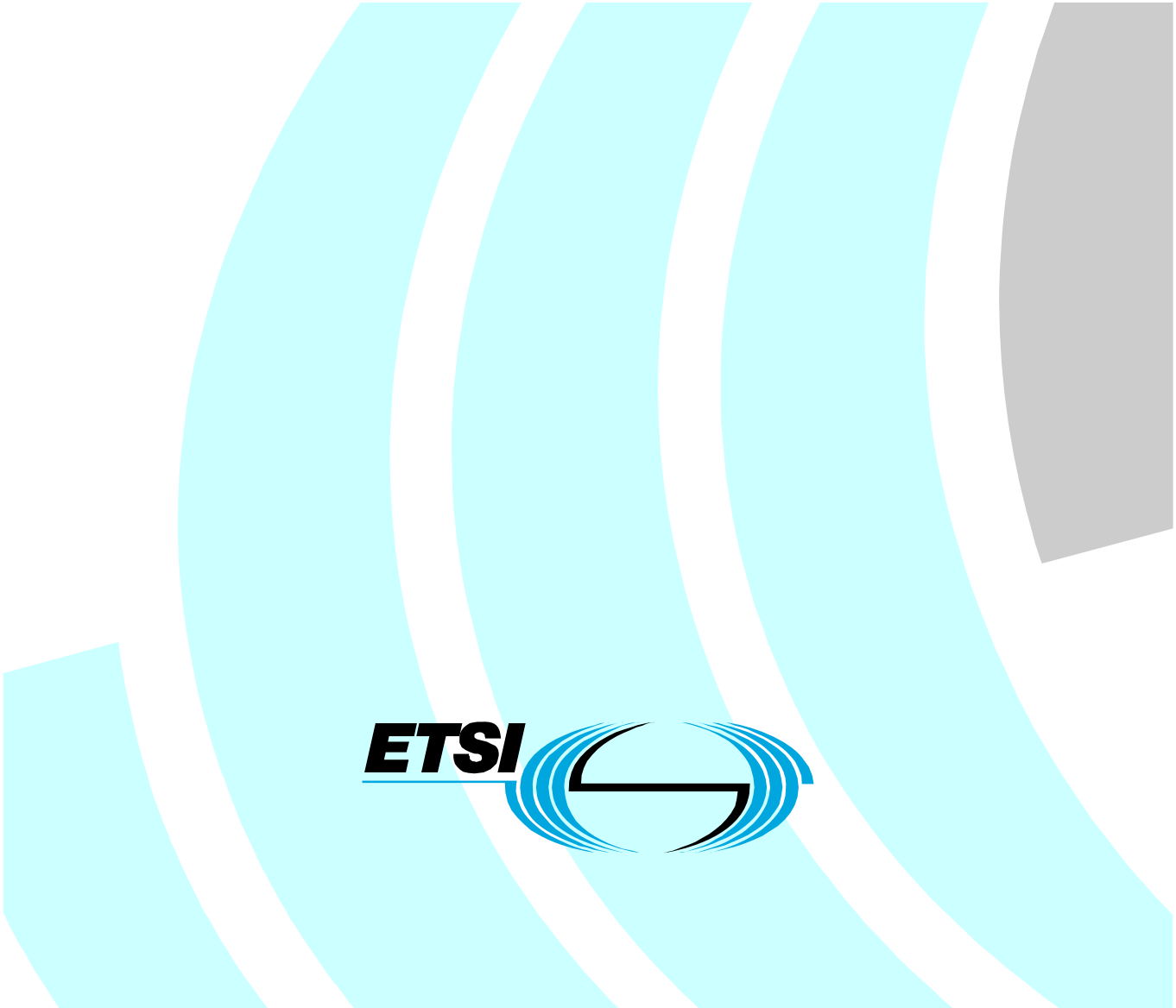
# ETSI TR 103 064 V1.1.1 (2011-04)

*Technical Report*

**Reconfigurable Radio Systems (RRS);
Business and Cost considerations of
Software Defined Radio (SDR) and
Cognitive Radio (CR) in
the Public Safety domain**



Reference
DTR/RRS-04007

Keywords
radio, safety

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Contents

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

# Introduction

The present document provides a study of the business and cost considerations for the deployment of Software Defined Radio and Cognitive Radio technologies (i.e. RRS technologies) in the Public Safety domain.

While RRS technologies can provide significant benefits and improve the operational capabilities of public safety organizations, their implementation and deployment may be heavily dependent on cost trade-offs. Business and cost considerations are common to all telecommunications markets, but there are significant differences between public safety domain and the commercial domain. One difference is that funding for Public Safety organizations is usually decided at political/government level and budget for new radio equipment may be limited or approved in specific timeframes. Another difference is that radio equipment used by Public Safety organizations has usually a longer lifecycle than a commercial domain. It is not uncommon the deployment of dedicated networks for 10-15 years of service. The different operational requirements for security, availability and reliability have also a considerable impact on the cost of communication equipment.

All these considerations may drive the evolution of communication technology in the Public Safety domain.

The present document describes the business and cost drivers, the potential evolution paths, the main specific features of the Public Safety radio equipment and the potential economical benefits of RRS technologies.

# 1 Scope

The current trend in Public safety communications today are characterized by a patchwork of separate, sometimes incompatible systems (e.g. TETRA and TETRAPOL) with widely varying capabilities in communicating between and amongst systems and user radios. Another key challenge is the lack of broadband connectivity to support the operational capabilities of Public Safety responders. Software Defined Radio (SDR) and Cognitive Radio (CR). technologies, here collectively described as RRS technologies can be a key component to improve the interoperability and to increase the flexibility and ability to public safety communications.

The scope of the present document is to investigate the business and cost considerations in the application of SDR and CR to the Public Safety domain. In particular the present document presents:

- the impact of SDR/CR technologies on the lifecycle cost model for public safety communication equipment.
- identification of the benefits or disadvantages of SDR/CR technologies, from an economical point of view, in comparison to conventional (but already digital) communication systems.
- definition of a business model able to develop the capabilities offered by SDR/CR adoption and to lower the life cycle costs associated with SDR/CR introduction.
- Definition of a cost model for SDR/CR technologies in Public Safety.

# 2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

## 2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

## 2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Public Safety Radio System Cost Model. SDRF-09-P-0001-V1.0.0. Wireless Innovation Forum (ex SDR Forum). Approved 21 April 2009.

NOTE: Available at http://www.wirelessinnovation.org. Last accessed 21/01/2011.

[i.2] "TETRA versus GSM for Public Safety".

NOTE: Available in the reports section in http://www.tetra-association.com/uploadedFiles/Files/Documents/TETRAorGSMinPS.zip.

[i.3] ETSI TR 102 745: "Reconfigurable Radio Systems (RRS); User Requirements for Public Safety".

[i.4] ETSI TR 102 680: "Reconfigurable Radio Systems (RRS); SDR Reference Architecture for Mobile Device".

[i.5] ETSI TR 102 021 (parts 1 to 8): "Terrestrial Trunked Radio (TETRA), User Requirement Specification TETRA Release 2".

[i.6] Report for the TETRA association from Analysis Mason. Public Safety mobile broadband and spectrum needs. Final Report 8 March 2010. 16395-94.

[i.7] Cognitive Radio Technology: A Study for Ofcom. Final Report, by QinetiQ LTD, Multiple Access Communication Limited, University of Surrey, University of Strathclyde, and Red-M., dated February 12, 2007.

[i.8] D3.13: "Market issues study".

NOTE: Available at http://www.psc-europe.eu in the library section. Last accessed 21/01/2011.

[i.9] 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.

[i.10] ECC Recommendation (08)04 on the identification of frequency bands for the implementation of Broad Band Disaster Relief (BBDR) radio applications in the 5 GHz frequency range.

[i.11] Jon M. Peha, "Sharing Spectrum through Spectrum Policy Reform and Cognitive Radio," Proceedings of the IEEE, Volume 97, Number 4, pp. 708-719, April 2009.

[i.12] ETSI TS 102 181 (V1.2.1): "Emergency Communications (EMTEL); Requirements for communication between authorities/organisations during emergencies".

[i.13] WINTSEC, D2.2: System Architecture for Interoperability - Core Network Layer, Roadmap for Subsystem Integration.

[i.14] D2.1: "Report on ICT Research and Technology Development status for public safety".

NOTE: Available at http://www.psc-europe.eu in the library section. Last accessed 21/01/2011.

[i.15] ETSI EN 300 392-1 (V1.4.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[i.16] ETSI TR 101 448 (V1.1.1): "Terrestrial Trunked Radio (TETRA); Functional requirements for the TETRA ISI derived from Three-Country Pilot Scenarios".

[i.17] "TETRA and the Inter System Interface (ISI)", white paper by TETRA Association, August 2010.

NOTE: Available at http://www.tetramou.com/ in Library/Reports. The white paper describes the status of TETRA interoperability and the Inter System Interface (ISI).

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Cognitive Radio (CR):** radio, which has the following capabilities:

- to obtain the knowledge of radio operational environment and established policies and to monitor usage patterns and users' needs;
- to dynamically and autonomously adjust its operational parameters and protocols according to this knowledge;
- in order to achieve predefined objectives, e.g. more efficient utilization of spectrum; and
- to learn from the results of its actions in order to further improve its performance.

**Cognitive Radio System (CRS):** radio system, which has the following capabilities:

- to obtain the knowledge of radio operational environment and established policies and to monitor usage patterns and users' needs;
- to dynamically and autonomously adjust its operational parameters and protocols according to this knowledge in order to achieve predefined objectives, e.g. more efficient utilization of spectrum; and
- to learn from the results of its actions in order to further improve its performance.

NOTE 1: Radio operational environment encompasses radio and geographical environments, and internal states of the Cognitive Radio System.

NOTE 2: To obtain knowledge encompasses, for instance, by sensing the spectrum, by using knowledge data base, by user collaboration, or by broadcasting and receiving of control information.

NOTE 3: Cognitive Radio System comprises a set of entities able to communicate with each other (e.g. network and terminal entities and management entities).

NOTE 4: Radio system is typically designed to use certain radio frequency band(s) and it includes agreed schemes for multiple access, modulation, channel and data coding as well as control protocols for all radio layers needed to maintain user data links between adjacent radio devices.

**public safety organization:** organization which is responsible for the prevention and protection from events that could endanger the safety of the general public

NOTE: Such events could be natural or man-made. Example of Public Safety organizations are police, fire-fighters and others.

**radio technology:** technology for wireless transmission and/or reception of electromagnetic radiation for information transfer

**RRS network node:** wireless communication terminal or base station which has cognitive radio capabilities or which is based on software defined radio concepts

**non-RRS network node:** wireless communication terminal or base station, which does not have cognitive radio capabilities or is not based on software defined radio concepts

EXAMPLE: A non-RRS network node is a conventional wireless communications systems based on TETRA standard version 1.

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| A/D | Analog Digital |
| AAA | Authentication, Authorization and Accounting |
| ADC | Analog-to-Digital Converter |
| APCO | Association of Public Safety Communications Officials, International, Inc |
| API | Application Programming Interfaces |
| BBDR | Broad Band Disaster Relief |
| BS | Base Station |
| CAP | Common Alerting Protocol |
| CEPT | European Conference of Postal and Telecommunications Administration |
| COMSEC | Communication Security |
| CORBA | Common Object Request Broker Architecture |
| CR | Cognitive Radio |
| D/A | Digital Analog |
| DAC | Digital-to-Analog Converter |
| DDC | Data Download Control |
| DEC | DECoder |
| DMO | Direct Mode of Operation |
| DQPSK | Differential Phase Shift Keying |
| DSP | Digital Signal Processor |

| | |
|---|---|
| DUC | DLC User Connection |
| ECC | Electronic Communication Committee |
| ENB | Equivalent Noise Bandwidth |
| FCC | Federal Communication Commission |
| FM | Frequency Modulation |
| FPGA | Field Programmable Gate Array |
| GPRS | General Package/Packet Radio Service |
| GPU | Graphics Processing Unit |
| GSM | Global System for Mobile communications |
| HMI | Human Machine Interface |
| HQ | Head Quarters |
| HW | HardWare |
| ICT | Information and Communication Technologies |
| IF | Intermediate Frequencies |
| ISDN | Integrated Service Data Network |
| ISI | Inter System Interface |
| LAN | Local Area Network |
| LINK | Access link |
| LTE | Long Term Evolution |
| MS | Mobile Station |
| NET | Network |
| NMS | Network Management System |
| NSD | Noise Spectral Density |
| OE | Operating Environment |
| OFCOM | UK communications regulator |
| OFDMA | Orthogonal Frequency Division Multiple Access |
| PAMR | Public Access Mobile Radio |
| PC | Personal Computer |
| PHY | PHYsical |
| PIM | Platform Independent Model |
| PMR | Professional Mobile Radio |
| PPDR | Public Protection and Disaster Relief |
| PS | Public Safety |
| PSAP | Public Safety Answering Points |
| PSBL | Public Safety Broadband License |
| PSC | Public Safety Communications |
| PSCE | Public Safety Communication Europe |
| PSM | Platform Specific Model |
| PSSIG | Public Safety Special Interest Group |
| PSSTC | Public Safety Spectrum Trust Corporation |
| PTT | Push to Talk |
| QAM | Qadrature Amplitude Modulation |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RAT | Radio Access Technologies |
| RF | Radio Frequency |
| RRS | Reconfigurable Radio Systems |
| RX | interface signal Receiver |
| SCA | Software Communications Architecture |
| SDR | Software Defined Radio |
| SDRF | Software Defined Radio Forum |
| SEC | Security |
| SRT | Smart Radio Terminal |
| SW | Software |
| SwCN | Switching and Control Link |
| SwMI | Switching and Management Infrastructure |
| TDM | Time Division Multiplexing |
| TEDS | TETRA Enhanced Data Service |
| TETRA | TErrestrial Trunked Radio |
| TETRAPOL | Proprietary digital private mobile radio network |
| TIP | Tetra Interoperability Profiles |
| TRANSEC | Transmission Security |

| | |
|---|---|
| UHF | Ultra High Frequency |
| UMTS | Universal Mobile Telecommunications System |
| VHF | Very High Frequency |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WinF | Wireless Innovation Forum |
| xPSK | any Phase Shit Keying |

# 4 Relevant input from other organizations

This clause provides the list of input documents and information sources, which are relevant to the present document. The list includes deliverables and other documentation produced by organizations or projects.

