EULER

The first pan-European SDR-based public safety communications platform project

O. Picchi (University of Pisa), T. Sturman (EADS Astrium), F. Vergari (Selex – Communications),
T. Bräysy (University of Oulu), R. Dopico (Indra), G. Baldini (JRC),
M. Luise (University of Pisa), E. Bolzan (Selex – Communications), J. Diez Ruiz (Indra)

***Abstract* — Effective international public safety communications has become in more recent times a principal focal point; partly motivated by the increased risk of concentrated natural disasters, such as flooding, earthquakes and fires, and partly, due to the risks and consequent impact of terrorist attacks. This paper focuses on a European Commission (EC) Seventh Framework Programme (FP7) initiative known as EULER – European SDR (Software Defined Radio) for wireless in joint security operations. The EULER project seeks to demonstrate the benefits of SDR pertaining to a natural disaster of significant stature such as to solicit a coordinated pan-European response. The SDR platforms interfaces with WiMAX and TETRA COTS networks with an underlying satellite link to guarantee the wideband capabilities for performing a full voice, image, file and video transfer. The main feature of EULER in this respect is the definition of a common waveform within the SCA constraints, and enabling portability. This paper discusses a range of issues which have been identified thus far within the EULER project, in particular the perceived pan-European interoperability needs of Public Safety, and of the latter with military devices/networks. Aspects of interoperability are also extended to the three dimensions of platform, waveform and information assurance.**

Keywords - Cognitive Radio, PPDR, Public Safety, SDR, Spectrum Allocation

I. INTRODUCTION

The European Commission and the member states of European Union have recognized the importance of providing the needed enablers for Public Protection Disaster Relief (PPDR) to ensure justice, security and protection.

The protection to be ensured by the PPDR primarily covers people but also the environment and property, and it addresses a large number of threats both natural and man-made, acts of terrorism, technological, radiological or environmental accidents, occurring inside or outside the EU.

In Europe, a major PPDR operational requirement is supported for effective cross-border cooperation, which requires adequate communication capabilities including interoperable radio communication systems in border areas and between operational services from different Member States. Difficulties in the use of radio communications in border areas are usually caused by the lack of interoperable interfaces between current systems, which prohibits effective roaming.

In Europe, a variety of wireless communication systems are used by Border Security organizations including TETRA, TETRAPOL, Analog Professional Mobile Radio and even commercial systems like GSM and GPRS. As a consequence, public safety responders in the field may not be able to effectively coordinate their efforts for the resolution of the crisis. Joint military and public safety operational scenarios are particularly important as they are usually related to wide cross-border natural disasters where lack of coordination may have huge impact for loss of lives and assets. It is therefore important to identify technology enablers to eliminate or mitigate the interoperability barriers.

Another important challenge for PPDR organizations is the lack of broadband connectivity. A considerable number of new PPDR applications require the transmission and distribution of images and video among field responders and to the remote offices. An increased data usage, especially for mission critical communications, will have a significant effect on the frequency need and justifies requirements for additional spectrum.

Finally, security is a critical requirement during joint emergency operations between different services, such as Governmental Forces (e.g. Police, Military, Fire Brigade), Non-Governmental Organizations or other emergency services. Security is needed to avoid possible SDR communication attacks which could endanger the lives of both Public Safety officers and the people they support and protect.

In this context, the EULER network and nodes are based on SDR technology porting a WF implementing the 802.16 standard (WiMAX), to leverage the interoperability and security provided by the communication systems.

II. MOTIVATION: MILITARY AND PUBLIC SAFETY INTEROPERABILITY

We consider the motivation aspects of shared usage for the military and public safety services from two aspects in this section: firstly, in the context of current spectrum usage and secondly, in the context of both the cost in terms financial and loss of life through disasters in recent times.

A. Shared Spectrum Motivation: Military and Public Safety

A recent EC conducted a study, undertaken in 2009, on public sector spectrum usage and the Radio Spectrum Policy Group (RSPG) indicated that public sector (defence, transport, public safety) uses about half of the spectrum between 108 MHz and 6 GHz [1]. However, this study concluded that pub-

lic safety used only 0.9 % of that in a typical EU member state. The resulting figures are provided in Table 1.

