety UEs are often clustered at an incident scene (on the order of tens of nodes), and so a vehicular node may even be able to act as a de-facto base station.

# 2 Description of Context Aware Cognitive Radio

This section presents definitions of context and context aware cognitive radio, and how these capabilities can be applied to the needs of public safety.

## 2.1 Definitions of Context and Context Aware Cognitive Radio

### *2.1.1 Context*

Communications deliver data from an originator to a recipient. A definition of context, in general, is

> “Additional understanding needed to convert data into meaningful information.”

The originator’s context and the recipient’s context can all have several levels, each one re-interpreting or modifying the message as it goes up or down the chain.

Context exists at a number of levels, ranging from detailed message formats to organization-wide goals and objectives. At a low level, if the data is a unit record, then the record format is needed to break the transmitted symbols into fields with numeric values or understandable data elements. If, for example, a field contains an alphanumeric customer identification, then the database that relates that identifier to a name and address is part of the system context.

A higher level example is natural language: if the data represents a paragraph, then the recipient needs to have an understanding of vocabulary and syntax of the natural language in which it is written. Depending on the complexity of the paragraph, cultural elements may also be needed to properly interpret the data.

Context can be delivered in a number of ways. It could be incorporated in the same transmission as the data, delivered as a separate message, built into system software or operational domain, or be inherent in the educational and social environment of the participants. The last is particularly true of verbal and written communications.

Misunderstandings may occur, which can have serious consequences if the sender’s context differs from the receiver’s or a recipient is missing some of the sender’s context elements. The popular “telephone” game illustrates this perfectly. Conversely, if the recipient is missing or uncertain of some of the data or suspects that some of it has been corrupted, then an understanding of the originator’s context can often help regenerate sufficient data for operational purposes (within some bounds of error). Sometimes, where multiple contexts are possible, the sender’s context may be inferred from the message, itself. A fire related message would be clearly different from a police action message.

Hence, for the purposes of this report, context can be classified into two types[2],

1. Communications Context: Additional information used to convert communicated data into valid information
2. Operational Context: Additional information required to make use of the communicated information to perform an operation or execute a mission

### *2.1.2 Context Aware Cognitive Radio*

A cognitive radio (CR) is a wireless device with a transmitter and a receiver that has information about the characteristics of the communication link it supports and has computational capability to evaluate options for establishing connections and improving their effectiveness. Self-organizing nets, for example, have radios that interact with each other to establish network topology without a pre-existing design. This is an example of Communications Context.

To be considered context aware, a CR must have information about the situation the user is in, what the user is trying to do, what resources are needed for that purpose, and what other entities are available within communications range to provide those resources. This requires it to be integrated into a larger cognitive system. The system makes decisions about what courses of action are appropriate in the current situation – an example of Operational Context. Then the (Operational) context aware functionality interacts with the cognitive radio's (Communications) capability to establish links over which those messages can be exchanged and their meaning understood. In the rest of this document, the Communications Context will be subsumed into the cognitive radio and "CR" will be used to represent a cognitive radio *system*, unless otherwise explicitly stated.

## 2.2 A Public Safety perspective of Context Aware Cognitive Radio

One of the first challenges facing first responders arriving at the scene of an incident is establishing a communication structure to facilitate incident command in order to assess conditions and deploy resources. As described above, context is needed to enrich transmitted data to provide additional usable information.

The report of the WInnForum Public Safety Special Interest Group (PS SIG) on applying CR techniques to a chemical plant disaster scenario[3] considered several context aware applications for CR, including proposing automatic role-based reconfiguration. In this scenario, CRs automatically recognize such contextual elements as the role being fulfilled by the users and the current mission profile to dynamically adjust device priorities, manage device profiles, and define talk-groups.

In the case of a disaster which destroys public safety infrastructure, replacement transmitters may unwittingly interfere with transmitters that survived the disaster. Formal coordination of communications systems through normal FCC processes is impractical. In this scenario, frequency allocations, power levels, operating waveforms, and device configurations must all be dynamically managed based on the type of scenario, specific information gleaned on the presence, location, and identity of systems from direct sensing and databases, and from interactions with human users (an example of the context concept known as *mediation*). In short, the CR must be context aware. Establishment of communications, in this case, is both communications and operational context dependent.

## 2.3 Context Elements in Public Safety

Initial CR research focused on the physical layer, especially on spectrum occupancy and coexistence. This report extends this perspective to look at those additional elements of context which can make the CR and network, as a system, more useful to public safety operations. Examples of this additional context could be location and incidence awareness. To generalize this further, context could be viewed in layers and usefulness to address the relationships associated with the users. For example, the hierarchical relationship between first responders, such as the group leader, incident commander, span of control, etc., could dictate the allocation of communications resources and priority.

Temporal elements of context could also be useful through the introduction of planning into the mix. Then, the radio network is not purely reactive, but more proactive. As an example, if there is knowledge that the wind will shift in the afternoon in a chemical plume scenario, then a relocation of the incident command center and redeployment of the first responders may require a reconfiguration of their communications depending on available non-interfering spectrum.

Similarly, if victim evacuation and fire suppression are immediate concerns – and we know from historical patterns that it is highly likely that the current available bandwidth is insufficient – the system can provision reconfigurable radios to use additional white space or dynamic spectrum concepts to increase data throughput. It may also be possible to coordinate with or request the shutdown of other known white space radios.

Carrier and data aggregation could also be contextual responses, if, for example, the incident context and historical knowledge or the arrival of additional resources indicates that the response will ramp up within a short time. This aggregation can be planned in advance. It could be a warning that 3.5 GHz radios (see section 3.2.5) might be needed and distributed to the responders or that a 3.5 GHz incident scene network needs to be established.

All of these examples point out the need for relevant context and raise the question of how needed contextual information could be conveyed to the CR system. Further, we must consider which elements of context can be gathered automatically and which other elements would need to be input manually.

As a result, a key concept at a higher level is that CRs go beyond the individual radios and point more to the idea of a Cognitive Radio System, or Network. *In the following discussions, CR will be taken to mean a Cognitive Radio System (CRS)*, as indicated before, unless explicitly stated otherwise.

# 3 Context Aware Cognitive Radio for Public Safety: Model and Resources

## 3.1 A Model for Context Aware Cognitive Systems

Following the discussions outlined above, a useful approach to a context aware cognitive radio system is to logically separate the cognitive and communications functions[4]. While some of the cognitive functions, such as the communications context, could sometimes be physically distributed in the communications elements, this logical separation allows more flexible consideration of the concepts.

Hence, a context aware cognitive radio system, as shown in Figure 1, could comprise of:

1. One or more cognition engines
2. One of more communications channels, using multiple technologies which could be used by cognition engines to serve the mission. These could include LMR, broadband cellular systems, TV white space, dynamic spectrum sharing, reconfigurable radios, airborne and satellite communications, etc.

Data Aggregation: the cognition engine could aggregate the data streams from two or more of these technologies to further increase the available data bandwidth. This could effectively become a composite communication channel accomplished by channel bonding at the radio frequency level, using a common technology, or simply by taking data streams out of multiple different radios.

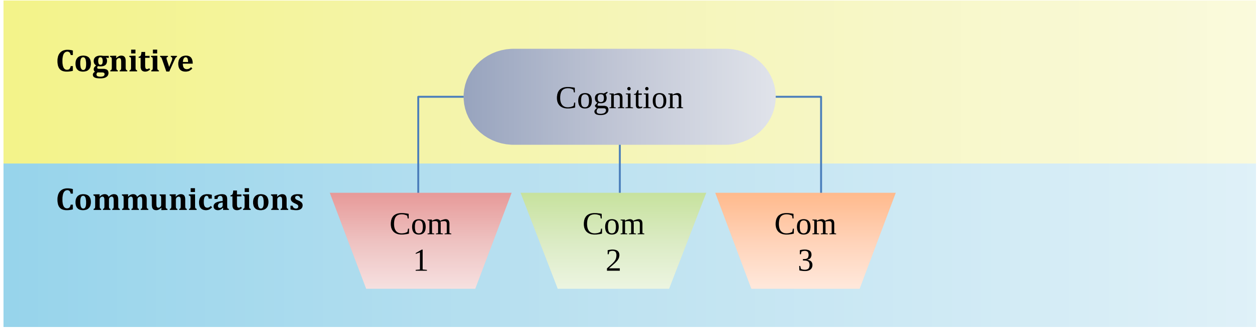

**Figure 1: A Basic Model for Cognitive Communications**

## 3.2 Communications Technologies: Resources

This section looks at classes of communications systems that could be used by the cognitive system.

### *3.2.1 Land Mobile Radios*

LMR has been the staple communications medium of the first responder for many years. Project-25 (P25), the standardized system chosen for use in the U.S. and now being adopted elsewhere, is being developed under the oversight of the Telecommunications Industry Association (TIA) technical working group TR8 as the TIA-102 series of documents. The work on standardizing P25 LMR has been long and ongoing; but usable. It is voice centric with some low data rate components.