Clauses 4.1.and 4.2 list the more relevant references and the relevant information to the present document.

NOTE: As described in the scope of the present document is to define the System Design aspects for the application of RRS to the Public Safety domain. The scope is not to define a new radio system for Public Safety. This means that some of the listed references will not be a direct input to the present document, even if they may still provide useful information.

EXAMPLE: An input document may describe Public Safety communication standards, which an RRS platform should support through waveforms.

## 4.1 Organizations

### 4.1.1 ETSI TETRA

TErrestrial Trunked RAdio (TETRA) is a digital trunked mobile radio standard developed to meet the needs of traditional Professional Mobile Radio (PMR) user organizations such as:

- Public Safety.
- Transportation.
- Utilities.
- Government.
- Military.
- PAMR.
- Commercial & Industry.
- Oil and Gas.

The document [i.17] is relevant for the present document. The white paper describes the status of TETRA interoperability and the Inter System Interface (ISI).

### 4.1.2 PSCE Public Safety Communication Europe (NARTUS)

The project NARTUS focuses on establishing and facilitating a Forum for regular exchange of ideas, information, experiences and best practices, and on seeking agreement among participating stakeholders.

The following documents are relevant for business and cost considerations:

- D2.1: "Report on ICT Research and Technology Development status for public safety". The purpose of the present document is to provide a list of background technical material of relevance for public safety communication [i.14].

- D3.13: "Market issues study". This document is intended for Public Safety Communications (PSC) stakeholders, including members of the PSC services (fire, police, ambulance and civil protection), manufacturers of PSC systems (applications, services, networks and terminals) and public authorities (strategic planning and purchasing decision makers). It discusses the major market issues associated with Public Safety Communications Services. The following issues are identified: the size of the Public Safety market, user requirements and their impact on the network, the long in-service period of the technology and the costs and the public-funded nature of the purchasing [i.8].

### 4.1.3 Wireless Innovation Forum

The Wireless Innovation Forum (WinF), which was previously called Software Defined Radio Forum (SDRF), is a non-profit organization comprised of approximately 100 corporations from around the globe dedicated to promoting the development, deployment and use of software defined radio technologies for advanced wireless systems.

The following documents are relevant for investigation of business and economic impact of SDR and CR technologies:

- Public Safety Radio System Cost Model. SDRF-09-P-0001-V1.0.0. This report, written by the Public Safety Special Interest Group (PSSIG) of the SDR Forum, describes a tool for estimating total lifecycle costs associated with any public safety radio system and a methodology for determining cost impact to that system for incorporating new SDR technologies [i.1].

- Quantifying the Benefits of Cognitive Radio. WINNF-09-P-0012-V1.0.0. This report provides the results of an extensive survey on open and public CR literature to assess the value proposition of CR [i.1].

WinF has also produced market studies on SDR and Public Safety, but they are not available per public access.

## 4.2 Projects

### 4.2.1 EULER project

The FP7 EULER project (www.euler-project.eu) gathers major players in Europe in the field of wireless systems communication integration and software defined radio (SDR), is supported by a strong group of end-users, and aims to define and actually demonstrate how the benefits of SDR can be leveraged in order to enhance interoperability in case of crisis needed to be jointly resolved. The proposed activities span the following topics: proposal for a new high-data-rate waveform for homeland security, strengthening and maturing ongoing efforts in Europe in the field of SDR standardisation, implementation of Software defined radio platforms, associated assessment of the proposal for high-data-rate waveform for security, and realisation of an integrated demonstrator targeted towards end-users. Significant interaction with E.U stakeholders in the field of security forces management will contribute in shaping a European vision for interoperability in joint operations for restoring safety after crisis.

# 5 Requirements and evolution paths for the Public Safety domain

## 5.1 Introduction

Public Safety (PS) applications and related users represent a market environment, which can be quite different from the commercial one regarding various aspects.

The main differences, both operational and technical, are described in Figure 1.

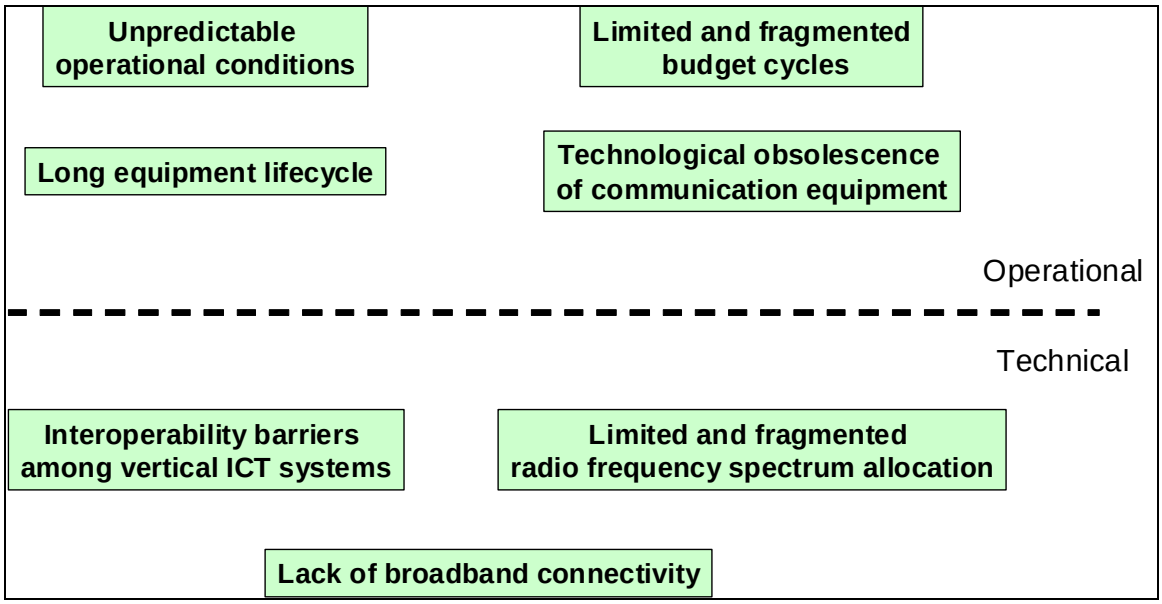



**Figure 1: Specific features of the Public Safety domain**

- **Limited and fragment budget cycles.** Funding for PS organizations is usually decided at political/government level and budget for new radio equipment may be limited or approved in specific timeframes. Furthermore, the budget is usually allocated to different public safety organizations.
- **Unpredictable operational conditions.** Natural disasters and emergency crisis are often unpredictable and they require PS officers to operate in difficult environment due to degraded or destroyed infrastructures.
- **Long equipment lifecycle.** Dedicated network infrastructures for PS organizations are usually created and deployed for a long timeframe (e.g. 10 to 15 years).
- **Technological obsolescence.** Because of the long equipment lifecycles, specific requirements and smaller market size, the services offered by PS communication equipment are usually less sophisticated than their commercial counterparts.
- **Interoperability barriers.** Interoperability barriers among the communication systems of various PS organizations are still present both a national level (among public safety organizations of the same region or nation) and at European level among PS organizations from different nations. Interoperability barriers are usually based on historical reasons: communication networks are created by each PS organization with a vertical structure to address the specific requirement of the organization.
- **Limited or fragmented radio frequency spectrum allocation.** Radio frequency spectrum is allocated to various PS organizations in a fragmented way. Furthermore, in specific geographical regions (e.g. Europe), spectrum can be allocated differently at national level.
- **Lack of broadband connectivity.** Existing or new PS applications are driving the need for broadband connectivity to transmit images or video, but there may not be available spectrum to support such needs. As consequence of changes in working practices, PS users are requiring broadband network capability in order to carry out video image transferring other than voice channel groups, all that maintaining a minimum level of resilience (see note), that is the combination of availability and reliability.

NOTE: Public Safety networks and terminals have to satisfy severe requirements of availability (i.e. 0,99999) and reliability meant as the capacity to withstand and recovery from failures.

Beyond these specific features, PS domain has also specific operational requirements, which are defined in clause 5.2.

## 5.2 Public Safety requirements

This clause has the purpose to identify the public safety requirements, which are the main cost drivers for the deployment of SDR and CR technologies in the Public Safety domain.

We can identify the following requirements:

- Interoperability. Public Safety organizations use a variety of communications systems based on different standards: mainly TETRA + TETRAPOL, but also Satellite communications, analog PMR, commercial systems (e.g. GSM/GPRS/LTE) and others. Such variety can create interoperability barriers for Public Safety responders and control centres.

- Radio coverage. Public Safety organizations need to operate both outdoor and indoor in variety of operational contexts including urban and rural areas.

- High data-rate communication. New public safety applications (e.g. mobile video surveillance) require wideband (i.e. 100 Kbits to 1 Mbits), and broadband connectivity (i.e. > 1 Mbits).

- Security. The network has to guarantee the protection of the transmitted/stored data and regulated access to communication services.

- Resilience, meant by the combination of availability and reliability. Public Safety networks and terminals have to satisfy severe requirements of availability (i.e. 0,99999) and reliability meant as the capacity to withstand and recovery from failures.

- Upgradeability. The deployment of dedicated Public Safety networks is usually very demanding for Public Safety organizations from an economic point of view. A national or regional network is usually an investment for 10 to 15 years or more.

- Energy efficiency. Public Safety officers are supposed to work and use their communications equipment for all the duration of an emergency crisis, which can last many hours or days. For usability reasons, handheld terminals cannot have large or heavy batteries. As a consequence, energy efficiency is an important requirement.

- Waveform reconfigurability. The capability to activate different waveforms to adapt to the environment conditions and equipment of the various public safety organizations.

The requirements described above translate to technical requirements and specifications for networks based on SDR and CR technology. For example, interoperability requires that a handheld terminal is able to establish a wireless connection to various communication systems and in a wider set of frequencies than a conventional terminal. This implies that the handheld terminal could be equipped with various front-ends and antenna. High-data-rate communication may instead have an impact on frequency plan and the related frequency management.

Communication systems based on SDR and CR technologies have to validate the technical requirements of the communications technologies used in the Public Safety domain including TETRA [i.5], Satellite Communications, Analog PMR and even commercial systems (e.g. LTE). The technical requirements are defined in the respective technical standards , but some common requirements include:

- **Dynamic range**: the need for high quality voice requires stringent adjacent channel rejection and intermod rejection requirements, which translates to A/D converters with many bits.

- **Spectral purity in transmission**: this requirement imposes stringent specification to transmit modulator (including D/A converters), power amplifiers, frequency synthesizer design, and transmission filtering.

The technical requirements and specifications, with further detail, are investigated separately for SDR and CR technology in clause 7.

Beyond the requirements described above, business consideration for the deployment of SDR and CR technologies in the Public Safety domain are also dependent on the potential evolution paths for Public Safety communications.

## 5.3 Potential evolution paths for Public Safety communications

At the current time (i.e. 2011), SDR and CR technologies are still considered in an early phase for deployment in the Public Safety domain. Critics of SDR technology suggest that deployment of these technologies can happen from 5 to 15 years in the future depending on the complexity of the proposed solution or the market drivers. Consequently, it is also important to describe what the potential evolution paths for Public Safety communications are. Each evolution path can have a positive or negative impact on the deployment of SDR/CR technologies.

Today, the following trends are driving the evolution of Public Safety telecommunication technologies:

1) Voice communications has always been the main critical mission application, but data communication is increasingly used to support a number of public safety applications.

2) The progress of the European integration is a driving force for a closer cooperation among Public Safety organizations across Europe. As a consequence, there is increasing support at political level to remove interoperability barriers (operational or technical) among national organizations or among European member states.