TABLE I. PUBLIC SECTOR SPECTRUM USAGE IN THE 108 MHZ TO 6 GHZ BAND[1]

Service Type	Proportion of Spectrum
Defence	27.2 %
Transport	20.7 %
Emergency services	0.9 %
other public	1.4 %

We observe from Table 1 that the largest proportion of current spectrum usage in 108 MHz and 6 GHz is by defence with emergency services having the smallest occupancy.

B. Motivation: Cost – Financial and Loss of Life

We note that whilst the current allocation of spectrum for public safety is very small, trends in terms of natural and man-made catastrophes indicate that public safety organizations have an increasing need of broadband wireless communications to support their operational capabilities. A shortage of spectrum will limit the wireless communication capacity of public safety organizations involved during an emergency crisis of a natural disaster. The potential impact is quite relevant both in terms of monetary value and in terms of the loss of life. According to Swiss Re, an insurance firm, more than 15,000 people died or went missing as a result of natural and man-made catastrophes in 2009 [2]. Figure 1 provides an overview of the natural disasters in terms of biggest insurance losses and loss of life, where we note that natural disasters in both Europe and the US predominate; with an excess of $6bn for this period.

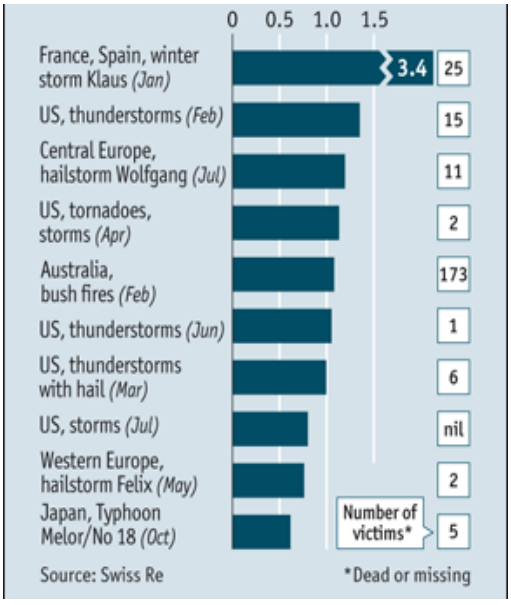

Figure 1. Natural Disasters in Terms of Biggest Insurance Losses and Loss of Life[2]

The chart indicates significant losses of life, especially for Australia where a single incident causes 173 report cases. Nearly 9,400 lives were lost in Asia of which around 1,200 of them in an earthquake in Indonesia in September. Winter storm Klaus, which hit France and Spain in January, was the most costly event of 2009. The storm caused heavy rain and flooding, claimed 25 lives [2].

III. A EUROPEAN EFFORT FOR MITIGATING MILITARY AND PUBLIC SAFETY INTEROPERABILITY ISSUES

As can be seen from the previous section, there is a pressing motivation for reducing the impact of man-made and natural disasters – both in terms of cost and for saving lives; Europe has responded with the EULER (European Software Defined Radio for Wireless in Joint Security Operations) project.

A. EULER Vision for Interoperability

In order to improve seamless communication between European public safety organizations a specific concern to address is the areas of dual use technology relevant to both civilian and military applications. This topic has been a focal point for the European Commission, who has funded various research and demonstrator initiatives which include the EC Framework Programme (FP) 7 Security Theme Work.

Crisis management is a key point with the need for fast response capability with a pressing need of minimizing loss of life by establishing communications and networking in the first few hours. First responders have to react without the risk of interoperability lack and the interoperable radio links have to be available according to the same timeline. Then, multi channels SDRs (Software Defined Radios) provide a natural solution in order to perform transport level gateway as multi RAT (Radio Access Terminal) base stations (BSs). For this purpose the minimum set of SDR capabilities should include major radio communications system standard like TETRA (in EU), P25 (in USA), WiMAX and satellite, typically required on Public Safety applications [3,4]. The EULER project aims to demonstrate the effectiveness of an applicable configuration depicted in figure 2.