### *3.2.2 Voice/Data, LMR/Broadband*

The creation in the U.S. of FirstNet by the U.S. Congress was motivated in part to move public safety communications to a global standard. The proliferation of smartphones and the commercial broadband revolution changed the way users interact with data, and to some extent, even their way of living. It was apparent that if the commercial broadband standards could be harnessed for public safety use, it could bring economies of scale to the equipment used by public safety and also bring in new data sets for their use. Thus, LTE was chosen as the broadband standard for all public safety and codified into law. However, it was also recognized that LTE will likely not meet the mission critical voice requirements of public safety, which especially relies on its voice radios operating with reliable coverage at life-critical moments. Hence, it is now clear that LMR and LTE will complement each other for a long time to come, removing a major barrier to the adoption of broadband by public safety in the US market.

However in the UK the situation is somewhat different in that the Airwave Public Safety Network based on the Terrestrial Trunked Radio (TETRA) standard is not owned by the Public Safety organisations but a commercial, albeit purpose built, network for which the licence fees are expensive. The UK Government have therefore commissioned a new LTE based Emergency Services Network as an overlay on an existing public commercial cellular network. The existing Airwave Network would likely continue to operate for some time under Motorola Solutions.

EE and Motorola Solutions together with Kellogg, Brown and Root have recently been awarded contracts to provide this Emergency Services Network (ESN). The ESN is expected to implement priority and push-to-talk later. It will also use Satellite backhaul for rural areas

But the use of LTE for public safety would require additional features not found in commercial LTE. These features could be standardized only if the changes required to support public safety were minimal and included in the global cellular standards effort, and were also seen to be of value in the commercial world. Therefore, the National Telecommunications and Information Administration (NTIA), as the agency designated by Congress, joined the Alliance for Telecommunication Industry Solutions (ATIS) and started the process of introducing public safety needs into the 3rd Generation Partnership Project (3GPP) forum, the international body which has now become the sole developer of commercial cellphone standards on an international scale. NTIA has successfully added the following services to commercial LTE:

- Group Communications Services (GCS) to bring group voice calling and group data services to LTE, along the lines that public safety is organized and communicates
- Proximity Services (ProSe) for off-network peer-to-peer or Direct Mode communications of both voice and data

The above would be part of LTE Release 12. Another element of GCS, for push-to-talk (PTT) services is expected to be part of Release 13 or beyond. Until then, PTT is being handled by specific applications, or APPS, which may or may not be compatible across vendors.

In addition to these standards related elements, it is also recognized that broadband terminals for public safety need to be ergonomically usable by the first responder. For example, terminals would need to be operable with thick gloves while wearing self-contained breathing apparatus (SCBA) gear. The terminals also need to minimize distraction and provide information in a convenient form that enables the first responders to still perform their primary functions of saving life or property, while helping keep them safe. Hence, there is a heavy HMI challenge to be met. The use of voice control and voice and haptic feedback are examples of new HMI constructs which may be employed.

At the same time, it is recognized that broadband could provide whole new capabilities for public safety. Helmet and body video cameras are an example, but the bandwidth requirements and utility in large deployments is unclear. Clearly, the first responder cannot be focusing on his broadband terminal's video at all times. Thus, it is recognized that there could be both logistical/tactical benefits of the additional information that can be provided by broadband communications and some operational benefits as well – most likely in that order, if it is carefully managed. The flood of information that can be potentially unleashed brings up the needs of information management. Some of this could be performed by information managers, such as the Info-M proposed elsewhere in this report. Others may be implemented by cognition directly in the system/network.

### *3.2.3 White Space Radios*

As a result of moving to digital television and recognizing that most UHF television channels were not in use over large parts of the country, the U.S. government consolidated the UHF television spectrum and allowed for the use of these frequencies under a TV white space protocol. This operates in conjunction with databases which inform communications systems of the availability of portions of the spectrum in a geographical area. Approved systems with the appropriate database subscriptions can then use TV white space for communications. This option could be valuable as an additional data pipe when an incident requires more capacity than is available in the area using LMR, cellular broadband or other licensed communications.

### *3.2.4 Satellite Communications*

Satellite systems have the advantage of being able to provide coverage and moderate capacity in areas that are not covered by traditional terrestrial communications. As the FirstNet system is built out, for example, its architecture includes the use of satcom in remote rural and wilderness areas which may not be covered by the FirstNet terrestrial system. In the context of Search and Rescue (SAR) operations, satcom may provide communications directly, or be used as backhaul to an air-dropped portable LMR base station or cellular RAN. Satcom comes in several flavors, with Low, Medium, and Geosynchronous (high) orbits. Services are provided by several private satellite mobile operators with a variety of terminals. It is also possible that a satellite solely for emergency use, a National Emergency Incidence Communications Satellite (NEICS), could be deployed in the future. Due to the wide variety of orbits and terminals, setting up and operating these systems could be complex, and hence these are prime candidates for context based intelligent set-up and operations.

### *3.2.5 Wi-Fi and other Listen-Before-Talk (LBT) protocols*

The use of Wireless Fidelity (Wi-Fi) access has exploded among consumers and first responders. Most homes have Wi-Fi access points which operate at 2.4 GHz, and more recently in the 5.8 GHz band. These are also often used, with or without enterprise level management, in public safety. Wi-Fi provides a low-cost, high bandwidth communications path, especially for indoor and short range applications. A separate band in the 4.9 GHz region is also available only for first responder use. These systems share multiple users within the available spectrum using listen-before-talk (LBT) protocols.

More recently, under a presidential directive, frequencies in the 3.5 GHz band have also been made available using LBT protocols.

### *3.2.6 Unlicensed LTE*

Broadband communications using the LTE protocol, have transformed cellular communications. These use the Frequency Division Duplex mode for operation, where separate uplink and downlink frequencies are needed. An unlicensed mode of LTE, called LTE-U, has also been defined in the standards; this mode uses the time-division duplex mode and works in a single unlicensed band. It could be of use to first responders for capacity augmentation, while allowing long range communications unlike Wi-Fi. However, LTE-U does not mandate LBT protocols, triggering concerns from Wi-Fi users. An alternative, developed by 3GPP, called Licensed Assisted Access (LAA), which includes LBT protocols, is expected in LTE Release 13.

### *3.2.7 Dynamic Spectrum Sharing Radios*

Dynamic spectrum sharing (DSS) is a developing area of wireless communications. The development of DSS has been encouraged by the presidential directive that requires the federal government agencies in certain bands to make spectrum available to DSS radios as secondary users. This is done under the rules of the Citizens Broadband Radio Service (CBRS), which defines two tiers of secondary users to share spectrum which already has a primary incumbent. The WInnForum has been very active in the area of spectrum sharing.

It is noted, as an aside, that the next generation 5G wireless communications standards effort, does not include spectrum sharing in its current form.

### *3.2.8 Reconfigurable Radios*

Evolving CR technology, such as those described in preceding sections, have great potential for significantly enhancing public safety communications systems. The PS SIG came to this conclusion after detailed analysis of two different scenarios: the bombings in London in 2005[5], and a hypothetical scenario of a chemical plant explosion in a small city[6]. From these analyses, the SIG identified capabilities that would enhance public safety communications by the use of reconfigurable radios in a network incorporating cognitive radio technologies.

For the purposes of this report, a Reconfigurable Radio System (RRS) is one that includes software defined and/or CR systems, and which can alter its communications based on defined policies, rules, and guidelines. The capabilities included improvements in:

- Interoperability for public safety;
- Coverage improvement;
- Spectrum utilization optimization and dynamic spectrum access;
- Communicate reconfiguration information;
- Managing communications resources; and
- Supporting incident management.

Further, the SIG assessed the state of research and development in these areas and concluded that the most significant research gap is in the application of evolving CR technologies to support incident command.[7] From the perspective of the general R&D community, this gap is not a surprising conclusion, as the support for incident command is specific to the public safety domain – whereas, technologies that enable dynamic spectrum access and coverage improvement are applicable to much broader areas.

From a public safety perspective, the support for incident command (see below) is also a logical opportunity for exploiting reconfigurable and CR technology. Public safety communication has a long history of extensive planning, training, and preparation for events and incidents. This preparation is vitally important for effective response and to ensure that communications plans, especially involving multiple agencies, are clearly thought out and understood by the participants. The ability to reconfigure radios enabled by software defined radio technology, combined with CR technology, brings the possibility of a true paradigm shift. With current capabilities, incident response is constrained by communications capabilities; the future potential is to configure the communications around the requirements of the incident response. The ability to reconfigure radios and networks in near-real-time provides opportunities to adjust communications capabilities as needed.

Such capabilities can enhance communications across the full range of activities from daily, routine, operations to small scale, “typical” incidents to situations (incidents) that rapidly evolve in unforeseen ways. Incidents can range from the small (e.g., traffic stop, house fire) to catastrophic (e.g., Hurricane Katrina, tsunami). Events, which are pre-planned, can evolve into incidents in unexpected ways (e.g., the 2013 Boston Marathon bombings). Incidents can also evolve unexpectedly (e.g., the December 24, 2012, incident in Webster, NY, where two volunteer firefighters were shot and killed by a sniper when they responded to a house fire). Incidents may involve responders from a single agency or multiple agencies, may include local, state, and federal agencies and personnel, and may last from a few minutes to months. Within the context of National Security and events related to that challenge, incidents are more likely to be managed at the Federal level, with significant partners in the State, Local and potentially Department of Defense environment; thus, the ability to leverage technology and features such as reconfiguration are of paramount importance. At the same time, CR capabilities can facilitate daily operations by adjusting for maintenance or minor communications disruptions, transient interference issues, and so on. The common theme of all of these examples is the potential for the communications requirements to evolve in ways that are different than routine, known, or expected.