3) Security challenges like terrorism and environment disasters have raised public awareness and increase the political support to increase the capability and efficiency of Public Safety organizations.

4) Government entities, industry and regulators are advocating a closer integration between public safety and commercial network infrastructures.

5) New public safety applications require new use and approaches for telecommunications: ad-hoc networks, sensor networks, support to high data rate ground-air links are some examples.

On the other side, conservative forces may obstacle the evolution of Public Safety communications:

1) Public Safety organizations have already made large investment in dedicated networks based on TETRA and TETRAPOL standards across Europe. It is unlikely that these infrastructures are replaced with new technologies in the near future.

2) Security and data protection are essential requirements in the Public Safety domain. Public Safety organizations have the concern that their data is safely protected from unwanted access by outsiders. Solutions to provide full interoperability may not be accepted if they do not provide adequate security.

3) Radio Frequency spectrum is increasingly congested for an increasing number of services and it may not be available for future technical solutions.

We can identify the following evolutions paths or future scenarios for Public Safety communications. Each of these scenarios can have a significant impact on the development and adoption of SDR and CR technologies. The implications of each evolution path are described below. More details are in the clause 7.

**Table 1**

| Evolution Impact | Implications for SDR technology | Implications for CR technology |
|---|---|---|
| Slow incremental growth. In this evolution path, working methods and infrastructures changes slowly. The deployment of new technologies is not encouraged and most of the efforts are dedicated to increase the efficiency of existing dedicated infrastructures. Availability of economical investment in the Public Safety sector is limited. Voice communications remains dominant. There is lack of political support for cross-border interoperability among Public Safety organizations of different member states. Public Safety network and commercial networks are separated. No new spectrum bands are allocated to Public Safety. | Deployment of SDR technology is slow as Public Safety organizations rely on existing dedicated infrastructures. The only development is related to research project and prototypes.<br>The SDR developments in the commercial and military domain are not translated to similar development in the public safety domain. | Development of CR technology is limited or nonexistent. |
| Information driven growth. In this evolution path, data communication is increasingly used to support voice communications. Wideband (i.e. up to 1 Mbits) communications is available and it is used to support a number of applications, including the creation of a "situational awareness picture" which can be shared among public safety officers in the field and in the control centres. Limited cross-border interoperability is available for voice and some data applications. There is limited use of commercial networks to support non-mission critical applications. Harmonized limited spectrum is allocated to Public Safety. There is a limited integration between commercial and public safety networks. | Very simple SDR technology is used in prototypes. There may be a limited deployment of multi-standards base stations and terminals, both vehicular and handheld in pilot projects and trials to support cross-border interoperability and inter-organizations communications. In this context multi-standards base stations (both fixed and mobile) could be used as a "relay" between two different communications systems. Multi-standards terminals can also be used to interface both public safety and commercial networks. | Simple form of spectrum sharing can be implemented and deployed in occasion of emergency crisis to address the increase of traffic. Simple multi-band base stations handheld and terminals can be used to address the lack of harmonization of spectrum bands across Europe. |
| Full multimedia and convergent networks. In this evolution path, data communication is the predominant form of communications and it is also used for mission critical applications. Political consensus is able to provide support for a significant improvement of public safety networks. Public Safety officers are used to conduct their operation on the basis of broadband applications like common operational picture. Interoperability barriers are removed through a number of technological solutions both a field level and among control centres. Innovative approaches for spectrum management allow a flexible use of the spectrum to accommodate needs of traffic capacity and broadband connectivity in the occurrence of emergency crisis or natural disasters. Commercial, military and public safety networks are fully integrated with resource management sharing solutions. | Full fledged SDR base stations and terminals are deployed in the Public Safety domain to provide full interoperability.<br>SDR technology is used to integrated public safety dedicated networks and commercial networks.<br>SDR base stations and terminals have the processing capability to support a wide range of communications standards.<br>Mass volume market and evolution of components technologies allow economies of scale for SDR technologies and components and upgrading of the Public Safety networks infrastructures to SDR based technology<br>Multi-levels security is implemented to provide support to public safety organizations with different levels of security. | New spectrum management approach like Dynamic Spectrum Access allows improved spectrum utilization.<br>Ad-hoc networks based on CR technology can be used to support first time responders in the field. |

The above potential evolution path provide other reasons to adopt Reconfigurable architectures and the level to apply reconfiguration (concerning functional requirements) and business involvement (useful characteristics offered by RRS adoption and not by conventional products):

- Policies adoption can require the interoperability with different procedures and different communication technologies due to national based different standards adoption. This can occur in cross-border operations or international aid operations.

- Spectrum sharing procedures adoption that allow PS networks to enjoy strict pre-emption (of the portion of the spectrum let to commercial and other entities) without fear of interference from these sharers.
- Definition of the main interfaces between PS networks and other networks to support interoperability at MS and BS levels and joint resource management.
- Interaction between PS networks and local ones eventually still active in urban and sub-urban areas. Local networks are different among geographical areas.
- Different policies and RAN technologies can be set and evolve independently.

Just for the sake of summary we can list the following reconfiguration related issues:

- Interoperability with national backbones, both public like 3/4 G and professional reserved like satellite networks.
- Security policies adoption according to pre-set configurations or on-field dynamically managed.
- Spectrum policies adoption according to pre-set frequencies plans or on-field dynamically managed with Cognitive Radio technologies.
- Interoperability among different RATs adopted by different PS involved users.
- Group-calls management through heterogeneous networks, where the term "heterogeneous" is due to different RAT/N and different users with common policies to adopt.
- PS dedicated networks could provide a set of centralized services, with remote services eventually connected, to the RATs and users involved on PS operations.
- Best effective adaptation to policies and technologies evolution.

The last issue could be the more sensitive reason to require RRS technology.

As far as **spectrum policies** are concerned, the SDR technology provides an effective contribution to the interoperability but in order to complete the effort at radio communication infrastructure level, an European harmonized spectrum policy has to be adopted. In 2008, ECC/CEPT committee provided a decision on the harmonization of frequency bands for the implementation of digital Public Protection and Disaster Relief (PPDR) radio applications in bands within the 380 MHz to 470 MHz frequency range (ECC/DEC/(08)05) [i.9]. This ECC Decision covers narrow band (see note 1) as well as wide band (see note 2) PPDR radio applications. Spectrum within the duplex bands 380 to 385 MHz/390 to 395 MHz has been designated for narrow band PPDR radio applications.

NOTE 1: Channel spacing up to 25 KHz.

NOTE 2: Channel spacing of 25 KHz or more, at least up to 150 KHz.

The provisions of the above ECC Decision regarding the wide band systems are based on a "tuning range" (see note 3) concept which provides flexibility for the administrations by implementing this Decision (within the tuning range on a national basis). The aim is to make radio spectrum available for wide band PPDR radio applications either in the 385 MHz to 390 MHz/395 MHz to 399,9 MHz sub bands, in the 410 MHz to 420 MHz/420 MHz to 430 MHz sub bands or in the 450 MHz to 460 MHz/460 MHz to 470 MHz sub bands. In the same period CEPT developed ECC Recommendation 08-04 [i.10] concerning frequency bands for the implementation of Broad Band Disaster Relief (BBDR) which recommends that administrations have to make available at least 50 MHz of spectrum for digital BBDR radio applications. However, this spectrum is shared with radio LANs and may be available for disaster relief during major incidents.

NOTE 3: Here we refer to harmonized frequency spectrum bands where the specific channels (tuning ranges) are defined on a national basis. The real application of the decision is based on national possibilities and national market demands and the indicated sub bands may not available in all CEPT countries.

Then a real harmonized band at European level exists only for narrow band level and currently it is quite difficult to identify new harmonized bands across Europe below 1 GHz. Above 1 GHz, the WiMAX frequency allocation is diffusing in the range 3,4 GHz to3,6 GHz with a good harmonization level.

Broadband capable networks (i.e. video) have as competitor solutions WiMAX and LTE and no definitive standard seem to be proposed for wideband application. Then, just as summary, the issue concerning "*Best effective adaptation to policies and technologies evolution*" refers the following ones:

- Rules fragmentation and delay at European level (only 10 MHz currently harmonized but other national based frequencies ranges are currently used in Europe).
- Different narrowband technologies (FM VHF, TETRA, TETRAPOL).
- Need to capitalize the current technology development investment allowing to adopt modular and incremental new technology insertion moving from the current narrow band solutions to the next wide and broad band technologies (from TETRA/TETRAPOL to TETRA TEDS and WiMAX/LTE).
- Many broadband technologies candidate and not yet a specific one to be considered like a favourite standard (ex. WiMAX Vs LTE) stress the investments decisions that can be effectively overcome by RRS adoption.

Many countries have their PS network (fully or partially private) and many of them have experienced many times what are the real capabilities of their networks. Interoperability lacks, radio coverage and traffic limitation, deployment time are been tested and the lessons learned are been collected. Some PS operators have verified how network models and resources can be efficient in some conditions but the same ones could be ineffective or with degraded performances in other scenarios.

The work carried out on PS area during last year does not aim only to resolve the radio communication limitation and the bandwidth enhancement, but it aims somewhat to resolve the interoperability gap and to set the basis for an effective new RAT integration. Broadband technologies for PS are already under design by several suppliers but this does not mean the current technologies will be early replaced. There may be a timeframe, where multi RATs and legacy systems coexist.

Reconfigurable systems tailored for PS application can be an effective help to deploy all-field solutions.

Then, with the above PS requirements and the potential reconfiguration capability applications on PS, an analysis can be carried out concerning the level the reconfiguration, which can be applied.

# 6 Reconfigurability benefits and trade-offs

Public Safety officers are able to specify the relations among authorities and organisations during emergencies in term of **policies** or **procedures** and required **services** (see also [i.12]). Among them there are the procedures involving Public Safety Answering Points (i.e. PSAPs) and emergency control centres, the latter also connecting with the mobile rescue teams and single rescuer or agent. In specific operational scenarios, military forces can also get involved and the relation between military authorities and civil ones has to be considered.

Then, in order to define the requirements of a PPDR communication network, first of all the operational requirements and the applicable procedures have to be considered. Subjects as time to deployment, security, interoperability, resilience, multi functions and distributed services requiring also high data-rate communication are the main requirements to meet to specify an effective next generation PS communication network adopting state of the art Radio Access Technology/Network (RAT/N) technologies.

As first step to develop in order to highlight the reasons to adopt Reconfigurable Radio System on PS communication networks, we can consider the following scenarios:

- In urban area, or sub-urban area, however where only locally the communication has to be re-established, at maximum extension involving one or more available backbone commercial RAT (e.g. GSM). In this situation a wide backbone is still active and the proper Spectrum Management has to be carried out (spectrum sharing and policies adoption referred to primary and secondary users; see note 1).

NOTE 1: PS is the "primary" user of the spectrum of which a portion is shared with other networks.

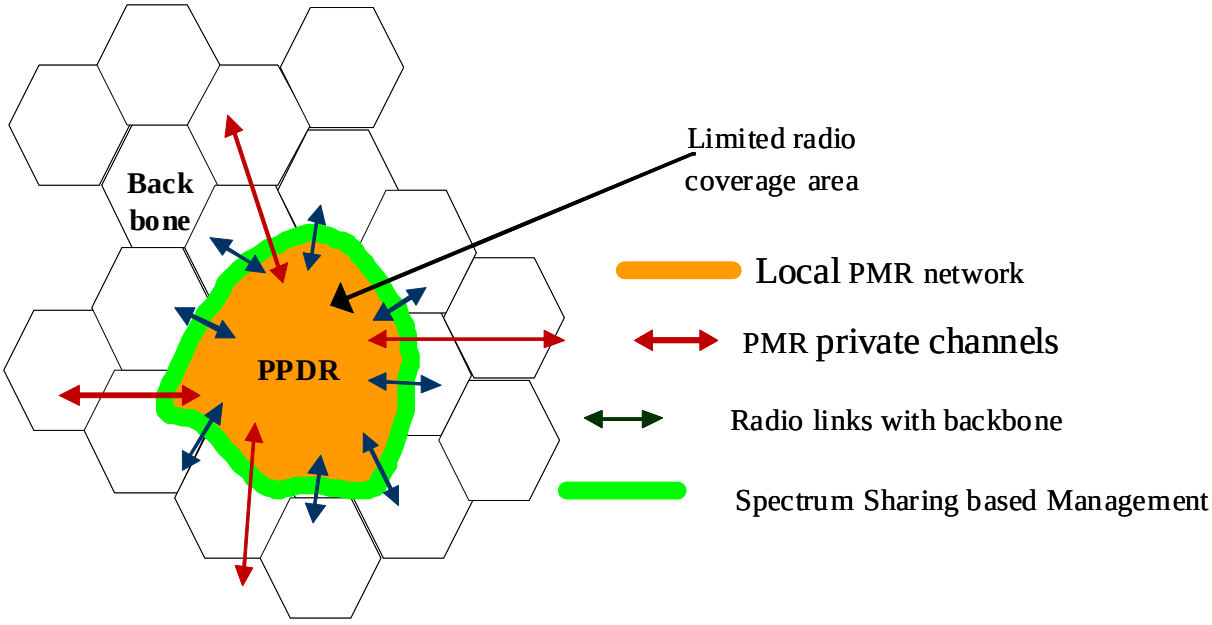



**Figure 2: Urban area operations**

- In isolated area where the communication re-establishment is a critical challenge but the spectrum policies are easier to adopt with less constraints.