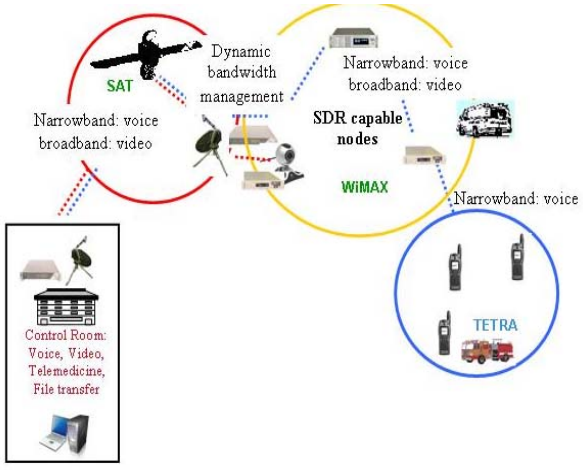

Figure 2. EULER Link Capabilities

B. EULER Communication Attributes

SDR benefits from its reconfiguration capabilities and can be supported by state-of-the-art software architectures – through periodic software upgrading, seems the most effective solutions in order to resolve the following inter-working aspect:

- Physical layer and protocols characteristics matched between the systems (RATs and RAN), including conversion of physical and electrical states, rate adaptation and transmission attributes, in-band signaling conversion, codec and encryption issues, PTT (Push-To-Talk) mode vs. duplexing mode [5];
- Mapping service data units with an inter-working protocol, including conversion, filtering and discarding;
- Handle compatibility information and service agreement;
- Provide conversion between numbering or channeling plans (see tuning range following);
- Information assurance.

IV. Spectrum Allocation issues

In Europe, 380-400 MHz frequencies are often used for narrowband (channel spacing up to 25KHz) public safety and the most common type of network is TETRA. A new ECC Decision [6] on the harmonization of frequency bands for the implementation of digital PPDR (Public Protection and Disaster Relief) radio applications in bands within 380 MHz to 470 MHz range has been approved in 2008. However, the reality is that numerous applications and technologies are already in use in the 410 MHz to 430 MHz and 450 MHz to 470 MHz bands making the possibility for broadband data communication impractical.

In the near future, as the specifications developed for public safety and disaster relief are becoming more and more specialized and demanding, the need to use dedicated spectrum sufficient to carry video and other wide-band data for operational communications will increase [7]. Organizations, such as PSC-Europe, are claiming [8] it is essential for Public Safety services to have access to appropriate spectrum in all parts of the territory sufficient to meet their evolving operational.

Furthermore, the political diversity of Europe is reflected in the variety of spectrum regulations at national level. The new frequency bands for PPDR in Europe should also be harmonized, meaning that the spectrum allocation for PPDR should be the same across the European member states.

These usage patterns may result in poor spectrum utilization. An alternative approach is based on the concept of "spectrum sharing" or "spectrum pooling" where military. PPDR and commercial users "share" the spectrum using various strategies described in section V. Spectrum sharing between Public Safety domain and commercial domain has been investigated in [9] and [14].

Within nations the need for harmonized frequency tuning ranges is undoubtedly important. However, the need for global spectrum identification is also important to allow worldwide Disaster Relief communications to be provided by different national organizations as well as for cross border assistance scenarios.