Reconfigurability could be a key to providing flexibility, but the potential number of decisions that can be made will overwhelm a human operator. Hence, the cognitive capabilities of radios (potentially, in both the user equipment and the network) should allow such decisions to be made autonomously while being monitored by a supervisor. One guiding principle throughout the analyses conducted by the PS SIG has been that the technology supports, and does not replace, the human operator (e.g., the Communications Unit Leader). The human role in monitoring and managing communications resources is critical.

# 4 Context Inputs for Cognitive Systems

Recent work within WInnForum (described above in Section 2) has developed the concept of Operational Context, in addition to the Communications Context. The latter provides the communications system with the information necessary to manage the radio and communications link to ensure that data is communicated with the highest possible accuracy. The Communications Context provides the critical information for a cognitive radio to appropriately interpret data and make decisions, which is useful in looking at how to implement cognitive radio technology in public safety systems. This report documents the elements of context used to operationally manage a public safety communications system, whether solely by a human or a human in conjunction with a system with cognitive capabilities. Such a human might work in the Emergency Operations Center (EOC) to manage the information and resources for a larger incident. The PS SIG proposes that this additional post be called an INFO-M.

### *4.1.1 The Incident Command System*

Much of this context is based on the structure of the incident command. In the U.S., that structure is typically referred to as the National Incident Management System/Incident Command System (NIMS/ICS). The ICS is a standardized, on-scene, all-hazards incident management approach that:

- Allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure;
- Enables a coordinated response among various jurisdictions and functional agencies, both public and private; and
- Establishes common processes for planning and managing resources.

ICS is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents being dealt with.

ICS is used by all levels of government—federal, state, tribal, and local—as well as by many nongovernmental organizations and the private sector. ICS is also applicable across disciplines. It is typically structured to facilitate activities in five major functional areas: Command, Operations, Planning, Logistics, and Finance/Administration. All of the functional areas may or may not be used based on the incident needs. Intelligence/Investigation is an optional sixth functional area that is activated on a case-by-case basis.

As a system, ICS is extremely useful. Not only does it provide an organizational structure for incident management, but it also guides the process for planning, building, and adapting that structure. Using ICS for every incident or planned event helps hone and maintain skills needed for the large-scale incidents.

In the U.S., the concepts, doctrine, terminology, and organizational principles for an ICS are defined in NIMS. A basic premise of NIMS is that all incidents begin and end locally. NIMS does not take command away from the authority having jurisdiction (typically local or state authorities, but federal authorities in situations involving national security). NIMS simply provides the framework to enhance the ability of responders, including the private sector and non-government organizations, to work together more effectively in a systematic manner. The federal government supports state and local authorities when those resources are overwhelmed or anticipated to be overwhelmed. Federal departments and agencies respect the sovereignty and responsibilities of local, tribal, and state governments while rendering assistance. The intention of the federal government in these situations is not to command the response, but rather to support the affected local, tribal, and state governments.

Other countries have similar approaches to incident command, with many countries adopting the ICS itself[8]. Recognizing there may be some variations worldwide, we use the term ICS generically throughout the remainder of this document.

### *4.1.2 Priority and Preemption*

As the NPSBN is being planned by FirstNet using LTE, two key requirements have been formulated: Priority and Preemption.

#### 4.1.2.1 Priority

It is recognized that in incident management, some traffic may need higher priority than others. For example, the live video of a shooter will most likely be a higher priority than a video from a helicopter showing the overall scene, though both are video feeds. Awareness of the context and content of the feeds could help make, either automatically or as a recommendation, adjustments to the priority of the feeds.

#### 4.1.2.2 Preemption

It has been specified that the NPSBN will lease part of its idle airtime and network capacity to other wireless carriers to help carry their overflow and generate revenue. However, in the event of a major incident, when network capacity and airtime fill up fast, the NPSBN is expected to specify the ability to pre-empt (i.e., knock off or force onto another network) non-critical traffic. For example, if one of the calls on those sharing the capacity is a 9-1-1 or Next Generation 9-1-1 call for a medical emergency, context aware cognitive communications would preserve that as an open channel without preemption until the call is done. However, if that was from an owner calling about a cat stranded on a tree, it is probably pre-emptible, though regrettable, when higher stakes are at issue. Clearly, this requires a greater degree of information about the call than simply that it is a 9-1-1 call, information that may not even be present today. Hence, the development of the context aware cognitive radio system or network could require upgrades to the surrounding infrastructure also. This raises several social issues and also questions of accountability.

Preemption is a major decision. Hence research is also needed on how priority can be used to minimize preemption and how successful this could be.

### *4.1.3 Next Generation 9-1-1*

Next Generation 9-1-1 (NG9-1-1) is an important initiative by the first responder community as it recognizes the use of smartphones by the public. Though the 9-1-1 service is voice centric today, the public has become more comfortable with text messages as well as the use of social media.

Hence, the NG9-1-1 effort tries to increase the ways in which the public can communicate with emergency services. Recent initiatives that are being rolled out include Text-to-9-1-1, which allows text messages to be sent to the 9-1-1 service. This option is valuable also when the sender is not able to talk to an operator for some reason. As Text-to-9-1-1 is implemented, the volume of messages from multiple sources is expected to increase, and hence the filtering role gets harder. It is possible, initially, that the call taker will still provide the traditional role of distilling the information and passing it on to the responders.

A natural extension is the use of multimedia input to 9-1-1 services. These could include photographs and video sent in by the public. Today's 9-1-1 services are just beginning to develop capabilities to handle text messages. This capability needs to include the ability to take multiple inputs, correlate them to a particular incident, and condense and pass them on to dispatch. The CONOPS of what happens to the information is still being developed. It is highly unlikely that even the filtered text messages will be passed on directly to first responders. It, therefore, places additional burdens on a filtering layer and the dispatchers to ensure that only relevant information that will aid, not distract, the responders is passed on to the field.

When the full NG9-1-1 is implemented, the scope of the problem increases dramatically. Information coming into the 9-1-1 center could now include photographs and videos, several of which could be duplicates of the scene. The call takers, or information managers, now need to be trained, not only to quickly scan the information received, but extract salient information and pass it on to the responders.

In addition, some of the information may be directly of use to the responders at the scene, including photographs or frames from videos that could be sent to the first responders. The precise nature of the information to the first responders will be incident dependent. Furthermore, there may be a need to contact the sender and ask for additional information to get a better angle, for example. Streaming video that provides a vantage point that is not available to first responders could, on the other hand, be sent directly to the field incident commander. The priority of this information over the communications network will also need to be managed.

A key consideration is whether the context filtering could be automated. The advantage of these forms of input is that they may be more amenable to machine manipulation and context extraction. That technology may not be here today, but it is expected that it will be developed in the future and could operate within the context of the incident. However, it is reasonable to assume that at least for the foreseeable future, a human being will always be in the loop to identify relevant information before it is forwarded to the responder in the field.

### *4.1.4 Automatic Crash Notification*

Many vehicles are now being equipped with automatic crash notification systems (ACN). In the event of a crash, these vehicles send a slew of information to their emergency assistance center; information that ranges from vehicle behavior prior to and after the crash, as well as some information about the occupants in the vehicle. The ability to detect vital signs information is also now being gradually introduced. When this link is completed, it will provide valuable information to the responding agencies, both to deploy all needed resources to the scene and prepare hospitals and emergency rooms in the vicinity to receive the patients.

It is believed that as the range of information about the occupants, the vehicle, and the nature of the crash expands, first responders will be better prepared to respond to the incident. Information about the appropriate way to extract the occupants in a hybrid or electric vehicle may be useful, for example.

However, there is currently no clear standardization of the information that is being sent from the vehicle. Also when that information is forward to public safety answering points (PSAP), often known as 9-1-1 call centers, their software is not always capable of extracting all the relevant fields of the information that is sent. Hence, operator intervention is often needed to select and re-type the information into the receiving PSAP’s dispatch system – resulting in context information that is often left unused at the present time. Public safety organizations, such as the Association of Public-Safety Communications Officials (APCO), are working to bring some order and standardization to this field. Again, care will be needed to avoid overwhelming the responder in the field. This, once more, points to the role of an INFO-M in the operations.

# 5 Applications of Context for Public Safety

## 5.1 Some Applications of Context

### *5.1.1 Capacity enhancement*

Despite the use of a dedicated broadband system built by FirstNet, i.e., the NPSBN, even in conjunction with civilian systems, there is concern that a significant incident can tax their capacities locally in an incident area or system. Hence, capacity enhancement, either using reconfigurable radios or dedicated systems which can operate in other bands and protocols to augment the size of the data pipe, either by themselves or with data aggregation, is thought to be a key use of context aware CR.