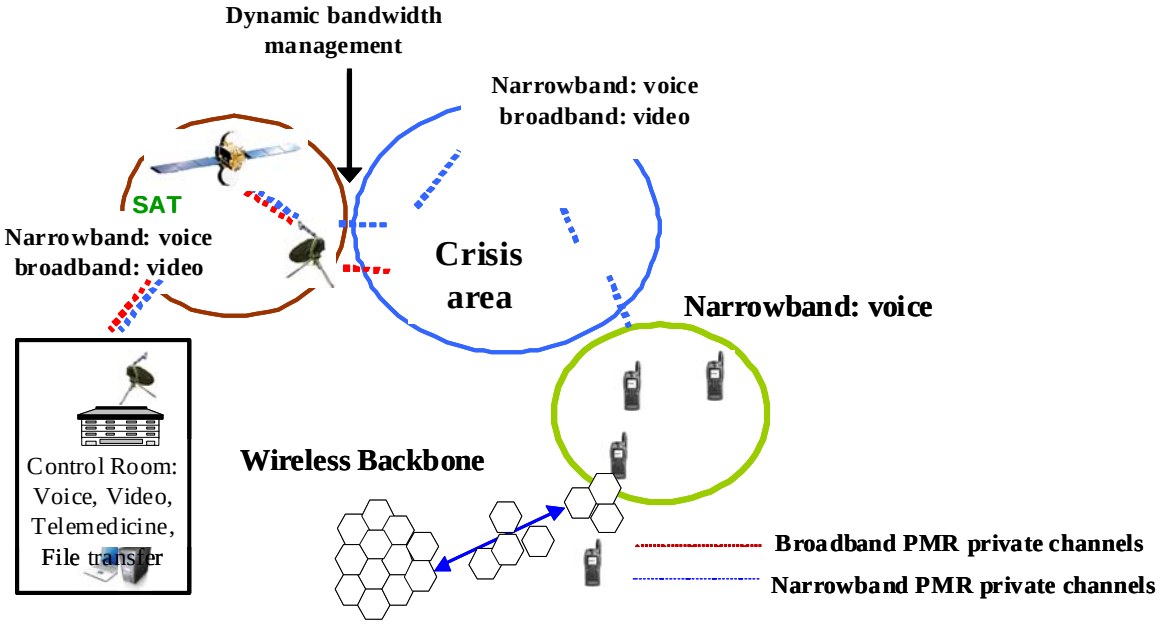



**Figure 3: Wide area communication re-establishment operations**

- In cross-border situation, eventually occurring on sub-urban or wide isolated area. Then specific policies for cross-border management have to be applied.

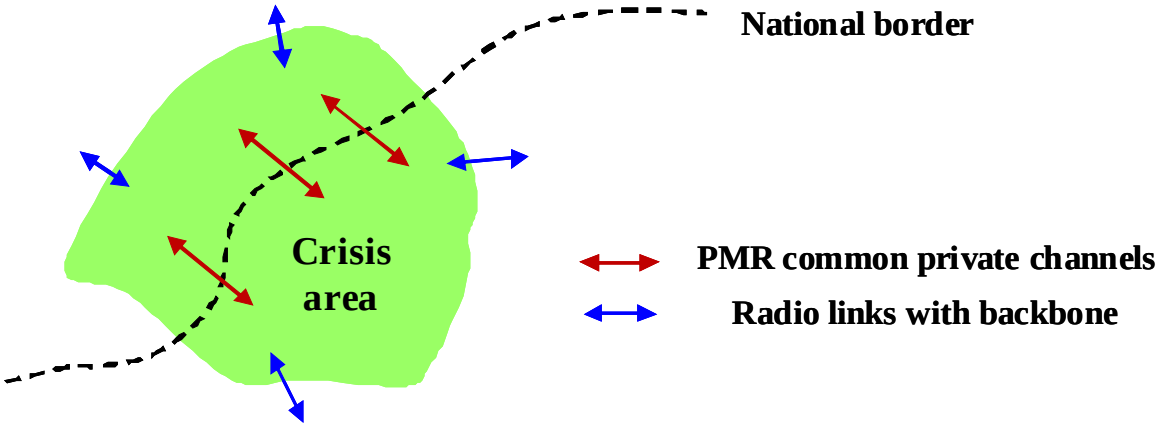



**Figure: 4 Cross border operations**

- In area where the daily communications are still active but security issues require adopting private networks.

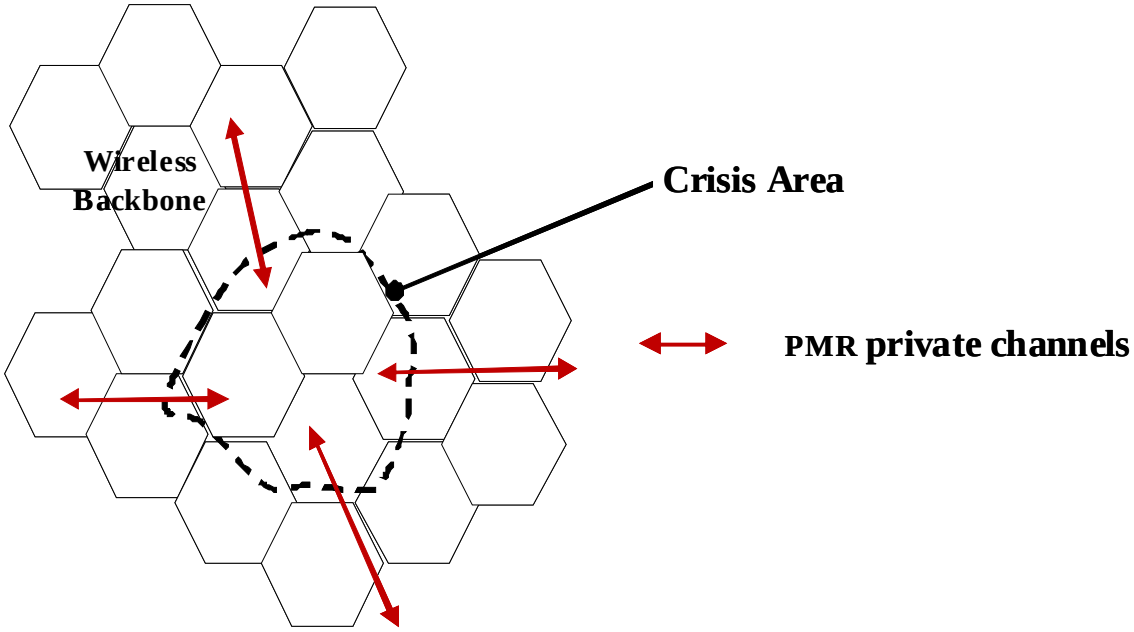



**Figure 5: Overlay PMR operations**

The above depicted scenarios require different radio coverage due to geographic extension and sometime due to orographic factors. Natural disasters and terroristic attacks require different security procedures and sometime the military participation in turn requiring information flow partitioning. But for all the above operational conditions, some procedures can be applied for wireless and wired based communications. In fact we can support:

- First responders include individual officers or institution authorized by public service (e.g. fire, police or health, civil protection).
- Local command centres deployed in crisis area connect first responders only between them and with the remote HQ, national and/or regional.
- Only higher level PS centres communicate with citizens. These centres can operate at national and/or regional level.

Regardless of the operational conditions, PS requires private networks for several reasons including:

- Public network does not offer a sufficient connection for the involved users. Trusted voice and data transferring and traffic constraints avoiding make not suitable commercial networks adoption (i.e. high levels of network availability and low latency).
- Public network does not offer a sufficient security level. Information protection is required both on the crisis area and on the interaction with external users.
- Public network could be not still active on the crisis area.
- Interoperability specific needs: Public Safety organizations use various communications systems based on different standards (mainly TETRA + TETRAPOL in Europe and APCO P25 in USA/Canada).

Then, there is not provision in current commercial networks for pre-emption capabilities or preferential measures which could always guarantee services for PS. In addition, specific requirements like Direct Mode (terminal-to-terminal capability) are not provided and foreseen by commercial networks.

The above reasons including the reliance on commercial operators and the roll-out of PS networks aligning with different users (e.g. police, fire dept, ambulance area boundaries) have made the PS users reluctant to make more widespread use of existing commercial networks and have favoured the development of their own dedicated networks [i.2] and [i.6].

The aforementioned operational scenarios always require the Interoperability among users involved and the consequent requirements. Here the term "Interoperability" is considered only from radio communications infrastructure point of view and the related information flow supported by (see [i.3]). With respect to the above topics (see Figure 5) some effort has been provided to investigate effective solutions including the SDR application in Core Networks able to enable transparent communication among different PS&G agencies using different RATs. WINTSEC (see note 2) program studied Core Network capabilities and role of SDR integration [i.13].

NOTE 2: WINTSEC was an EU funded PASR program. PASR = Preparatory Action on the enhancement of the European industrial potential in the field of Security research.

Among the needs of users involved in crisis management, fast response for link re-establishment is a capability sensitive more than other ones which are not necessary in the first hours.

First responders have to react without the risk of lack of interoperability and the interoperable radio links have to be available according to the same timeline. Then multi channels SDRs provide a natural solution in order to perform transport level gateway as multi RAT base stations. For this purpose the minimum set of SDR capabilities may include major radio communications system standard like TETRA (in EU), P25 (in USA), WiMAX and satellite communications, typically required on PS applications.

SDR, with its reconfiguration capabilities supported with a state-of-art SW architecture, 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 signalling conversion, codec and encryption issues, PTT (Push-To-Talk) mode vs. duplexing mode, etc.
- 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 channelling plans (see tuning range following).
- Information assurance.

Security enforcement is constrained by the information sensitive level, the related clearance any involved user has and the specific emergency operation. Natural disasters are typically managed by not military forces like Civil Protection and Fire Department but the support of military forces are often required for their logistic and technology capabilities. Transportation recovery like bridge temporary re-building is the typical skill 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 performs Transmission Security (TRANSEC) other than Communication Security (COMSEC, e.g. crypto).

Then 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 provide by SDRs and the correspondent subsystems hosting AAA and Data confidentiality and other services for the specific RAT (e.g. TETRA). In order to meet fast response capability the above subsystems and the housed services could be integrated on SDR BSs included in RAN. This solution is depicted in Figure 6, where the reference is to the EULER FP7 program demonstration features. Then the RAN is a fast deployable network and it provides the radio communication infrastructure and a set of centralized services for the different RATs and different users.

As a consequence of multi-users/multi-RATs connections provided by the RAN, the information flow consists of messages exchanged among users with different security clearance not only defined at military level but also among Public Safety users (e.g. Civil Protection and Fire Department). That means the RAN has to support multi security levels even if we do not consider interaction with Public networks. In addition, the heterogeneous environment requires specific policies for key management including key-fill interfaces as with respect the well standardized military environment there is not communality in civil systems, whether they are used for Public Safety or Governmental Security context.