A. EULER PERCEIVED REQUIREMENTS

Another requirement is provision of broadband connectivity. Public Safety communications were historically based on voice with guaranteed requirements on call set-up, resilience and security. In recent years, Public Safety responders have been increasingly dependent on data communication to support a number of new applications. The following list provides some examples:

- **Verification of biometric data.** Public Safety officers may check the biometric data of potential criminals (e.g. fingerprints) during their patrolling duty.
- **Wireless video surveillance and remote monitoring.** A sensor captures data in video-streaming format, which is then collected and distributed to public safety responders and command & control centers.
- **Automatic number plate recognition.** A camera captures license plates and transmits to headquarters for the plate data to verify that the vehicles have not been stolen or the owner is a crime offender.
- **Documents scan.** Patrolling or border security operations, public safety officers can verify a document like a driving license efficiently.
- **Database checks.** All the activities where public safety officers must retrieve data from the headquarters to support their work.
- **Transmission of Building/Floor plans.** Building or floor plans can be requested to the headquarters and transmitted to the public safety responders.
- **Monitoring of vital signs of Public Safety officers.** This is particularly important for firefighters and officers involved in dangerous operations (e.g. search & rescue during a fire).
- **Remote emergency medical services.** Through transmission of video and data, medical personnel may intervene or support the team in the field for an emergency patient.
- **Collect and share.** This applies particularly to the common situation picture among Public Safety responders of various organizations.
- **Access to images.** This applies particularly to aerial photographs, satellite images & maps.

V. EULER Backbone Discussion

A. Spectrum Strategies

The EULER backbone network waveform, which is based on WiMAX technology [10], could be made to operate in both licensed and unlicensed bands. Therefore the possible strategies are:

A) Licensed bands allocated to it so that EULER would be the primary user, guaranteeing the performance of the services (suitable for scenario 1). Obviously this would require new spectrum allocations [11].

B) Licensed bands owned by another (primary) user, so that EULER would be the secondary users (suitable for scenario 2). This requires spectrum sensing method from EULER devices and related functionality from the network. Also performance is not guaranteed.

C) Licensed bands shared between EULER and another network(s) with a spectrum sharing mechanism for the band, where EULER has priority.

D) License-exempt bands requiring no license (suitable for scenario 2). However, this may lead to interference from other users of the same spectrum and to performance degradation [12]. Currently, 801.16h is working on Improved Coexistence Mechanisms for License-Exempt Operation (802.16h). They are also proposing improved co-existence with 802.11

B. Cognitive Radio for Public Safety

Let us consider two different spectrum usage scenarios:

- *In the aftermath of a major disaster, the communication infrastructure remains (mostly) operational. In this case the cellular bands and ISM bands will be filled with traffic (emergency calls etc.) so that dynamic spectrum access using these bands may not be possible.*
- *The disaster causes the communication infrastructure to be destroyed. In this case the public safety communications could use the available cellular bands because they could be assumed to be unoccupied.*

1) PPDR system as a secondary/primary user of spectrum

Cognitive radio techniques could be used to locate free frequency bands for public safety communications in case of emergencies. These bands could be initially licensed to some (primary) user like cellular operators. Especially in scenario 2), there would be available spectrum, which is not used by commercial users, because most of the infrastructure is shutdown. Thus cognitive techniques could be used for identifying the available bands and use them for public safety communications, thus avoiding spectrum congestion. This is similar to the concept of "white spaces". Note that current policies set by regulators do not allow this type of dynamic spectrum access [13]. However, even now unlicensed bands could be used in scenario 2) (due to white space probably existing also in the unlicensed bands).

The above discussion assumes that the PPDR would be the secondary user of the spectrum. For example, in the US, FCC has allocated the 700 MHz band jointly to public safety and private sector. The private sector has interruptible secondary access to the spectrum, provided that the primary user (public safety) is not present. Shared infrastructure between public safety and private sector will lead to higher cost effectiveness. PSC being the primary user would increase the spectrum utilization and overall efficiency in scenario 1). In this approach, Military and PPDR organizations would be the primary owners of the spectrum bands, but it would allow commercial users to use them or a portion of them during routine operations. In occurrence of a major event or natural disaster, military and PPDR organizations would pre-emptively gain back the spectrum bands by notifying the commercial secondary users (networks and terminals). Such approach would need cognitive radio systems based on SDR, which have the capability of reconfiguring their spectrum usage and reception/transmission parameters.