### *5.1.2 Disaster Management*

Another application of context aware CR is in a disaster incident that includes the use of an airborne communications layer (AL) as proposed in the March 2013 Mission Critical Communications article, "3 Layers of Disaster Recovery"[9]. The AL provides substitutes for damaged ground infrastructure in the terrestrial layer (TL) for public safety land mobile (and broadband) radios and civilian systems. Context aware systems can be used to first observe the transmissions that survived the disaster. After assessing the impact of the disaster, the system can then make decisions (such as platform height, power levels, associated protocols, antenna parameters and pointing, and frequencies to be used) by the AL to provide support to replace infrastructure that did not survive the disaster. This decision requires careful assessment of ground situations and decision making so that communications can be reestablished while minimizing interference to the neighboring bands/systems which survived the incident.

### *5.1.3 Automated System Configuration*

As indicated above, capacity enhancement could include the use of more than one system and data aggregation to increase the effective size of the data pipe. Taking note of the fact that the user today looks at communications only as an information portal, and would rather not concern himself with how it is accomplished, this augmentation of system capacity by automated system configuration is well suited to a cognitive communications system. The precise mechanisms could be shielded from the user, with only the concurrence of the system manager required to implement these connections.

### *5.1.4 Automated Equipment Configuration*

A major disaster can also require the use of satellite communications.[8] However; each responder group may be subscribers to different satellite carriers. The set-up, pointing/alignment, and frequency configuration combined with the network address allocation can become an overwhelming task. While "rapid" deployment satcom services are still available, they often have a lower capacity data rate due to simplified antennas and pointing.

We suggest that, "*No one ever wanted to become a firefighter or a policeman because they wanted to twiddle radio knobs.*" While communications is a primary component of their work, by necessity, a frustration that is often heard from first responder personnel is that "*communications should just work.*" Communications is an ancillary tool, albeit an important one, but not the primary mission of their deployment. An analogy today could be to the modern automobile, which is expected to just start and work when needed, to provide transportation under all conditions. Its enormous complexity and myriads of microprocessors are hidden from the users and unknown to most owners, who only have to deal with its well-known operating controls.

Therefore, whatever can be done in the realm of context aware communications to intelligently automate the deployment and configuration of equipment could become valued attributes.

## 5.2 Network Aspects of Cognition

Up to this point, cognition has been discussed primarily in a local context and network, centered around the incident scene. However, there is the possibility of using information from a wider area or even different contexts to improve the response to an incident, using intelligence in the network. An example could be the use of Big Data analysis to bring additional historical knowledge about plume behavior, population behavior, etc.

Depending on the nature and seriousness of the incident, we may need to make changes to the network or traffic. Examples are:

- Network coverage extensions
- Incident scene communications frequencies or modes
- Additional resources
- Reconfiguration
- Moving traffic to other networks
- Changing priority
- Changing frequencies
- Bringing in white-space communications
- Data aggregation
- Dynamic spectrum sharing
- Uplink/downlink asymmetries
- Advanced technologies to overcome limitations, such as the role of cognition to make the human interface easier
- Benefits that can be seen from using broadband services such as video streaming, on demand video surveillance, etc.

At some point there will be thousands of sensors sending out low density, infrequent information. Examples could be sensors to monitor bridge conditions, or from other Internet of Things (IoT) applications, which send them by Machine-to-Machine (M2M) communications. It is expected that these will be sent over either a commercial network, or with preemption capability over a national public safety broadband network. The intelligent transportation system (ITS) of the future also will be using sensors to automatically control the flow of traffic, rerouting it around accidents, for example. These intelligent capabilities could also be possibly used to facilitate the easier deployment of public safety responders to the incident scene. Some cognitive capabilities that could be used here over shared networks could include clearing bandwidth over nearby RAN, rerouting non-emergency traffic to RAN that are further away from the incident scene, raising the priority of the first responder traffic, etc. It may also be possible, in the future, to dedicate secondary access and control channels solely for emergency response use to overcome radio access congestion, though this may tie up additional resource blocks and reduce the system air interface capacity.

The larger network based intelligence may be able to adjust frame rates, resolution, and other parameters of videos or manage the use of certain Application/Network (APN) interfaces, to optimize network capacity usage. In a public safety environment, contextual cognitive capabilities can be used to determine what videos can be compressed and what cannot be degraded.

Network intelligence may be used to avoid the so-called “circle of death” congestion symbol by rerouting traffic to certain edge servers that are not as busy. It may be also able to gracefully degrade some services depending on criticality.

Despite these efforts, at some point, there may be a need to drop certain data streams. Deciding what and when to drop brings policy issues. These decisions could be usefully managed by a policy engine, either with a human in the loop, or by itself.

### 5.3 Policy in Context Aware Cognitive Networks

Policy is an important element of managing cognition. There is a need to balance the needs of first responders with network sharing for revenue generation, for example. In short, not every incident should automatically invoke preemption.

Some policy-based decisions may also need to consider:

- Contract issues, Grade of Service (GOS) for those who share the spectrum as primaries by agreement.
- Policies that govern Secondary responders and their network access (Salvation Army, Red Cross), as well as volunteer agencies and volunteers.
- During the London underground bombing in the 7-7 incident, the implementation of Access Overload Control (ACCOLC) by the City of London Police independently of the Metropolitan Police caused volunteer organisation ambulances from the Red Cross and St John Ambulance organisations, called out as part of an agreed major incident plan by the London Ambulance Service, to be unable to communicate with Emergency Doctors on scene.
    - Emergency doctors were supposed to call ambulances that were standing at a safe distance by cell phones to collect casualties after triage. They were unable do so.
    - In the UK, the Red Cross and St John Ambulance may be issued an Airwave LMR unit on a regional basis to communicate with dispatcher as relay for major incidents
    - This event also highlighted the need for establishing cooperating policies for agencies and users as well as technology.

In general, large disasters trigger a large number of secondary responders (Red Cross, volunteer groups, etc.,) whose roles are vital. Most of their operations rely solely on commercial networks. They do not all have access to LMR or public safety broadband radios.Their needs must be captured and accounted for in the policies, especially when they are using spectrum shared by the NPSBN with commercial entities.

- The U.S. Federal Emergency Management Agency (FEMA) responds according to the national response framework. Damage assessment is done by a large army of staff using communications networks to generate and distribute photographs, damage reports etc. They store and forward the data from their terminals. They often use the commercial network as part of their tool set.

Other examples of variations in communications procedures include the following in Canada:

- Oil tanker derailment in Quebec: Provincial response
- Mud slides in Vancouver: Used commercial communications
- Floods in Manitoba: the Army was called in, which took over incident management
- Royal Canadian Mounted Police (RCMP) maintains a national emergency network and radios. However, the RCMP provincial role varies from province to province.

Similarly in the UK the Buncefield Oil Storage Depot Fire, requiring the presence over a long period of some 600 fire crews from across the country, had to be coordinated by the Fire Officers using cell phones as at that time all the Fire Brigades purchased their own Radio systems. This exacerbated the introduction of the Airwave system into the Fire Service. It is assumed that they will ultimately use the LTE based ESN network.

Hence, useful questions to ask are, “What are broadband services that first responders need in case of a major disaster? Are they different from day-to-day needs? If so, what are the differences?” Answers to these questions will govern the design of the network.

## 5.4 Security in Context Aware CR

The security needs of communications networks have never been more front and center than at present. Several high profile security breaches have made system administrators move to tighten security even more in their systems. Wireless, by itself, is inherently more vulnerable, providing greater opportunities for disrupting communications[10]. CR systems/networks present yet another opening in the security domain. The tension between security and usability is ever-present. The mechanisms and implications of this are just being studied.

Data aggregation, for example, will open the system to multiple data streams coming over different systems, not all of which will be equally secure. Could the data stream with the weakest security provide easier ingress to a cyber attacker?[11]

## 5.5 Spectrum for First Responders

The public safety community has long been using narrowband communications using 12.5 and 25 KHz bands. In the U.S., the predominant network uses the P25 protocol, whereas in Europe and elsewhere TETRA, using 25kHz, has been more common, though these are being re-bid. Several agencies employ their proprietary narrowband systems as well.

However, the public safety community is beginning to use broadband data applications to perform their day-to-day operations, as discussed in the following links (Texas PS LTE[12], Utah BB[13], PS Alliance[14], Rivada[15]). These operations include high definition video streaming, infrared sensing, biometric tests, automatic license plate reading, facial recognition, database queries, etc. Also, more spectrum is needed even to perform narrowband applications when first responders encounter major incidents such as the attacks on September 11, 2001, hurricane Katrina, and the London bombing in 2007. Contextual information such as location, time of day, traffic pattern, and user behavior is critical to make such decisions. In situations that require data-extensive communications or in incidents that require more capacity than what was originally planned/ allocated, these contextual elements can be utilized to manage spectrum demand. The system can utilize the 3.5 GHz band on a secondary access mode to alleviate bandwidth demand or can roam in cellular network if there is some capacity available. The use of geographical fencing databases for managing these bands removes complex requirements such as spectrum sensing and use of interference avoidance mechanism, in case a primary user occupies the spectrum somewhere else. However, it should be noted that such a real-time database should be extremely accurate, otherwise an approach where some spectrum sensing is combined with a database would be more viable. We believe that intelligent decisions and utilization of such context aware tools can greatly facilitate public safety personnel in performing their duties while also meeting spectrum demands.