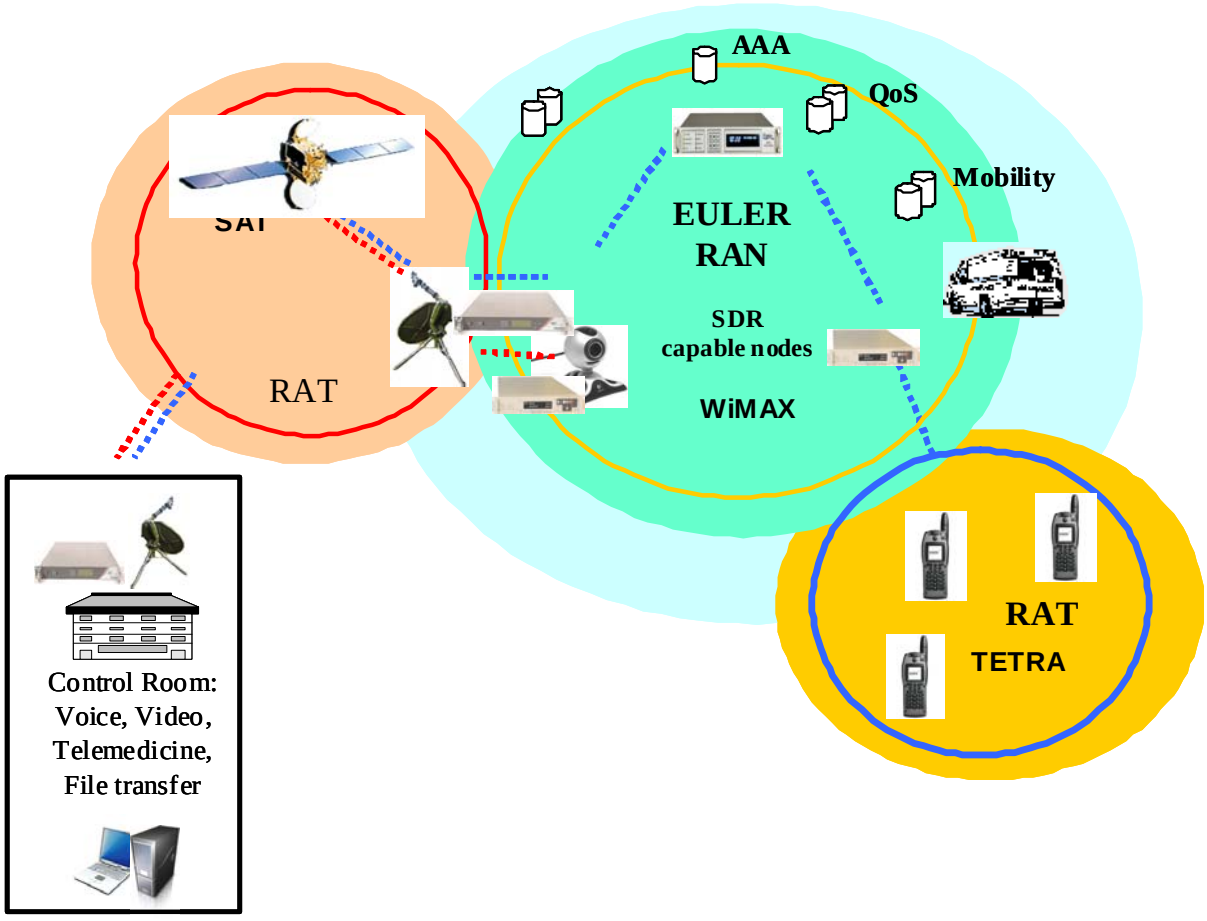



**Figure 6: Centralized services in RAN' components**

The above described needs in turn provide other reasons to adopt Reconfigurable architectures and the level to apply reconfiguration (concerning functional requirements) and business involvement (useful characteristics offered by RRS adoption and not by conventional products):

- Policies adoption can require the interoperability with different procedures and different communication technologies due to national based different standards adoption. This can occur in cross-border operations or international aid operations.

- Spectrum sharing procedures adoption that allow PPDR networks to enjoy strict pre-emption (of the portion of the spectrum let to commercial and other entities) without fear of interference from these sharers.

- Definition of the main interfaces between PPDR networks and other networks to support interoperability at MS and BS levels and joint resource management.
- Interaction between PPDR networks and local ones eventually still active in urban and sub-urban areas. Local networks are different among geographical areas.
- Different policies and RAN technologies can be set and evolve independently, and then an effective updating for adaptation strategy may be applied.

Just for the sake of summary we can list the following reconfiguration related issues:

- Interoperability with national backbones, both public like 3/4G and professional reserved like satellite networks.
- Security policies adoption according to pre-set configurations or on-field dynamically managed.
- Spectrum policies adoption according to pre-set frequencies plans or on-field dynamically managed with Cognitive Radio technologies.
- Interoperability among different RATs adopted by different PS involved users.
- Group-calls management through heterogeneous networks, where the term "heterogeneous" is due to different RAT/N and different users with common policies to adopt.
- PS dedicated networks may provide a set of centralized services, with remote services eventually connected, to the RATs and users involved on PPDR operations.
- Best effective adaptation to policies and technologies evolution.

The issues described in the previous clauses, once allocated respectively in the application/service domain and in the radio communication infrastructure domain represented in Figure 6, they allow to depict a technological environment already mature to offer solutions in order to implement the reconfiguration capabilities.

Just to follow the information flow depicted in Figure 6, we start the analysis from the application and service level. The information content is a subject directly involved on the interoperability issue in the User Domain. Here we consider the above issue has seen only from radio communications infrastructure point of view and the related information flow supported by the Application/Service Domain, distributed among HQs, local command centers and responders, includes applications like emailing, short data/short message sending, data base access for image storage and retrieval. That enables incident reporting to be handled directly via computing mobile devices eventually integrated into the radio terminal, in addition reducing the responder need to return to HQ/command centre to access office applications. Figure 7 provides a description of the on-field applications.

Currently, the responders and mobile command centers need to connect portable PC running the above applications to radio terminal for network access. Then, already now, logical interfaces and protocols have to be applied at waveform and radio services level so as to adapt to new applications, typically designed as web applications.

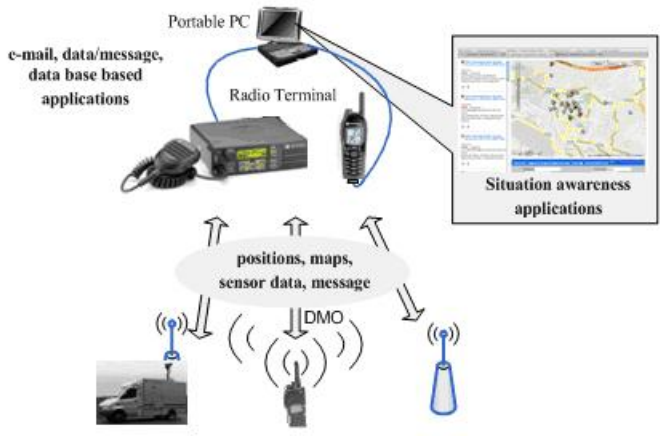



**Figure 7: On-Field Applications**

Now we can already think and design Smart Radio Terminal(s) (SRT; see note 3) able to integrate computer applications into it. The application can consist of client side with presentation (HMI) executed on the terminal and server side with data gathering executed on the network referred base station (network node). Some Base Stations could temporarily (see note 4) collect sensor data, like images and maps retrieved by remote data bases or sensors, so as to perform most intensive computation and send pre-processed data to the terminals for user management (Figure 8).

NOTE 3: Here with terminal we mean both vehicular and handheld.

NOTE 4: Some information could be sensitive and not suitable to be stored in unmanned base stations.

Emergency related messages based on diffused standards like Common Alerting Protocol (CAP) can be exchanged and locally managed by users directly by means of their SRTs. The standard concerning data exchange is an important issue constraining the applications. In fact, data needed in emergency application, and also in daily operations, may be used by multiple applications. These ones can share data with one another and present data in format which is usable by other applications.

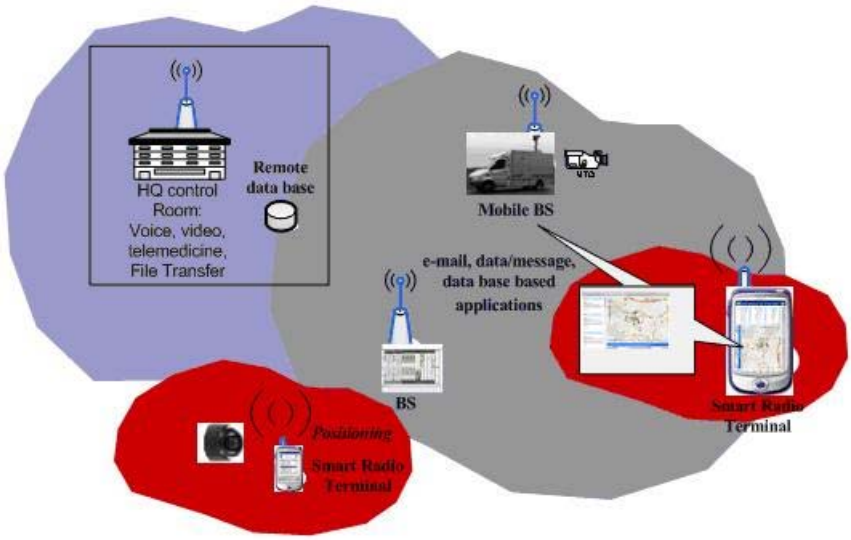



**Figure 8: Applications integration in Smart Radio Terminal**

The above depicted applications distribution just includes many issues concerning the operational scenario and the reconfiguration capability. At PS user level (responder) the terminal allows to activate group-calls (multicast services) with the capability to share information output by situation awareness applications locally executed and actually provide a common operating picture (data and position at least). The reconfiguration capability of the terminal concerns the applications and also the applicable policies. These ones include procedures to follow for data sharing (whom and how), common formats, spectrum policies adoption according to pre-set plans or dynamic management. Every involved terminals have to adopt policies tailored for the specific operation among those ones defined previously in this clause and sometimes agreed among users of different nations. All that could require the policies up-dating and the support to the dynamic creation of multi-services teams connected across multiple networks ([i.12], clause 5.3.1.2). Then the reconfigurable terminals are able to load common standard based policies and update their applications suite in order to meet the PS users need evolution. With respect this terminal reconfiguration capability application, the terms, conditions and involved stakeholders are among the issues referred by the business model analysis carried out in the next clause.

Hence the applications distribution and integration model described above can be implemented by well-designed reconfigurable devices adopting suitable SW and HW solutions. Logical interfaces (Figure 9) adopted by the devices have to allow the installation of new applications and interoperable data management. These interfaces have to be standardised in order to make technology independent new application installation.

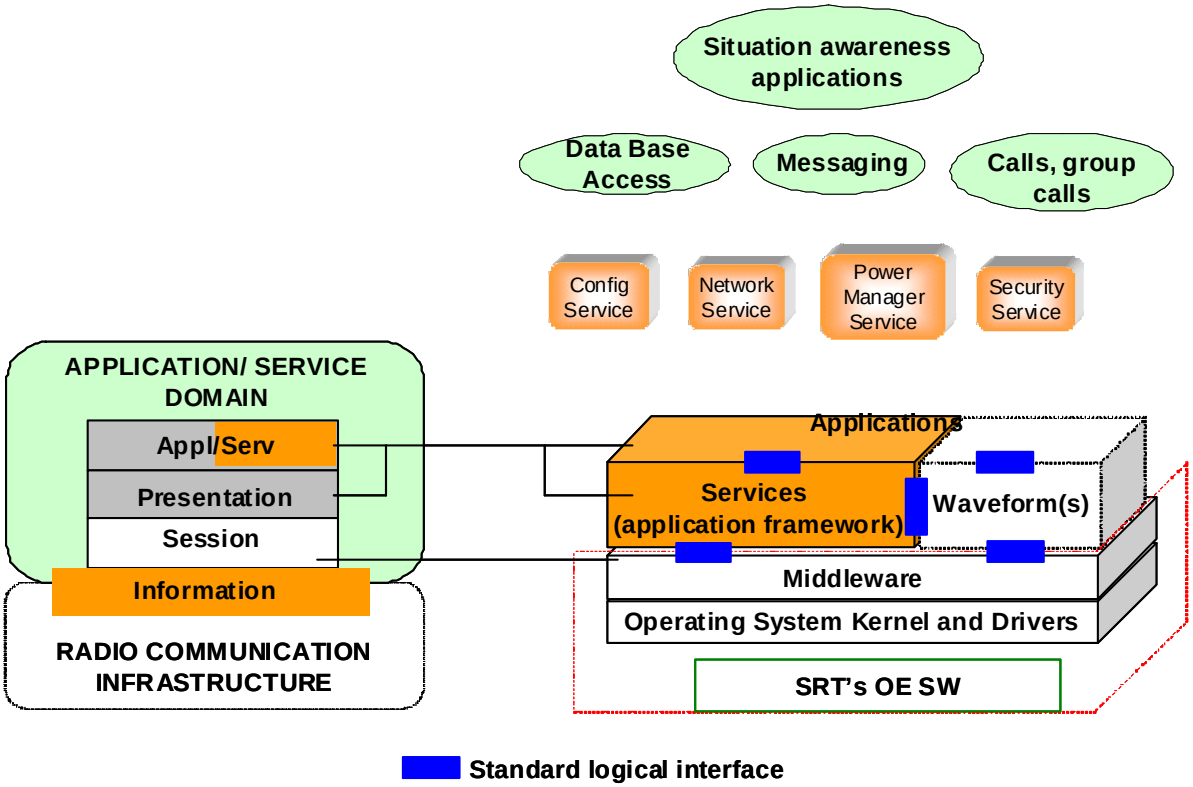



**Figure 9: SW Environment for applications distribution and integration model**

Concerning the Platform Independent Model (PIM) of the SW architecture, some general concepts could be applied in order to propose an acceptable standard for SRT. As already applied on commercial high performances smart phones, the application layer relies its execution on platform services or application framework. The waveform layer provides the radio communication capability to the SRT.

The applications and the services share the logical interfaces in between and with the waveform layer and the SRT's OE (see note 5) SW. This latter component and the mechanism the logical interfaces are based on for their information exchange are the main subjects of the Platform Specific Model (PSM; see note 6).

NOTE 5: OE = Operating Environment (it generally includes the middleware, the application program interfaces framework, the domain description and the operative system).

NOTE 6: The main references concerning the PIM/PSM concept application are the OMG adopted specification [14] and the new SCA Next Specification [15].