2) Related spectrum sensing issues (as a secondary user)

Spectrum sensing can never be error-free process. Two metrics for spectrum usage detection are miss detection and false alarms probabilities. If the primary user(s) are not detected (missed detection), spectrum usage is likely to cause interference to the primary user. On the other hand, the band may be detected to be occupied when in fact it is free (false alarm). High false alarm limits the spectrum utilization by secondary radios. There is a tradeoff between false alarm and misdetection probabilities, i.e., if we reduce false alarm, then (for the same parameters) the misdetection probability will be increased. There are several ways to implement spectrum sensing and set the related threshold, but in this paper we will not address them.

Figure 3 provides an indication of the evolution of public safety systems; we note that the key influence is Cognitive Radio – in tune with the strategies which we have listed above. The goal of which is to attain multi-user, multi-channel and multimedia functionality, as indicated in the diagram.

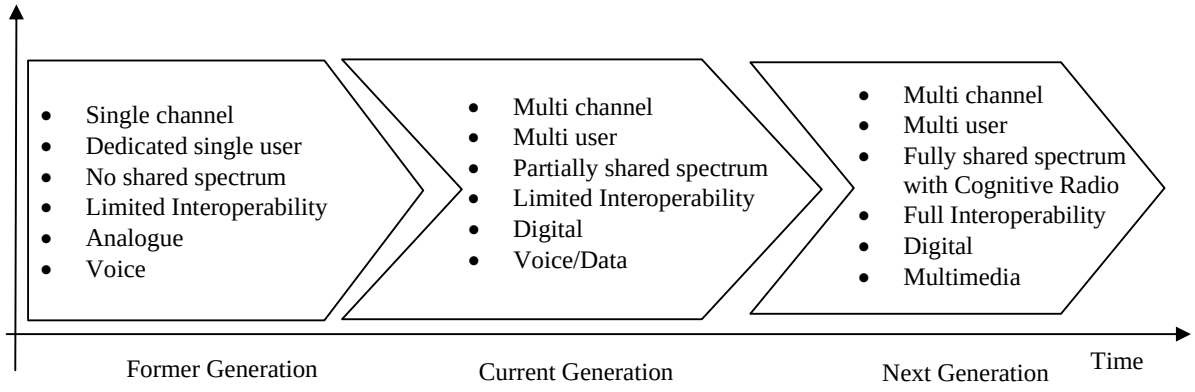

Figure 3. Public-Safety Functionality Evolution

VI. PERCEIVED EULER HDR WF ARCHITECTURE

A. *EULER HDR WF architecture definition*

Among the topics required to address by the EC in the EULER project the high data rate waveform (HDR WF) development requires a specific effort; we refer to a radio processing able to transport data at the rate in the range of 1-100Mbit/s. Even if the channel bandwidth extension depends on the use of spectrally efficient technologies (source coding), this one can spread up to the limit of some 20 MHz specified on IEEE 802.16 standard. The EULER WF Architecture results from the decomposition of a wireless protocol waveform obtained from a customized subset of WiMAX profile in turn defined according to the operational, functional and performance requirements output from the system analysis addressed on the previous section.

Time performances of SW processes running interacting with a Real Time Operative System can be predicted by means the RTOS performances in turn described by timelines among process' threads (process's components) and inter-process communications. Then a design for peak load can be made. All the above considerations are applicable to traditional real time digital signal processing systems.

Figure 4 represents the decomposition of a wireless protocol waveform obtained from a customized subset of WiMAX profile defined according to the operational, functional and performance requirements. It provides also an indicative EULER HDR WF architecture using the SCA based waveform definition; which benefits from:

- Security aspects including the authentication process.
- Link aspects including scheduling
- Physical layer aspects.
- O&M - Operations and Maintenance.
- Backbone infrastructure.