## 5.6 Sharing the NPSBN Spectrum with Commercial Networks

FirstNet is relying on sharing its capacity with other commercial carriers to generate essential revenue. Some questions that need to be examined include:

- Do first responders have sufficient frequency spectrum to support their broadband needs?
- If the NPSBN is shared with commercial providers, would it compromise the commercial cellular system?
- How much capacity is used in daily routine operations?
- How big is the increase in traffic in a disaster scene?
- What contextual awareness can public safety provide to the network?
- How much more spectrum is needed in a disaster scenario?
- How does the cognitive network get those numbers of usage, and how can they be programmed into policy engines?

- In a smaller disaster, video may be used only for a short time. In a large disaster, such as a collapsed building, for example, video could be on at all times. How does that affect demand and need?
- Studies in Alameda County, CA, showed the need for bandwidth greater than a 5 MHz x 5 MHz system to support 4 VGA quality video streams. NPSTC did a follow-on study based on this later to estimate bandwidth needs. The NPSBN has been granted a 10 MHz x 10 MHz channel. What mix of traffic, both uplink and downlink, will this support?
- Does the change of any factors over time change the capacity need and make it more difficult to estimate maximum capacity?

The following developments call for caution.

- Commercial carriers are constantly trying to improve their networks. Compression techniques are improving. The deployment of these technologies could also change the needs of first responders.
- First responders are beginning to use broadband in trials for incident response. Estimates of bandwidth usage from these trials are critical to check assumptions.
- The estimation of data flow can also be optimistically low. Increased data flow from smart buildings and vehicle-to-vehicle (V2V) communications of the future are some examples of underappreciated demand.
- In general, it is safe to say that data will expand to fill the available transport pipe!
- Hence, it is better to specify that the role of cognition is not just to manage a network but all the resources available to maintain GOS/Quality of experience, which are deemed appropriate for first responder use.
- Resource management depends on applications that are running. The demand of application considered for use vs available capacity of the network is key. It is not just an issue of transporting offered traffic. Hence, a cognitive network will also have to manage the applications that are running, which will make demands on the capacity of the network.

## 5.7 Network Planning and Context Aware Networks

One of the main issues in public safety spectrum management is the highly challenging and dynamic environment of public safety communications. Incidents may involve responders from a single agency, multiple agencies, local, state, and federal agencies and personnel, and may last from a few minutes to months. It is this dynamic environment that makes it essential to perform extensive planning, training, and preparation for events and incidents. This preparation requires careful study in laying out the requirements and possible scenarios that first responders might encounter in their day-to-day operations. Different contextual elements in public safety communications can then be used for situational awareness and rapidly deploy and adapt public safety networks.

### *5.7.1 Dynamic Analysis and Prediction*

One area where contextual elements can be used is in the analysis and prediction of network behavior. A context aware public safety system can analyze prior network usage and make some predictions on the future use of its network. Contextual elements such as the type of incident, time and location, as well as number of radio users in a certain geographical location could be used for better network planning. The network must be able to predict and identify capacity loading to meet the requirements and limits that were set in place at the time of network deployment.

However, public safety communications has to handle unexpected incidents from time to time. A contextually aware public safety system can help in deploying a role-based system that leverages prior experience; but could be changed/modified according to the situation. A contextually aware system can reconfigure itself based on the user profile and the role that user is assigned in the response. The concept of 'roles' (as discussed in detail in the use cases SDRF-07-P-0019-V1.0.0[4] and WINNF-09-P-0015-V1.0.0[5]) can allow the communications to evolve automatically without human intervention as the incident evolves and responders assume various roles. Implementation of a role-based communication system is a challenging task, and will require using new tools that allow intelligent decision making.

### *5.7.2 Coverage Enhancement*

Another area that is of great concern for public safety is coverage enhancement. States, counties, small towns, and cities that use public safety LMR communications for its first responders generally specify coverage requirements that are usually more stringent than in the commercial cellular world. Attempts to provide additional in-band coverage could also degrade the existing system by causing increased interference. Different elements of context can be used for enhanced network coverage in public safety. Using available tools and techniques in this area, public safety systems can be improved to provide better coverage, and reliable and more optimized service. A report published by the WInnForum[4] on the London bombing identifies the lack of public safety coverage in certain geographical areas of the network. . Following this incident this problem was partially addressed by extending the coverage of the Airwave Network to the London Underground Railway. However there has been recent concern highlighted in the press that the new LTE based ESN will not cover London Underground or large parts of Wales and Rural Scotland and there is no provision for priority for emergency services over the public networks. This moves away from the principles and requirements of Public Safety Communications highlighted in this report.

Context aware CR can be implemented to automatically reconfigure radios to provide an extension to the existing network. This ability allows immediate connectivity for all users without requiring additional hardware. It is observed that no matter how well the public safety network is planned initially, there will still be some areas in the network that will have coverage holes. Context aware public safety communications system can learn about these areas through measurement and experience, and then make appropriate adjustments in order to fulfill coverage needs of first responders.

Certainly in the UK one can see that local coverage solutions implemented through Context Aware CR are likely to play an important part in UK Emergency Services Communications in the future to mitigate concerns regarding the new ESN contract.

Data stream aggregation using multiple systems add complexity to the network planning process since the use of all of these networks need to be planned in a coordinated manner to satisfy data throughput. This may not require the maximization of available throughput from each individual link, since they may be serving other high priority uses as well.

The LTE standard is capable of measuring and reporting coverage parameters by each user device using appropriate applications, under the rubric of Minimized Drive Testing. This provides valuable feedback. When data from multiple technologies are aggregated, not all of these may have this capability. Hence, this complicates planning coverage for a multi-stream system.

### *5.7.3 Integrating Non-Terrestrial Systems*

There is a possibility of using of unmanned aerial vehicles (UAV) for coverage enhancement. There are some recent trials where it is demonstrated that a UAV can remain in air for up to 14 days. DARPA has a goal of deploying aerial vehicles that can carry a load of half a ton with 5KW energy supply and can stay in the air for five years. These are High Altitude Platforms (HAP) which may operate over long durations. Such aerial deployments may be used by public safety to provide coverage. In many cases, smaller, lower altitude platforms may be needed for coverage enhancement, to operate within available link margins, to control the coverage footprint, and to minimize interference to neighboring systems. It is desirable that these vehicles are equipped with autonomous decision making mechanisms in order to find available spectrum, and appropriate transmission protocols while maintaining minimal footprint in order to minimize interference to neighboring bands. Lower altitude aerial platforms may also need peer-to-peer networking to relay out-of-cell traffic to another airborne cell or to pass it on to surviving terrestrial networks.

### *5.7.4 Self-Healing*

Another area that is highly desirable is the capability of the network to perform self-healing. We believe that public safety networks will start to experience self-healing capabilities as device manufacturers and network providers embrace this technology that is quite popular in commercial cellular world, especially in future 4G LTE networks. If there is a base station failure in a certain geographical area, the remaining base stations will cooperate in such a manner as to provide coverage to make up for the failed network. They might perform intelligent decisions with the remaining base station or deploy a UAV and perform automatic network planning such as transmit power setting and antenna beam forming, in order to provide seamless connectivity to the first responders.

### *5.7.5 Cognitive Hierarchy*

It is clear that not all of the above elements may be performed by a single general purpose cognitive engine. Human supervision or intervention may also be required at all times, even if it is only for legal purposes. Some functions may still be best performed by humans. Some may need specialized cognitive engines. Hence, cognitive systems may be divided hierarchically, with overall supervisory human control overseeing automated supervisory control, and one or more subordinate and peered cognition engines, some of which may provide redundancy or be selected by voting among competing courses of action.

## 5.8 Body Area Networks for First Responders

Public safety has also recently seen a significant increase in the use of wearable devices and sensors. WINNF-09-P-0015-V1.0.0[3] identifies the use of cognitive sensor networks and realized their effectiveness in scenarios such as personal protective equipment (PPE) for firefighters. These body sensors can form their own Body Area Networks (BAN) to communicate with each other. The BAN could use intelligent (cognitive) decision making to determine the health of the wearer, and alert the system with out-of-BAN transmissions only when the vital parameters of the wearer or his physical posture indicate problems.

## 5.9 Other Uses of Sensors

Other places where use of such sensors are identified are in in-building mechanical and emergency systems, environment measurement facilities, video streaming for situational awareness, cellular system traffic information gathering, and intelligent traffic systems. A practical demonstration of such an application is the use of wireless sensors in public safety for flood monitoring as in the wireless sensor actuator network (WSAN)[16]in Indiana. Sensors are playing an increasing role in critical infrastructure protection. A large number of sensors actively transmitting data in a given geographical area could require much wider bandwidth for public safety, unless they form an intelligent (Cognitive) network that only send out alerts for out-of-limit conditions. Also the awareness of locale, provided with geographic information systems (GIS) could add geo-fencing capabilities to minimize uncoordinated out-of-area transmissions.

The use of sensors can also improve network performance. With the introduction of M2M communications, we expect to see several connected devices and sensors in a public safety network providing detailed and updated information about the environment. Different types of sensors such as in PPE worn by first responders, in-building sensors providing temperature and related information, video cameras, cellular traffic information etc. could be used by public safety to facilitate its daily operation and avoid future incidents. Sensors are usually designed to transmit data periodically. With increasing number of sensors deployed, there are issues such as how to synthesize data and interpret useful information from it. As discussed above, another issue to be considered is mitigating network congestion and contention management. The use of sensors is beneficial for public safety but it will open new challenges. There is more data to process, and useful information needs to be extracted from that data to derive context.