The specific adopted PSM can leverage in different ways the components and their relationship of an applicable business model. The reconfiguration process and the SW portability are deeply constrained by the technologies building-up the PSM which should provide an environment of fully or partially technology independent applications and services for information management. The same concept can be applied to the radio communication infrastructure SW components (waveforms) mainly applied to base stations network components (BS; see note 7), as these are most suitable to adopt multi RAT.

NOTE 7: Here with BS we mean node and higher level network components (e.g. Switching and control node, network management stations).

The contemporary activity of responders using different RATs can be sustained until the inter area responder groups can be effectively connected among them by means of BSs performing Gateway functionality. Generally an emergency operation can be managed without using heterogeneous intra-area RATs, but in specific scenarios, the close activity of different types of responders could require the usage of different RATs. At least for narrowband radio link this interoperability issue could be resolved deploying multi RAT terminals, both handheld and vehicular versions.

Legacy solutions until now, adopted forced often public safety users to carry multiple radios during emergency and responders' vehicles commonly have multiple radios installed in them as a makeshift interoperability solution.

The user interface is a critical element for public safety users because they depend on easily accessible radio communications during emergency situations to help save lives and protect property. Public safety users demand radio user interfaces that are simple to use, easy to navigate, and easy to learn. It is not uncommon for each different radio to have a unique user interface.

The applications described above (Figures 8 and 9) transfer their information relying on the communication infrastructure in turn designed and deployed according to standard RATs. Every specific standard RAT, like TETRA, defines all the functionalities supporting the radio communication link, that is the air interface (physical level) and the link level (access and link control) including the mobility management (e.g. vertical handover). In addition, according to the minimum set of PMR user needs, some standards like TETRA offer intrinsic mechanism in order to perform basic services, like group-calls and short message sending contemporary to voice connections [i.15]. TETRA standard includes also the capability to connect to public and private telephone networks and Internet at mobile terminal level. All that provides the framework upon which is built the application layer (see Figure 10).

Current standard RATs providing narrow band and wideband services (ex. TETRA and TETRA TEDS respectively), could be paired and in the future replaced by broadband RATs like WiMAX and/or LTE. However, conformance to PS user requirements has to be maintained.

Node level and higher PS network components support services in different ways. BSs performing RAT support to group connections involve sometime multiple geographic units then supporting group services across multiple networks. BSs perform all the functions of the radio communications infrastructure, allowing physical and logical connections between remote user groups including the authorization verification and sensitive data protection. Addition of new applications and policies for fast reaction in different operations can require reconfiguration capability that for the BS means to involve multi RATs eventually installed in it.

The service availability and the minimum level of QoS are two overall requirements mainly resolved at BS level. The additional bulk of traffic in the network rises during the first hours of the crisis, when different users require to set the coordination network suitable for the specific scenario (see Figures 1 to 4). Then, the network management function has to allow the available and suitable resources selection also following priority schemes. Sometimes the network has to activate priority mechanisms to ensure that specified users in a wide area group call spanning multiple base station sites are connected together when some links are busy.

As far as security mechanisms concerning, cryptographic algorithms for data protection are applied at terminal level performing end-to-end encryption. Apart from source data encryption, performed at application and service level, BSs perform encrypting connections between them and terminals (subscriber stations). The BS protects unauthorized access to data transport services by enforcing encryption of the associated link level transport services across the network (ex. service flows for WiMAX). In addition, in order to protect from "denial-of-services" attacks, the encryption is generally applied so as to protect the network signalling. The security procedure at transport level sets an additional issue concerning interoperability that rises at higher level of complexity in heterogeneous or multi-RAT networks (see Figure 10). This condition may go on again for many years because legacy technologies cannot be replaced in a short timeframe.

New RAT insertion in deployed PS networks would have to be carried out without constraining or limiting the applications available to the users making the PS application environment more and more "infrastructure independent".

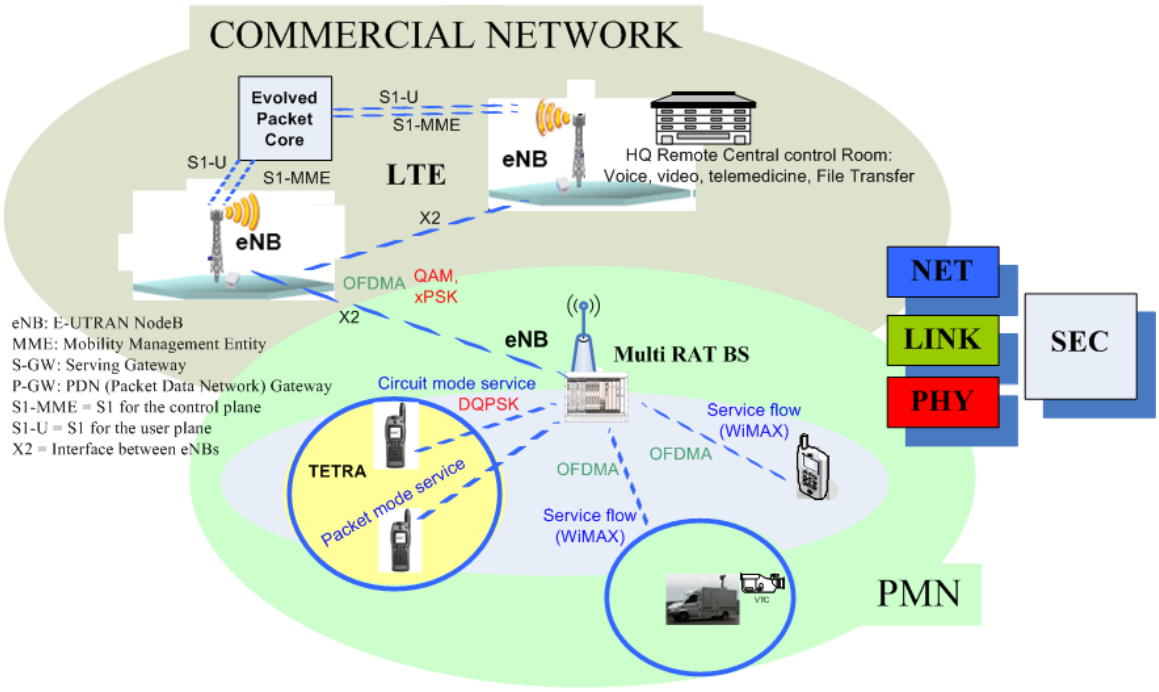



**Figure 10: Heterogeneous or multi-RAT networks**

Currently in Europe the PMR network interoperability is not only related to TETRA-TETRAPOL but also involves TETRA-TETRA and TETRAPOL-TETRAPOL connections. A specific topic concerns nationwide network interoperability for effective cross-border cooperation. This subject has been faced from 1990 when the standardization of TETRA Air Interface and Inter-System Interface (TETRA ISI) began. TETRA ISI represents a set of basic services necessary to support cross-border communications between independently owned and operated TETRA networks. It may provide a limited subset of TETRA services need for the above purpose. The ETSI TETRA ISI standards began focusing on a small window of functionality and the following features and functions were seen as the most important aspects of any ISI solution:

- Allow terminals to use a foreign 'independent' network when required.
- Allow users in one network to communicate with users in another 'independent' network (individual call, group call).
- ISI Gateway to control the system's access policy regarding foreign users.
- Basic services such as Group Call, Individual Call and Telephony services including status and short data service.
- Mobility management.

The above functions may be provided taking into account that even when two networks from different suppliers are connected together, which both comply with the physical and link levels of ETSI standard and have demonstrated full interoperability with many suppliers' terminals, they are very different from one another through their chosen system implementation. For example one national network could adopt Single Slot Packet Data, Scanning and perhaps ISDN Dialling, whilst the other one will be optimized to support Multi-Slot Packet Data and eventually adopt different national level end-to-end encryptions.

A migrating terminal may have only access to a subset of basic services over the TETRA ISI and the Networks connected together via a TETRA ISI may operate as independent networks. This allows a mobile terminal to access to home network services and, following the roaming phase, the services available in the host network (TETRA migration).

The TETRA ISI standard content is partially defined (see note 8) [i.16] and [i.17] and it is still not in operation today. Some companies have faced the first step of ISI certification but the list of functionalities currently tested was limited and it did not include a minimum set of necessary user services. The experience suggests suppliers to agree on common set of services they can offer collectively as part of a TETRA ISI.

NOTE 8: Progress has been made over recent years to complete the ETSI standards, TETRA Interoperability Profiles (TIP) and Test Plans for the features that comprise Phase 1 & 2 as defined in the 'ISI Adoption' paper. More recently, the Group Call specification and test plan has now been completed. Functionality described as Phases 3 & 4 remains incomplete, with some elements not yet agreed within ETSI. The first proof-of-concept testing was completed successfully in March 2009 and witnessed by the independent test house. The functionality tested was individual call and short-data.

In recent times, the majority of TETRA network suppliers are moving from Time-Division Multiplexing (TDM) to IP-based architectures. This suggests that a new ISI standard has to be defined based on IP protocols. The new ISI may address not only TETRA-TETRA interoperability but also TETRA-TETRAPOL interoperability, even if no TETRA-TETRAPOL ISI draft standard is available.

Then TETRA-ISI is a chance to adopt reconfigurable solutions able to make compatible and interoperable a suitable minimum set of basic services that can be aligned and standardized across national systems. Furthermore, the reconfiguration capability may offer an effective way to allow additional services and additional suppliers to be integrated in the business model and relevant value chain. TETRA-ISI interface may be implemented at Switching and Control node level, that is a specific border BS that perform its functions coordinating cell level multiple BS and network management (see Figure 11).

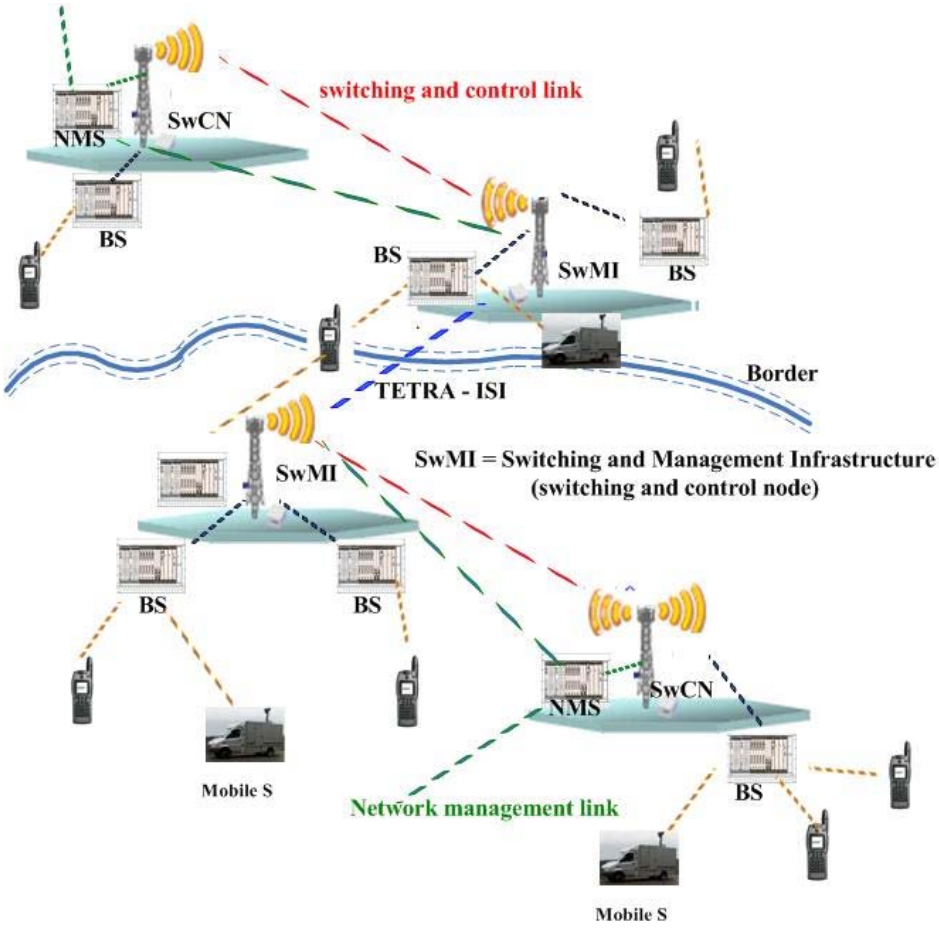



**Figure 11: Cross border TETRA interface**

# 7 Business and cost considerations for SDR in Public Safety

## 7.1 Introduction

SDR base stations and terminals have to satisfy the requirements described in clause 5 and the technical specifications of the telecommunications standards already defined in the Public Domain. As a consequence, the design and cost considerations for SDR technologies can be different from the commercial and defence domain.

The purpose of this clause is to present the most common architectures and components of SDR technologies and identify the main elements, which can drive the cost and obstacle the deployment of these technologies.