VII. SECURITY ISSUES

A. *Public Safety Information Security Issues*

Security enforcement is constrained by the information sensitive level, the related security clearance owned by each involved user has and the specific operational context. Natural disasters require the support of military forces for their logistic and technology capabilities beyond the participation of non-military forces like Civil Protection and Fire Department. The recovery of the transportation ways like bridge temporary rebuilding is the typical capability provided by specialized military corps. The need of interoperability between military and not-military forces increases within crisis situation caused by terroristic attack and the necessary countermeasures that have to be established. In this case, citizens security and, generally, National security, could require systems able to perform Transmission Security (TRANSEC) and Communication Security (COMSEC, e.g. crypto).

A wider-scale vision of interoperability has to consider all the aspects concerning security and to define specific security profiles for specific operations. In addition, security services have to be available during an emergency together with the Network infrastructure. Hence, crisis operation environment shows a situation where main security services have to be integrated with RAN's components provided by SDRs and the correspondent subsystems hosting AAA:

- **A = Authentication:** the service to ensure that the communication entity is the one that it claims to be.
- **A = Authorization:** function determines whether a particular entity is authorized to perform a given activity.
- **A = Availability:** that the wireless communication resources are available and usable by authorized users.

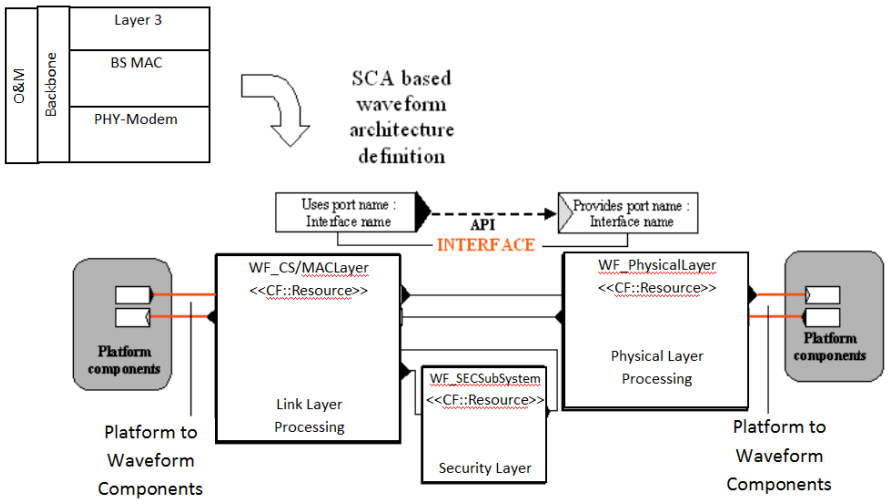

Figure 4. Indicative EULER HDR WF Architecture

There are possibly two meanings to triple A; from the Commercial Operators perspective, the AAA nomenclature would have the third A to represent Accounting; which refers to the tracking of the consumption of network resources. However, for the purposes of the public safety/military world, the aspect of provisioning Availability which is of greater importance.

B. *Security Sublayer Issues*

The platform hardware and software for each SDR node needs to implement the necessary security capabilities; it is possible to take adaptations from the SCA Specification. The complete platform security implementation is out of EULER objectives, which aims at demonstrating a secure WiMAX WF portability between some pre-selected international platforms rather than implementing security within a SDR platform. However, it is worth mentioning the main assets needed to implement a secure SDR set, many of them introduced by SCA Security Annex [16], taking into account that some of them are inherently covered by the Platforms provided in EULER:

- HW, which includes the implementation of an isolated and distributed architecture with different boundaries.
- Operating Environment, includes a secure Operating System, Drivers, Middleware and Core Framework.
- System Applications, integral to the function of the radio or able to service multiple waveforms.

A secure high-data-rate WF, which follows the WiMAX 802.16 Standard, will be implemented in EULER to fulfill some of the requirements identified by Public Services for their communications. The WiMAX standard was selected since it provides several strong mechanisms to resolve these issues, and some additional ones, through two main protocols:

- Key management protocol, known as Privacy Key Management Protocol (PKM), is included to provide secure management and distribution of keying material. PKM is also used to enforce conditional access to network services, providing mutual authentication between nodes and protecting the network from theft of service, and making available a secure key exchange.
- Encapsulation protocol ensures confidentiality and integrity of the packets transmitted across the network. Working in close relation with the PKM protocol, this protocol employs a set of supported cryptographic suites, i.e., pairings of data encryption and authentication algorithms, and other associated data, as keys, IVs and lifetimes.