Another consideration in respect of M2M is that there is a drive towards the use of LTE for M2M applications and the LTE-M standard is being developed. Network Operators are increasingly wishing to re-farm their spectrum from 2G and 3G towards LTE and this means that again all the IoT and M2M sensors will be sharing the LTE band.  Hence, future signaling capacity of the network, as well as data capacity could be considerations.

### 5.10 Economics of Cognitive Radio for Public Safety

While there are attractive benefits from cognitive technology in public safety, the cost of implementing such features is a significant economic issue. Chipset and equipment manufacturers need profitable business models in order to invest in this area. FirstNet estimates that there are about 5.4 million potential public safety users of its network nationwide in the U.S. This is a relatively small number compared to commercial cellular network subscribers, even if this were to be doubled by adding non-public safety responders, federal users, *et. al*. Furthermore, systems cannot be sold solely on the premise of managing large disasters, which are infrequent and sufficiently varied, to justify these systems. Hence, equipment needs to be multi-purposed, targeted not only toward large disasters but also useful in day-to-day operations. This contributes to operational familiarity, which is key to effective use. Using cognitive management of shared spectrum, or the added use of alternative spectrum such as TV white space, the new CBRS, or data aggregation, to avoid congestion, interference, and slow communications response times at any incident scene, are some examples.

Hardware and network capabilities alone do not an operational system make. The usability and types of applications (or APPs in broadband) in use will determine how resource intensive applications could become. Hence, it may be useful to study if there is a minimum resource requirement for applications. Their costs are also a deciding factor.

The cognitive communications community needs to be sensitive to whether it is being Procrustean (pushing capabilities just because they are possible) or if the capabilities genuinely serve the needs of first responders in incidents. The public safety community is cautious, since life safety is potentially on the line. Hence, it will not embrace any “gee whiz” technology without being convinced that it is reliable, cost effective, and does not interfere with life safety or, better, contributes to enhancing life safety.

# 6 Topics for Work Needed

Introduction of new technology and evolution of more capable first responder systems will require system design and engineering in a number of areas. Some relevant topics follow.

1. Using other Cellular Operators/systems with available capacity or capacity management policies needs study.
    a. We do not have a good model for how spectrum usage ramps up on commercial and Public Safety networks in an incident. The diurnal variation in traffic usually seen in commercial networks may not be reproduced in public safety.
    b. Commercial operators are also unable, due to regulatory reasons, to prioritize some traffic over others, or preempt traffic altogether.
    c. Commercial operators do not share their traffic data publicly, since that information is business sensitive. It is not clear how public safety could know, for immediate planning purposes, what the available capacity of a commercial network is.
    d. The NPSBN, as part of its business model, expects commercial users to share its spectrum by using its network to off-load their traffic. For this reason, the NPSBN has, from the outset made it clear that it will have the ability to prioritize and preempt non-public safety traffic if needed. Clearly, minimizing preemption would be a good business practice to maintain viability and maximize revenue.
    e. However, if an area is evacuated ahead of a storm, this could result in availability of commercial spectrum for use by public safety.

2. It may be useful to consider regulatory set aside of alternative spectrum (such as some channels of TV white space) for public safety at some point in the future. However, since the bandwidth needs of public safety have not yet been established, this is probably premature.

3. APPs capabilities should also be considered in the resources mix. APPs could be context aware, providing spectrum to first responders based on their prior (usage). The same APP, used under different circumstances, may use spectrum for different durations. Similarly, the needs of short burst text communications would be very different from extended video streaming applications. Hence, study topics could include:
    a. Whether there is an upper bound on the bandwidth needed to handle an incident, based on number of users and the APPS that would be typically used.
    b. Whether, based on the location context and prior behavior, the spectrum needs to manage the incident can be determined.

Hence, context aware resource usage could is also a prime topic for study:

4. The availability of using TV white space around the country.

5. Reliable use of the 3.5 GHz band to support additional broadband needs.

6. The consequences of sharing partnerships with commercial operators.
    a. Public safety community could roam on commercial network in 700 MHz in scenarios where more capacity is needed and commercial capacity is available.
    b. In-network and out-of-network coverage is important because it cannot be always assumed that an incident occurs within NPSBN coverage, while commercial

coverage may still be available. The commercial network provider would have to decide how much bandwidth could be given to public safety without degrading service to its customers. However, if the incident also affects commercial networks, then bandwidth on those networks may be reduced or unavailable.

   c. Could some administrative non-critical data be sent on commercial networks?
   d. How network and processing delays affect the utility of the network for some (near) real time applications.

7. Using location information as a context, for example by ensuring that all nodes have availability of the frequency band that is planned to be used.
8. Information sharing on the data bandwidth and spectrum usage with the cognitive engine.
9. Coverage hole identification and its use in a cognitive engine (use feedback about intended vs actual communications behavior due to some inability to communicate to deduce coverage holes).
   a. Also explore if there are companies that provide coverage hole identification as a service to network service providers (possibly as a Big RF application).
10. The use of vehicular repeaters in an incident scene is a critical study area. These are small base stations that are mounted in vehicles. In the LMR world, these are usually devices that need to be manually configured. Broadband vehicular repeaters which are cells/systems-on-wheels (COW/SOW) may also need such configuration. The first vehicular repeater on scene may establish a local coverage umbrella. However, if this is occurring in an area that already has strong coverage; the vehicular repeater may interfere with the capacity of the serving cell. The arrival of a second vehicular repeater on the same band may render them both useless and reduce service to the responders on scene.

    A similar effect is observed when multiple LMR vehicular repeaters arrive on scene although, in this case, they may be able to mitigate the issue by using different LMR frequencies. This is not the case with Band Class 14 LTE, for example.

    Equipping the repeaters with some intelligence, a location context, and the ability to sense the environment could make them more effective.
11. The use of automatic beam forming to improve vehicular repeater coverage within a building using location context, information that the operation is inside a building, and information about the building, is another study area. Automatic beam-forming, both to reach the network better and to send data to the repeater’s coverage area could increase data rate or connection reliability. This function is well suited to cognitive operation.
12. High power UEs have been authorized by 3GPP, but only for public safety. When can that capability be turned on? A single high power UE can degrade communications to many normal UEs. High power also raises some issues similar to vehicular repeaters
13. Identifying other ways location information can be used by the system to facilitate cognitive operation.

# 7 Other Issues for Consideration

Some other issues not covered above are given for completeness, though not explored in detail.

- Initial Response vs follow-on planning for next shifts. This is important since the initial response may not have a COML available at the incident or an INFO-M at dispatch to support the responder.
- INFOSEC, security of systems. Network and data security.
  - This is a huge and vital topic; but outside the scope of this document. It suffices to say that security should be considered and built into every element of the system, while bearing usability in mind
- Representation of the incident command structure and communication structure in:
  - COML view/tools
  - Incident command view/tools
  - Network management view/tools
- Standard shared "screens" – collaboration tools for use with other managers.
- Other elements that may be of use to the COML and INFO-M.
- Context for the COML vs context for incident command.

  Many incidents don't get a COML at the initial response stage, where the person first on the scene is designated the incident commander. The ability to integrate a COML into an operation where the ICS is being expanded is of great importance. The incident commander, Area Command, or Unified Command dynamic would be better able to leverage these advances in technology if a competent person such as COML was assigned. This issue may happen quite frequently on smaller events and more so when agencies don't normally respond to areas where there are jurisdictional boundaries and other "non-home system" areas. Ideally, whenever an event is beginning to overwhelm the first few resources and an expansion of the system is required, a COML should be engaged. With the extended use of the internet protocol, resources may experience technical problems with mobile data terminals (MDT), subscriber units, UE's, and other tools that a COML would be able to quickly resolve for the incident commander (IC).

  With much more information now available with broadband use, it is possible to explore if the context presented to the IC could/should be different from the context of the COML. A broadband information manager, such as an INFO-M at the emergency operations center, would be forwarding information to the IC in the field which describes the incident in different terms than the COML in the field, who may be focused on the details of the communications and integrating broadband with LMR use, for example.
- "Simplification and compatibility"– capabilities needed to handle catastrophes must also work for daily use so that they are in the practiced skill set of the first responder.
- Most sensors make point measurements. However, the effects of interference are often seen in the aggregate. Hence, some information may need to be passed up to a higher level of the cognition engine in order to make a more informed decision that takes additional factors into account. This again relates to the hierarchical partitioning of the cognitive elements.

- Privacy: Infrared and other sensors may impinge on privacy. The increasing use of UAVs in the civilian population has heightened awareness of unauthorized photography or videography. This could limit the use of such tools by first responders.
- Border issues which have been touched on above.
- Big data processing for cognitive management, so that the results are meaningful for cognitive decision making.
- Affordability
- Regulatory issues.

# 8 Conclusions and Recommendations

A general assumption that is implicit in the discussions above is that the first responder will demand more and more data, and will need more sophisticated data collection, delivery, and dissemination. First responders have always evolved radio discipline to use the available communications bandwidth. Legacy LMR has limited capacity that constrains the information they can provide and influences system hierarchy and operational protocols, prescribed in standard operating procedures (SOPs) for managing the communications. The availability of broadband eases data bandwidth restrictions significantly, and allows a much richer set of information to be made available to first responders managing an incident. However, they could still run out of data bandwidth if its use is undisciplined. The community must evolve new SOPs, CONOPS, and ICS procedures for broadband, to make optimal use of these new resources.