## 7.2 SDR architectures and main components

The purpose of this clause is to present the possible SDR architectures and the related components. There is not a single potential architecture for SDR.

Figure 12 is a classical schema of a SDR based on a Software Framework and modules (e.g. SCA). In this architecture, the main hardware components are the antenna, RF front-end, ADC/DAC and the DSP and FPGA components where the software waveform (e.g. the implementation of specific communication standards) executes. The RF front end includes amplifiers and filters.

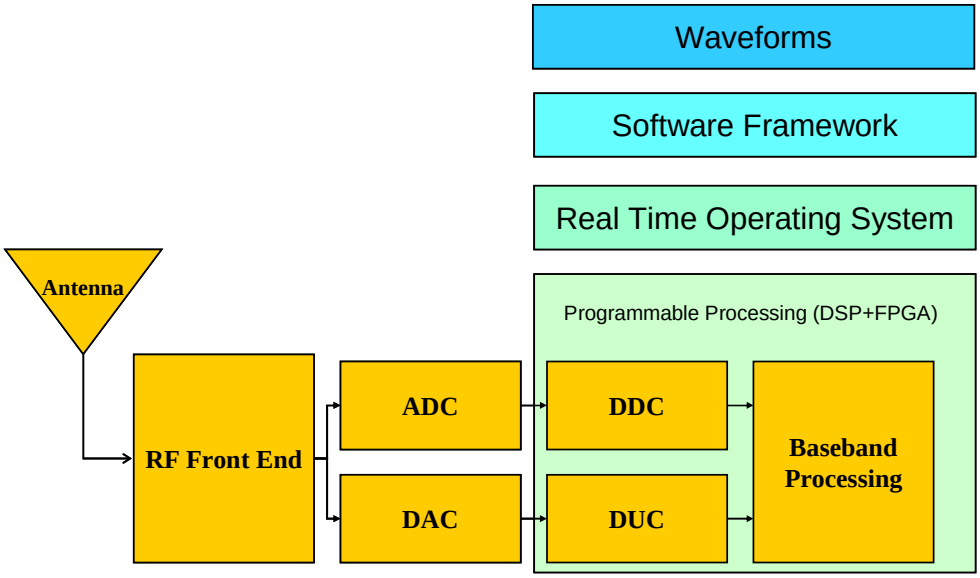



**Figure 12: A potential SDR architecture**

Figure 13 describes the architecture proposed in "Reconfigurable Radio Systems (RRS); SDR Reference Architecture for Mobile Device" [i.4], where the main functional blocks are present. This architecture is more suitable for handheld terminals than base stations.

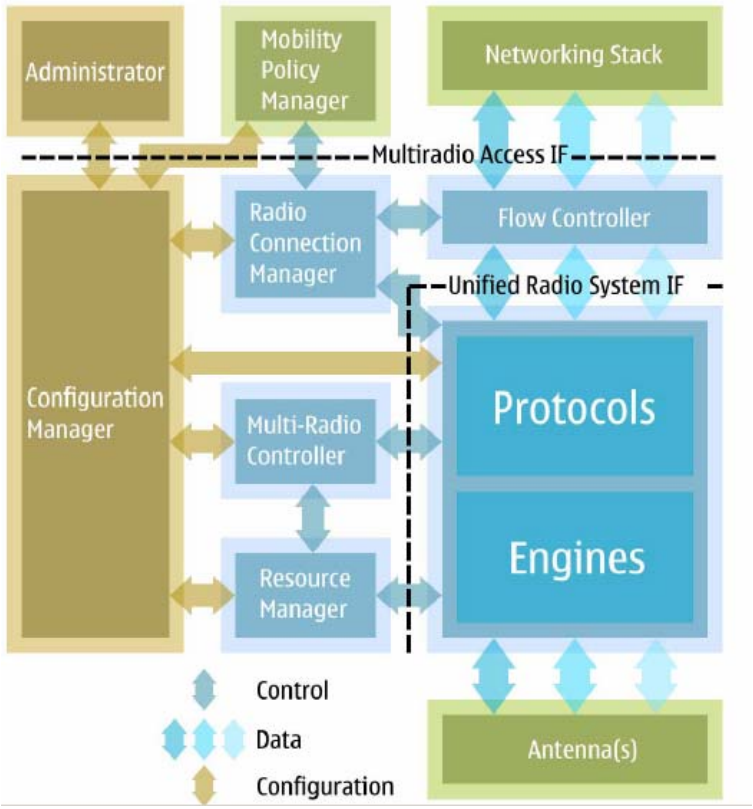



**Figure 13: A potential SDR architecture**

One of the driving forces for the deployment of SDR technology is the Moore's law, which claims that the number of integrated transistors can double every two years, increasing considerably the capability of digital processors and the capacity of memory. Digital processors include ADC/DAC, FPGA, GPU, DDC, DUC and the memories presented in the terminal.

However, the analogue RF technology like low noise amplifiers, power amplifiers and filters, develops at a different pace. Although digital components support analogue functions, high performance radio equipment station is heavily dependent on analogue components.

## 7.3 Cost implications and trade-offs for SDR components

- **Antennas:** a SDR may support a wide range of air-interfaces in (theoretically) a wide range of frequencies. Historically, public safety networks have operated in the VHF or UHF frequency range (e.g. 380 MHz to 400 MHz) and most of the existing dedicated networks operate in these spectrum bands. If public safety operates in a wide range of frequencies as proposed by various spectrum regulators, the antennas could be tuneable to a wide range of frequencies. It is unlikely anyway that the future range of frequencies may be beyond 5 GHz. In this case, antennas have to be impendence or frequency invariant, which can increase the price of the base station or terminal. A trade-off is the availability of invariant wideband antenna against the cost of the antenna and the capability to provide a constant frequency and impedance response. Innovative type of antenna like fractal antenna and software-controlled micro-electromechanical devices may facilitate the requisite gains in efficiency.

- **Amplifiers:** to achieve all the benefits of SDR technology, SDR communications systems have to be equipped with high power amplifiers. This is the consequence of the coverage requirement identified in clause 5.2. Specific urban environment such as buildings can introduce at least 30 dB propagation loss. Consequently it is not uncommon to have handheld with 3 Watts transmission power, which is much higher than commercial counterparts. Usually, Public Safety handheld have a transmission power in the order of watts (e.g. 3 Watts to 5 Watts) while commercial handheld have transmission power in the order of hundreds of milliwatts. On the other side, amplifiers have to be very efficient to decrease battery consumption. For SDR technology, amplifiers have to provide limited distortion wide range frequencies.

All these technical requirements are usually conflicting and they generate trade-offs. It is possible that only few parameters can be optimized and only for specific platforms: base stations and vehicular terminals do not have stringent requirements in terms of battery power, weight and cost.

- **ADC/DAC:** represents an important trade-off in the design of public safety radios. As identified in clause 5.2, Public Safety radios requires a high dynamic range, which translates with ADC/DAC into many bits and therefore expensive. ADC/DAC with higher sampling rates and bits imply a higher processing power of the other data acquisition devices (e.g. DSP/FPGA) and increase power consumption. On the other side, higher sample rates do improve the noise spectral density (NSD). In an ideal software radio, ADC/DAC have to be as near as possible to the antenna. On the basis of the needed dynamic range and the requested wide frequency bands, the current ADC/DAC technology is not able to implement an ideal software radio, especially for portable radios. Digitizing at the antenna is not a realistic design decision as there is pre-selection and down-conversion to IF. This means that analog pre-selection components may be present. With this assumption, the sampling rate of a 12-bit ADC is in the order of 5 Gs to 20 Gs depending on the frequency range and bands. The advantage of SDR technology in Public Safety domain is that the spectrum bands are usually in a low frequency range under 500 MHz, which require less processing resources than higher bands of commercial networks (e.g. 2 GHz to 3 GHz). Even if recent developments in ADC/DAC design are providing this order of magnitude in sampling rate, the cost of the components can be still too high for deployment in the Public Safety market; at least for handheld.

- **DSP/FPGA:** It is quite likely that DSP and FPGA may be increasingly used in SDR to support the needed levels of flexibility and reconfigurability. This flexibility and reconfigurability come at a cost, as dedicated ASICS are always cheaper than DSP and FPGA. Therefore, on average, every 18 months we can expect a doubling in processing power for the same volume, power consumption, and cost. This equates to an order of magnitude (or 10X) improvement every six to seven years. It is this exponential improvement that has leveraged the software radio from the university laboratory into the commercial marketplace. DSP and FPGA have specific advantages and disadvantages. FPGAs offer re-programmability and the simple advantage of high levels of parallelism that cannot be achieved by the essentially sequential DSP. Parallelism is an important feature as many algorithms used in wireless communications require parallel processing. FPGA presents the disadvantage of a significant power penalty, especially in the static power consumption. Unfortunately, this problem is not likely to disappear as FPGA devices move toward smaller transistor geometry to achieve higher chip density and faster dynamic speed, the leakage current in each transistor goes up substantially. This is an important issue especially for handheld terminals used by Public Safety officers, which are usually battery powered. It is not so important for vehicular (i.e. on cars or trucks) terminals or base stations.

- **RF Filter and mixer:** True SDR systems include software reconfigurability up to the power amplifier; this means that RF filters and mixers are also reconfigurable, something not available today. Generally Public safety terminals have higher RX spurious specs in comparison to commercial terminals. For example: TETRA terminals have usually a spurious rejection limit in the receiver side in the order of -45 dBm.

- **Software Frameworks:** One of the main technical challenges for the deployment of SDR in the Public Safety domain is the choice of the software/hardware architecture. The current SCA framework and CORBA middleware is considered to be very resource intensive and it does not fit in the business model of the commercial market, where cost effectiveness is a primary requirement. Public Safety domain can be an intermediate solution between the commercial and military domain by choosing a less resource intensive framework and middleware.

  Another possibility is to implement different software frameworks on different platforms: a software framework based on SCA and CORBA middleware in the base stations and a software framework defined for the commercial domain for the handheld.

# 8 Business and cost considerations for CR in Public Safety

## 8.1 Introduction

The SDR technology provides an effective contribution to the interoperability but in order to complete the effort at radio communication infrastructure level, a harmonized spectrum policy has to be adopted. In 2008 ECC/CEPT (see note 1) committee provided a decision on the harmonization of frequency bands for the implementation of digital Public Protection and Disaster Relief (PPDR) radio applications in bands within the 380 MHz to 470 MHz frequency range (ECC/DEC/(08)05) [i.9]. This ECC Decision covers narrow band (see note 2) as well as wide band (see note 3) PPDR radio applications. Spectrum within the duplex bands 380 MHz to 385 MHz/390 MHz to 395 MHz has be designated for narrow band PPDR radio applications. The provisions of this ECC Decision regarding the wide band systems are based on a "tuning range (see note 4)" concept which provides flexibility for the administrations by implementing this Decision (within the tuning range on a national basis). The aim is to make radio spectrum available for wide band PS radio applications either in the 385 MHz to 390 MHz/395 MHz to 399,9 MHz sub bands, in the 410 MHz to 420 MHz/420 MHz to 430 MHz sub bands or in the 450 MHz to 460 MHz/460 MHz to 470 MHz sub bands.

NOTE 1: ECC/CEPT = Electronic Communication Committee within the European Conference of Postal and Telecommunications Administration.

NOTE 2: Channel spacing up to 25 KHz.

NOTE 3: Channel spacing of 25 KHz or more, at least up to 150 KHz.

NOTE 4: Here we refer to harmonized frequency spectrum bands where the specific channels (tuning ranges) are defined on a national basis. The real application of the decision is based on national possibilities and national market demands and the indicated sub bands may not available in all CEPT countries.

In the same period CEPT developed ECC Recommendation 08-04 concerning frequency bands for the implementation of Broad Band Disaster Relief (BBDR) [i.10] which recommends that administrations make available at least 50 MHz of spectrum for digital BBDR radio applications. However, this spectrum is shared with radio LANs and may be available for disaster relief during major incidents.

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.

In the future, allocation of harmonized spectrum bands for public safety may become increasingly difficult, especially in the lower frequency bands (below 500 MHz) where the majority of the existing public safety networks are operating.

Allocation of bands in higher frequencies is not convenient for economical reasons because:

1) the existing dedicated networks (e.g. TETRA in Europe) may be redesigned and upgraded to use the new frequency bands. This is a massive investment for each European member states and it is unlikely to happen;

2) at higher frequencies, a larger number of radio terminals/base stations are needed to provide the same coverage.

As a consequence, there is a need for new approaches and new technologies to overcome the current spectrum deadlock.

Radio communication devices based on SDR and CR technologies may have the multi band and the reconfiguration capabilities needed to adopt the policies for cross border cooperation and interoperability. Here the term "Interoperability" is considered from radio communications infrastructure point of view and the related information flow. Some operational conditions could require connections with commercial networks for limited emergency communications using reserved channels. Current 3G RAN and next 4G (LTE) cellular networks have to be considered in the technology basket as multi RAN/RAT base stations could provide the infrastructure access point eventually still active in crisis situations.