C. *Compatible Security with Legacy Public Safety systems*

Legacy public safety systems feature a number of security mechanisms including end-to-end encryption removing of any need of trust to existing infrastructure; these systems include both standard algorithms available or national solutions. Furthermore, there are local Key Management Centres with a suite of COMSEC methods which may have National policy.

The EULER security sublayer implementation aims to offer a commensurate suite of security mechanisms and corresponding key management infrastructures which either corresponds or exceeds the minimum level of security which is expected by the end user.

VIII. CONCLUSIONS AND FUTURE DEVELOPMENTS

There is an increasing demand for the Military and public safety services to provision interoperability and support spectrum sharing; this demand is driven by the need to increase the capabilities of military and public safety organizations in the resolution of man-made and natural disasters. The EULER project advocates the use of SDR systems and terminals to implement “spectrum sharing”.

In Europe, spectrum challenges are even more severe than in other political regions, because of the political diversity and consequent fragmentation of Public Safety organizations and spectrum regulations.

We have presented an outline EULER HDR waveform architecture that has the potential to fulfil these needs; the scope of which includes radio channel access, networking and security. Our solution is in the developmental stage and explores these aspects with the target of providing a security commensurate with that expected from legacy systems and significant enhancements to communications and networking with interoperability features.

REFERENCES

[1] “*Efficiency of Use of Public Safety Spectrum in Europe Published by the TETRA Association*” TETRA Association, February 2010.

[2] “*Natural disasters – Biggest insurance losses in 2009*” http://www.economist.com/markets/indicators/displaystory.cfm?story_id=15721454 , 18th March, 2010.

[3] L. Harte, *Introduction to Private Land Mobile Radio: Dispatch*, LTR, APCO, MPT1327, iDEN and TETRA, 2004.

[4] L. Nuaymi, *WiMAX: Technology for Broadband Wireless Access*, 2007.

[5] A. Shah (VANU Inc.), J. Nimmer (VANU Inc.), D. Franklin (Ucentgric Systems), “*A Prototype all-software Public Safety Interoperability System*”, , 2004 Software Defined Radio Technical Conference and Product Exposition, November 15-18, 2004 - Phoenix, Arizona.

[6] ECC Decision (08)05 on the harmonisation of frequency bands for the implementation of digital Public Protection and Disaster Relief (PPDR) radio applications in bands within the 380-470 MHz range.

[7] K. Koufos, K. Cziner and P. Parviainen, "*Multicast Video Performance Evaluation for Emergency Response Communications*". ISCRAM 2007

[8] PSC-Europe/EG/2007/002_v2 Spectrum Petition for Public Protection and Disaster Releif.

[9] Qi Wang; Brown, T.X.; , "*Public safety and commercial spectrum sharing via network pricing and admission control*," Selected Areas in Communications, IEEE Journal on , vol.25, no.3, pp.622-632, April 2007.

[10] WiMAX forum www.wimaxforum.org

[11] http://www.fcc.gov/pshs/techtopics/techtopics11.html

[12] L. Berlemann, C. Hoymann, G. Hiertz, B. Walke, “*Unlicensed Operation of IEEE 802.16: Coexistence with 802.11(A) in Shared Frequency Bands*”, PIMRC 2006.

[13] FCC Web site http://www.fcc.gov/pshs/techtopics/techtopic9.html

[14] W. Lehr and N. Jesuale, "*Public safety radios must pool spectrum*," Communications Magazine, IEEE , vol.47, no.3, pp.103-109, March 2009

[15] JPEO JTRS, *Software Communications Architecture Specification*, Version 2.2.2, 15th May 2006.

[16] JPEO JTRS, *Security Supplement to the Software Communications Architecture Specification*, MSRC-5000, SEC V1.1, 17th November 2001