The availability of new communications networks also poses another problem for first responders. Spectrum sharing must be addressed. The first responder community has always had exclusive access to its own pieces of spectrum, and continues to need basic communication capability with a level of survivability that far exceeds commercial standards. Programs to develop systems with a hard core of basic communications supplemented by more vulnerable broadband capability are a key recommendation of this report.

The move to broadband data and the attendant explosion of information available to first responders has accelerated need to manage both the data and the networks that deliver it. Information is data taken in context. As data volumes increase dramatically, their conversion to useful information will introduce new techniques for context management,

The following broad trends will influence development of needed capabilities:

- An increase in the complexity of incidents.
- An increase in the availability of sensors to provide more information.
- An increase in the information that is flowing into the EOC.
- An increase in the bandwidth of the communications channels available to the first responder in the field.
- The desire to catalog and manage the flood of information that is now available, often in real time.
- A coupling of the incident with big-data analysis, to obtain additional information that may not be directly provided by the incident, such as trend forecasting.
- A need to determine and control the extent to which information can flow into and from the field.
- A need to find suitable wireless and backbone network capacity to send the information to the field.
- The requirement of managing several individual networks, and even aggregating networks to provide the necessary communications bandwidth.

- The need to automate the setup and provisioning of equipment in the field to reduce the burden on the first responder, who would rather focus on his life-saving mission
- The reconfiguration of devices, networks and their deployment as the need arises, or the trend is forecast, to continue information flow. This could be ideally done autonomously, but may need supervision, at least initially.

These developments highlight the need to broaden the capability of the COML function to include introduction of broadband communications and its integration with Land Mobile Radio.

Additionally, the need to manage the flood of information that that could flood answering services with the deployment of advanced 911 services also introduces requirements for an information manager (INFO-M) at the operations center or dispatch. This is a new position that has not been part of the traditional incident command structure.

These trends could have the beneficial effect, if managed properly, of helping the first responder focus on the mission at hand and enhancing their personal safety. The communications networks should adapt to enable these goals.

These goals are served by the development of context aware cognitive radio and communications networks, which facilitate reconfiguration of communications parameters and networks that forecast the need for, and bring in, assets as needed to accomplish the mission.

This report has identified several elements of context which can be useful for public safety communications and recommends ways in which these elements can be used.

This report also recommends that the elements of information identified be examined in their context, and an enhanced CONOPS be defined to describe how they can be used to enhance and improve the mission of managing routine and major incidents. These concepts can guide the implementation of context-driven actions in devices and networks to facilitate support of the first responder. They will expand the capability of COML, as well the possible creation of an INFO-M position to manage the flood of information at the dispatch or EOC.

A major problem that needs to be addressed is the standardization of the presentation of context information so that it can be used by multiple context aware organizatons, networks, and systems. Some of the elements of context identified in this report could form the basis of that standardization of efforts to present and derive context.

Additional considerations, such as network and information security, which are outside the scope of this document, must also be considered in deployment of context aware CR systems.

# 9 References & Resources

[1] D. Devasirvatham: "The Reality of Broadband" APCO Public Safety Communications Magazine, p45, April 2014.

[2] J. Neel, et. al.: "The Role of Context in Cognitive Systems", Journal of Signal Processing Systems, Springer Verlag, Vol. 78, No. 3, pp 243-256.

[3] Wireless Innovation Forum, "Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario," *WINNF-09-P-0015-V1.0.0, Feb 11, 2010.*

[4] J. Neel, P. Cook, N. Mellen, I. Akbar, D. Devasirvatham, C. Sheehe, R. Schutz: "The Role of Context in Cognitive Systems", Journal of Signal Processing Systems, Springer, Vol. 78, No. 3, 2015, pp 243-256

[5] Wireless Innovation Forum, 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, available at http://groups.winnforum.org/d/do/1565.

[6] Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario, Report No. WINNF-09-P-0015-V1.0.0, available at http://groups.winnforum.org/d/do/2325.

[7] Wireless Innovation Forum, Assessment of Cognitive Radio Technology for Public Safety Communications, Report No. WINNF-13-P-0003-V1.0.0, available at http://groups.winnforum.org/d/do/6705.

[8] At the International Wildland Fire Summit, 2003, an agreement was reached by the Food agriculture Organization of the United Nations that an Incident Command System (ICS) based on the ICS developed in the U.S. should become the international standard for all wildland incident management participating in international or interagency agreements and exchanges. See the *International Wildland Fire Summit Communique,* 8 October 2003, available at: http://www.fire.uni-freiburg.de/summit-2003/International%20Wildland%20Fire%20Summit%20Communique-Final-230402.pdf. (Last accessed 20 September 2013). In addition, the *Use of Incident Command Systems in Fire Management Proceedings* (February 3, 2009) includes descriptions of how a number of Asian countries are adopting ICS for fire services, available at http://www.fire.uni-freiburg.de/GlobalNetworks/Northeast-Asia/Pan%20Asia%20proceeding_ICS%28final%29.pdf (last accessed 10 September 2013).

[9] D. Devasirvatham, J. Neel, C. Tompsett and K. Link, "3 Layers of Disaster Recovery," *Mission Critical Communications*, March 2013, pp. 62-65.

[10] D Devasirvatham and W Austad: "Wireless Adds Vulnerability to Cyber Threats", Mission Critical Communications, May 2014

[11] D Devasirvatham: "Spectrum Sharing and Critical Infrastructure Protection: Opportunities and Challenges", Proc. WInnComm-Europe 2014, pp 62-66

[12] Texas PS LTE http://www.txdps.state.tx.us/LTE/

[13] Utah BB http://broadband.utah.gov/resources/public-safety/

[14] PS Alliance: Building A Nationwide Public Safety Broadband Network http://www.psafirst.org/uploads/documents/D_Block_Briefing_Documnet_-_Final_reduced.pdf

[15] Rivada: The Future Role Of Spectrum Sharing For Mobile And Wireless Data Services, http://stakeholders.ofcom.org.uk/binaries/consultations/spectrum-sharing/responses/Rivada_Networks.pdf

[16] Indiana Floods: http://www.govtech.com/public-safety/Wireless-Sensors-Reduce-Flooding-in-Indiana.html

# Related Sources

These resources have not been explicitly referenced in the text; but are included here to expand the resource material.

A. Dey, J. Mankoff, “Designing Mediation for Context-Aware Applications,” *ACM Transactions* 2005.

A. Dey, J. Mankoff, G. Abowd, and S. Carter, “Distributed Mediation of Ambiguous Context in Aware Environments,” *Proc. 15th Ann. Symp. User Interface Software and Technology (UIST '02),* pp. 121-130, Oct. 2002.

A. Dey, M. Futakawa, D. Salber and G. Abowd, “The Conference Assistant: Combining Context-Awareness with Wearable Computing,” *Proceedings of the 3rd International Symposium on Wearable Computers (*ISWC '99*)*, San Francisco, CA, Oct 1999. pp. 21-28.

A. Frank, “Tiers of ontology and consistency constraints in geographical information systems,” *International Journal of Geographical Information Science,* 15 (7), 2001, pp. 667–678.

C. Bostian, J. Reed, “Understanding the Issues in Software Defined Cognitive Radio,” Tutorial presented at *IEEE DySPAN*, Baltimore, MD, Nov. 2005.

D. Devasirvatham. Recovering Communications after Large Disasters, http://groups.winnforum.org/d/do/4627

FCC, “Second Memorandum Opinion and Order In the Matter of Unlicensed Operation in the TV Broadcast Bands and Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band,” FCC 10-174, Sep 23, 2010.

J. Mitola, “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio,” Doctor of Technology Dissertation, Royal Institute of Technology (KTH), May, 2000.

H. Chen, T. Finin, A. Joshi, “Semantic Web in the Context Broker Architecture,” *Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications*, 2004.

K. Henricksen, J. Indulska, A. Rakotonirainy, “Modeling context information in pervasive computing systems,” 1st International Conference on Pervasive Computing (Pervasive), vol. 2414 of Lecture Notes in Computer Science, Springer, 2002.

K. Henricksen, S. Livingstone, J. Indulska, “Towards a Hybrid Approach to Context Modeling, Reasoning and Interoperation,” *Proceedings of the First International Workshop on Advanced Context Modeling, Reasoning and Management*, 2004.

O. Wang et al., “A Context-Aware Light Source,” ICCP 2010. Available online: http://zurich.disneyresearch.com/~owang/pub/context.html

A National Broadband Plan for Our Future- “Public Safety, Homeland Security, and Cyber Security Elements”, https://prodnet.www.neca.org/wawatch/wwpdf/1112telcordia.pdf

Wireless Innovation Forum, “IPA – Information Process Architecture Volume I,” WINNF-09-P-0020-V1.0.0, *Nov 01, 2010.*

http://www.readwriteweb.com/archives/nokias_new_situations_app_makes_phones_self-aware.php

https://developer.qualcomm.com/blog/context-awareness-gimbal-platform-new-white-paper

http://code.google.com/p/rscm/

# Appendix 1 A Summary of Elements of Operational Context for Public Safety

In the main body of the document, an approach and rationale for context aware public safety communications was presented. This appendix provides a quick reference listing and description of some elements of context needed for effective public safety communications system management.  This listing is not exhaustive.