At the same time, Cognitive Radio capabilities can provide dynamic spectrum management for:

- link and traffic optimization;
- network entry of different RATs;
- support for secondary spectrum usage.

Both for SDR and CR related businesses, common stakeholders could be involved, that is electronic components and sub-assemblies manufactures and systems/subsystems suppliers. SW components and application developers can be interested on all the above businesses and, for CR, a specific stake may be by licence owners.

## 8.2 Economical benefits and trade-offs of CR

The economical benefits of CR and Dynamic Spectrum Management has already been discussed and investigated, mostly in the commercial domain.

A report prepared by Qinetiq for OFCOM [i.7] on the commercial use of CR technology, concluded that determination of the economic benefits of the CR and spectrum sharing applications was not possible due to the lack of available economic and usage data. The report provided a case study based on the competitive cellular market. It was assumed that at a future date (i.e. 2025) cellular spectrum would become insufficient and cellular congestion would occur. In this scenario, CR technology would be deployed to achieve needed extra capacity. Simulations performed showed that maximum call volume increases of between 3,1 % and 10 % could be obtained in the GSM and UMTS expansion band using CR. The report assumed an investment in CR technology of 5 % of the expected annual revenue gain in 2025, assuming a high demand. With an assumption that the investment depreciates completely after only 3 years, the analysis shows that investment cost will be repaid with an efficiency gain of 3,7 % of call volume for consumer surplus.

This case study was based on the UK market and the commercial mainstream domain. A similar study was not done for the Public Safety domain, which has significantly different specifications for radio coverage and traffic capacity.

Public Safety cellular networks have the following differences in comparison to commercial cellular networks:

- Public Safety cellular networks (e.g. TETRA) are usually configured to provide guaranteed traffic capacity to all the users present in the area (e.g. jurisdiction). They are basically designed for peak capacity. This is significantly different from commercial networks where the traffic capacity is a fraction of the potential users.
- As described in clause 5.2, Public Safety networks have to provide a high level of coverage and resilience (i.e. 0,99999). These requirements imply that network equipment (e.g. base stations) have to be designed with high redundancy and increased number of radio terminals in comparison to commercial cellular networks.
- As described before, Public Safety networks used a lower frequency range (e.g. 400 MHz to 500 MHz) in comparison to commercial cellular networks (e.g. 800 MHz, 1,8 GHz). As a consequence, the density of base stations can be lower in the Public Safety domain.

Due to the considerations above, Public Safety cellular networks are much more expensive than commercial cellular networks in terms of capacity per user. Obviously, public safety is considered a public benefit for all the citizens and the property of the state and its deployment does not follow the same business logic of the commercial market. Nevertheless, cost considerations are still quite important, because public safety networks are usually funded by the government, which does not have unlimited funding. The consequence is that public safety cellular networks may have limited coverage over the national territory and they may not fully satisfy the requirements above of coverage and traffic capacity over the entire extension of a nation because of limited funding. Natural disasters like flooding and earthquake are not uncommon in rural areas where dedicated public safety infrastructures may not be present.

CR can provide the capability of dynamically changing the transmission parameters.

In recent times, sharing with commercial networks has been advocated (see [i.11]) as a solution to improve the support to public safety officers and to improve the efficiency of the networks.

In terms of spectrum regulation for public safety communications, the FCC has established a single nationwide Public Safety Broadband License (PSBL) for the 700 MHz public safety broadband. The licensing of this band was assigned to the Public Safety Spectrum Trust Corporation (PSSTC) that is expected to form a Public Safety/Private Partnership with the commercial licensee(s) of a band contiguous to the public safety band to develop a shared network for both commercial and public safety users. Under the Partnership, the PSBL may have priority access to the commercial spectrum band in times of emergency, and the commercial licensee may have pre-emptable, secondary access to the public safety broadband spectrum.

In addition, as discussed, supra, utilizing the communications networks of other network operators is another way to increase network capacity and provide a capability backstop to public safety. There may be times that 10 MHz, 20 MHz or even 30 MHz of capacity, even with sound network design and management principles might be insufficient to support demands during a major incident. In these cases, it is critical that public safety have access to additional broadband wireless networks, such as those operated by commercial network operators. Guaranteeing access to these networks may enable the public safety community to have access to substantially more capacity than a dedicated network can provide without vastly more dedicated spectrum than is under consideration.

In conclusion, we can identify the following economical benefits for CR in the public safety domain:

1) CR is an enabler for spectrum sharing, which may lower the costs because it may facilitate opportunities to share the costs of network infrastructure, in addition to spectrum assets. Such cost sharing may occur over space and time.

2) Greater level of reconfigurability to address unpredicted events. Transmission parameters (e.g. power, modulation, coverage) can be dynamically adapted to the deployment in the field of public safety responders.

3) Greater level of flexibility to support harmonization across European member states. With CR technology, we may mitigate the challenge for harmonized bands across European member states, because CR devices could adapt their transmission bands for the member state where they are present. Obviously, this does not solve the problem if the bands are used by communications systems based on different standards (e.g. TETRA/TETRAPOL). In this case, support to different waveforms with SDR technology is also needed.

# 9 Lifecycle and Deployment aspects

## 9.1 Equipment lifecycle

As described in the previous clauses, the deployment of dedicated Public Safety networks is usually very demanding for Public Safety organizations from an economic point of view. A national or regional network is usually an investment for 10 years to 15 years or more. Conventional communication equipment is not easily upgradeable as hardware components are the ones to be replaced. A communication network based on RRS technology can be upgraded to support new versions of the communication standard or an entirely new wireless communication technology if such changes do not require a modification or replacement of the RF front-ends (e.g. different transmission frequency bands). The upgradeability provided by RRS technology can significantly increase the lifetime of Public Safety networks and enable a faster evolution of the communication equipment.

The benefits of upgradeability can have a different impact on the different classes of communication equipment: fixed infrastructure (e.g. switches and base stations) and user equipment (e.g. terminals). Equipment upgrade can be achieved more efficiently on the fixed infrastructure rather than the user equipment due to the cost and design constraints of the latter. Even with this limitation, RRS technology can provide a significant benefit considering that the greater cost of the PS communication equipment is the fixed infrastructure, because the number of potential users (e.g. PS officers) is relatively small in comparison to commercial networks (e.g. civilian population).

## 9.2 Deployment considerations

The deployment of a new technology in the PS domain has often a high cost, not only from the technical point of view, but also from the organizational/procedural point of view, because PS officers have to learn to use the new technology and its capabilities. It is easy to forecast that the introduction of RRS technologies can have a significant impact on PS organizations and procedures as it may provide new capabilities like spectrum sharing, a new range of applications and it may remove interoperability barriers.

We can identify the following impacts:

- the adoption of cognitive radio and spectrum sharing may require new procedures in case of emergency crisis where new spectrum or network resources could be acquired to address the increasing needs of traffic capacity and bandwidth;
- the capability to interoperate with a wide range of wireless services may enact new procedures for interaction among PS organizations. Cross-border operations will be especially affected;
- RRS technologies may enable a new range of applications, which require organizational changes and new procedures.

## 9.3 Certification considerations

Certification of the equipment and software is an essential process in the Public safety domain. This is particularly important for the introduction of new technologies like SDR, which have be validated against specific operational and technical requirements. It is possible that the certification procedures for SDR technology will be more complex than conventional radio wireless equipment. This is a consequence of the SDR reconfigurability and the possibility of different combinations of HW platforms and SW waveforms. Furthermore, the certification of the CR capabilities should be executed too. In Europe the certification process could be even more complex than other countries (e.g. USA) because of the political fragmentation, which may require a network of certification centres and unified procedures across Europe. Obviously certification is based on the existence of standards and specifications against which validate the SDR equipment. These standards are not well defined yet in the Public Safety domain.

# 10 Business models for RRS technologies in Public Safety domain

## 10.1 Vertical business model

This is the traditional business model adopted in conventional public safety communications systems, where a manufacturer designs and deploys networks and terminals on the basis of specific standards (e.g. TETRA). The capability of producing interoperable networks and terminals by different vendors is proportional to the availability and maturity of the standards. In conventional public safety communication technology, the equipment is not easily upgradeable: base stations cannot be upgraded to transmit a new wireless service without expensive hardware changes. Application and services are usually developed on proprietary Application Programming Interfaces (API). This model creates constraints to third party application developers, which do not have access to the API.

## 10.2 Open business model

Software Defined Radio in the Public Safety domain could enable an open or horizontal business model where vendors can have different roles: SDR platform vendors, SDR waveform vendor, SDR integrator, Network providers and application developers.

Figure 14 describes the various roles and the relationships.

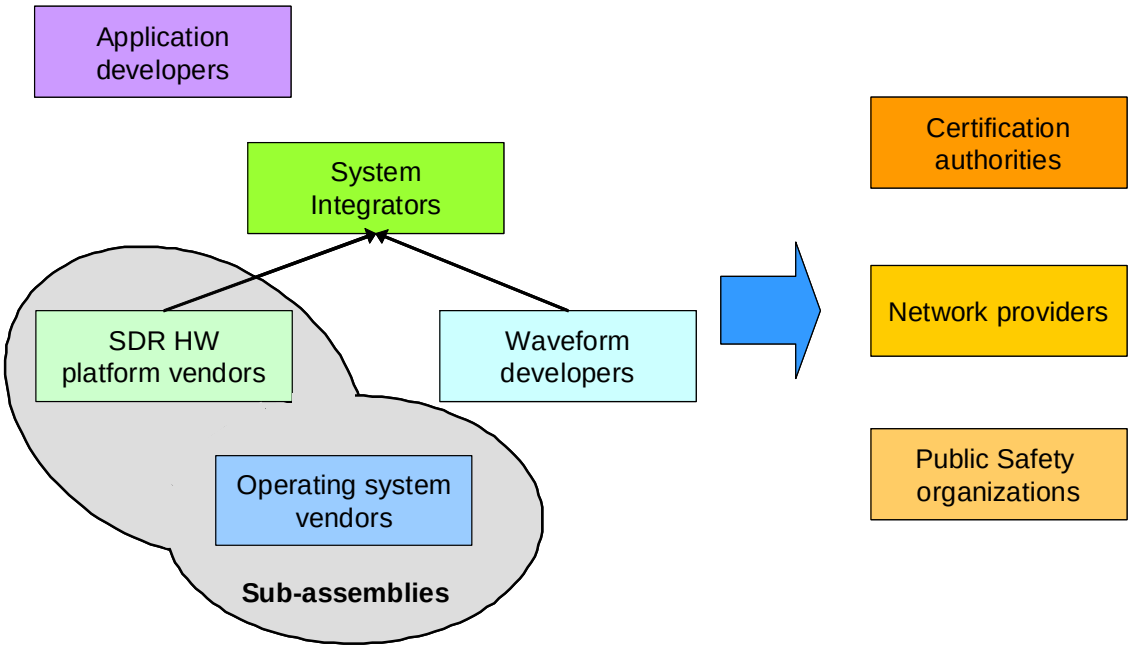



**Figure 14: Open business model**

The operating system vendors are quite similar to their counterparts in the conventional telecommunication market. Core Framework providers develop and maintain the framework libraries (e.g. SCA) and middleware (e.g. CORBA) which provided support to Waveform developers through well defined API. SDR HW platform vendors are responsible for the development of the generic SDR hardware platform.

System Integrators are responsible for the integration and validation of the combination of waveforms/SDR HW platforms. Certification authorities are responsible for the certification of the combinations of waveform/SDR HW platforms. This can be a challenging task as there may be many combinations to certify.

Public Safety organizations provide a direct input to certification authorities to ensure that the certification requirements are mapped to operational requirements. Certified products are then used in the networks managed by network providers for the benefit of Public Safety organizations.

Application developers are responsible for developing new applications, which take advantage of the SDR capabilities on the basis of the needs of Public Safety organizations. In this open model, third party developers could create applications in a similar way to the commercial domain (e.g. appStores) with the significant difference that such applications should be certified by the certification authority before being deployed into the market.

The open business model has to guarantee the protection of the user data and equipment. Any software module (i.e. waveform or application) is certified against a specific combination of SDR platform/waveform and it is marked with a specific signature. Only certified and signed software modules are allowed for activation on the SDR platform.

An open business model can provide significant benefits to the Public Safety organizations by enabling an enterprise environment with developers of new applications and waveforms and by decreasing the cost of the equipment and improving the upgradeability of the network equipment.

# 11 Conclusions

The present document has described the most relevant aspects for the deployment of RRS technologies in the Public Safety domain from a business/market point of view. Benefits and challenges have been identified. Reconfigurability of the communication equipment can have a significant impact on the equipment lifecycle and mitigation of the interoperability barriers.

A consideration is worth to be done at this point. A lot of publications, which were referenced in the present document, consider the public safety sector a niche market with respect to the commercial market. Anyway, if we think about all the emergency crisis occurring in the last ten or more years (including terrorist attacks), then we have to note the vast number of first responders involved all over the world and the major economical impact of these events.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | April 2011 | Publication |
| | | |
| | | |
| | | |
| | | |