## Event/Incident Context

### *Event/Incident Type - Classification*

These context elements characterize the type and nature of the incident or event. The word "incident" is used in the public safety sense to denote unplanned/uncontrolled scenarios such as fire, tsunamis, calls for police action, etc.

1. *Event/incident Type*: characterizes whether the situation is planned or unplanned. Note that this is not a binary element—planned events can be disrupted, and there may be "degrees' to which an event evolves differently than planned. There are also nuances between a situation which is covered by contingency plans, situations which are similar to previous experience or training scenarios, versus something "completely unexpected."
    a. Note that a large planning gap could drive the need for additional decisions which may need to be made by the operators or the system.
    b. Incident types could include structure fire, wildfire, explosion, crash (with or without medical emergency), shooting, hostage taking, search and rescue (SAR), missing child, missing elderly person, kidnapping, etc.
    c. An incident such as a bridge collapse could include several of these categories.
2. *Projected duration*: hours, days, or weeks as an incident goes beyond a single operational period, it can evolve into different stages and even responses. It may require relocation of the command center, depending on weather or the evolving needs of the incident.
3. *Lead time*: an event with a long lead time and extensive pre-planning, an incident for which some specific plans can be drawn up (e.g., hurricane landfall), or one with no specific planning.
4. *Size of response*: numbers of agencies, number of responders, levels of response (e.g., local only or federal support).
5. *Operations Tempo*: Single event with evolving response (e.g., bridge collapse), evolving event (e.g., wildfire, multi-action terrorist event such as the London bombing), and the rapidity with which an incident evolves (e.g., flash flood versus flood).
6. *Risks/hazards*: radioactive release, chemical plume, etc.
7. *Population demographics*: urban area versus rural area.
8. *The speed of response*: This could affect the course/evolution of the incident.

*Geospatial overlays*

These context elements characterize geospatial information relevant to the incident or event.

1. Jurisdictional boundaries
2. Terrain and terrain classification, whether land or water, urban, suburban, etc.
3. Weather, wind direction and speed, rain and intensity, tornado and its track, etc.
4. Division, groups, and sections
5. First responder locations (staging areas, command center location)
6. Incident area characteristics (e.g., plume/flood maps—note FEMA tool set for emergency management, evacuation zones, corridors, epicenter/radius))
    a. NIMS map symbology may provide a useful list of relevant characteristics
7. Incident site characteristics (e.g., buildings, hazards, blueprints)
8. Traffic/transportation

Examples of the application of location information as a context use-case could be:

i. Find locations of all the nodes in a network
ii. Estimate or measure the data bandwidth that is going to be needed by the network and if it could be served by the broadband network in use.
iii. Check the TV White Space database and see if there is an availability of spectrum that can be used
iv. Check the 3.5 GHz band and see if the location permits the use of this band
v. Check whether both bands are going to be needed. May need to use carrier aggregation or channel bonding in that case
vi. These channels may be using different protocols. Treat these as bit pipes.
vii. Determine if the characteristics of these bit pipes affect the cognitive system?
viii. Instruct each node to provide a spectrum report to make sure it is appropriate to use the band of interest

*Incident strategies and tactics (plans)*

1. Availability and assignment of non-communications resources
2. Requesting more resources, possibly from different agencies.
3. The communications needs could change as the incident evolves. The needs may be predictable or possibly subject to pre-planning. (e.g., change in wildfire characteristics as the sun rises may require changes in deployment/locations of resources)

*Data Source and availability*

1. Video feeds, sensors, citizen inputs / NG9-1-1, building systems, weather
2. M2M input
3. ACN information
4. What data are to be accessed and used? These raise questions of data quality. Not all data may be generated from a public safety source. Big Data concepts, where large amounts of diverse data are analyzed to find relationships and inferences that add value are an example.
5. Usability of the data for public safety needs is a consideration. Real time video analytics and feature extraction tools may be used to avoid being flooded with raw feeds from citizen cellphones. However, the effectiveness of these tools in extracting relevant features, detection of a gun in the hands of a suspect, etc. are to be determined, and may be a context factor.
6. The language(s) to use when multiple countries are involved could also be a contextual element, for example in Europe. This could also influence the decision making process.
    - A subset of this is the use of plain language instead of 10-codes in communications. This is mandated in the NIMS/ICS process
7. Cross-border incidents may pose different problems. An anecdotal case could be that of a border control agent who is shot from across the border.

**Response Context**

The second major contextual element that is critical to communications operation planning and implementation is the response itself—the responders, their equipment, their location, their relationships within the structure of the response, their information requirements, and similar contextual elements. Further, this context changes over the course of an incident, so projections of how these elements will change are also important. Some of these are codified in incident command procedures and provide a ruleset of response.

1. Incident command structure
2. First responders use, including command, since their familiarity with ICS may vary, at least by agency
3. Relationships (incident command hierarchy)
    - Interface to the EOC and/or Management Center (impact of changing responsibility)
    - Interface to fusion centers and joint information centers
    - Responder roles and functions
4. Equipment

5. Location
6. Plans
7. Ancillary and support organizations
8. Utilities
9. Transportation
10. Medical and public health
11. Volunteers, relief organization, Non-Governmental Organizations
12. The use of amateur radio emergency service/radio communications service (ARES/RCS)
13. Military, National Guard, Reserves

### Policy Context

Examples of policy context are:

1. Jurisdictional policies (These may be uniform across small European countries).
2. NPSBN: local vs national. FirstNet which manages the NPSBN across the nation, may not have policy jurisdiction within state boundaries, except to manage its own network.
3. Security of data (some agencies have policies and some don't, especially for data sent across jurisdictions).
4. Video and privacy considerations. In some cases, streaming video may be treated differently. An officer may stream video or may require supervisor to authorize it. Deployment of Cameras, body-cams and dash-cams and their use are governed by policy (e.g., shutters on cameras may be physically closed as the default under some policies, to be opened only under specified conditions and authorization). Other policies may require the dash-cam use for all traffic stops. The recording of audio is also controlled by policy, which could differ across agencies.
5. Regulatory
6. Partner network policies
7. Policies at boundaries, such as jurisdiction in the middle where there is a jumper (for example on the Woodrow Wilson bridge, which crosses the Potomac between Alexandria, Virginia, and Prince George's county in Maryland).
8. Similar cases arise in bridges and tunnels between countries such as the Chunnel, and at borders.
9. Usually, policy decisions are made by supervisors. Then the system could analyze how that affects communications.

**Communications Resources Context (dynamic usage and availability)**

These entail knowing what communications resources are available and the capabilities to set up the communications, matching them to the resources. Related parameters are:

- Network physical/logical topology and resources
- Capacity/utilization, for example, recognizing overload conditions

Resources could include:

- Deployable Aerial Communications Architecture (DACA) equipment, such as UAVs
- TV White Space. This has resulted in equipment and commercial TV white space databases in the U.S. The CCIR has initiated a similar project on white space in Europe
- CBRS equipment at 3.5 GHz and their usability in the location. CBRS requires all priority 2 and priority 3 customers (opportunistic users) to share the spectrum, while not causing interference to the incumbent (priority 1). Hence 3.5 GHz could be a useful resource in many places for capacity augmentation.
- Wi-Fi and LTE-U or LAA equipment
- Ad-hoc self-organizing public safety networks could turn on peer-to-peer communications in broadband when needed, when several repeaters are deployed to cover a larger area.
- Furthermore, the use of Proximity Services (ProSe) allow user equipment of operate in direct mode, to perform UE2UE communications off network. If equipped with multiple hop relay capabilities, individual units could act as “bread crumbs” to backhaul communications from a UE that is deep inside a building to enable it to reach the network outside the building.

# Appendix 2 Additional Information on the Wireless Innovation Forum and Public Safety Special Interest Group

The Wireless Innovation Forum™ is a non-profit “mutual benefit corporation” dedicated driving technology innovation in commercial, civil, and defense communications around the world. Forum members bring a broad base of experience in Software Defined Radio (SDR), Cognitive Radio(CR) and Dynamic Spectrum Access (DSA) technologies in diverse markets and at all levels of the wireless value chain to address emerging wireless communications requirements through enhanced value, reduced total life cost of ownership, and accelerated deployment of standardized families of products, technologies, and services. The PS SIG is an organization within the Wireless Innovation Forum that provides a focus for activities in which the public safety community has an interest. Goals of the PS SIG are to interface with both communications users and commercial vendors associated with the public safety community with a goal of increasing awareness of SDR related issues, publicize activities of the Forum that address those issues, and increase participation by the public safety community in Forum activities. The PS SIG also interacts with other forum committees and working groups to ensure that the public safety community’s inputs are addressed in other publications and initiatives undertaken by the Forum.

The public safety community, as defined by the PS SIG, includes all first responders (e.g., emergency medical services, fire services, police/law enforcement. It also includes secondary responders (e.g., civil government, emergency management, environment health personnel, civil protection/homeland security/homeland defense units, search and rescue units, hospitals, relief organizations, public utilities, transportation), and other elements of the criminal justice system.