# ETSI TR 102 733 V1.1.1 (2010-03)

*Technical Report*

# Reconfigurable Radio Systems (RRS); System Aspects for Public Safety

Reference

DTR/RRS-04005

Keywords

radio, system

*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

## *Important notice*

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

## *Copyright Notification*

# 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 feasibility study of the Systems Aspects for the application of reconfigurable radio systems to the Public Safety domain.

While the Public Safety domain has specific sets of requirements and challenges in comparison to the consumer domain, reconfigurable radio systems can provide improved operational capabilities to public safety organizations.

The purpose of the present document is to provide an overview of the main system design areas to investigate, to present potential design solutions and related trade-offs.

As a feasibility study the present document provides basis for decision making at ETSI Board level on standardization of some or all topics of the systems aspects in Public Safety domain.

# 1 Scope

The present document gives guidelines for the application of reconfigurable radio technologies in the Public Safety domain and how they can solve or mitigate some of the challenges faced by Public safety communications today:

- Public safety organizations use many separate and often incompatible systems with quite different capabilities.
- New Public Safety applications or the evolution of existing ones require an increase need for broadband connectivity.
- Public Safety organizations usually operate in uncertain and changing operational scenarios.

In this context, the present document establishes the general principles for the application of dynamic spectrum management and cognitive radio in public safety domain. Security aspects will also addressed in the present document.

The document will also present relevant past and current activity in this context from other projects and standardizations bodies.

# 2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
    - for informative references.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

## 2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] SDR Forum - Software Defined Radio technology for Public Safety, Working Document SDRF-06-W-0001-1.0.

[i.2] "Framework for sharing common waveforms", NATO C3 Board software Defined Radio Users group (SDRUG), working paper AC/322-WP92008.

[i.3] "Business Models for Wireless Interoperability using Software Defined Radio", NATO industrial advisory group. DRAFT.

[i.4] Software defined radio to enable NNEC: technical challenges and opportunities for NATO by Michael Street and Darek Maksimiuk, NATO C3 Agency.

[i.5] An Evolution of SDR, Ofcom Study. QinetiQ/D&TS/COM/PUB0603670/ Editor Taj Sturman.

[i.6] European Secure Software Radio Programme (ESSOR) Jerzy Lopatka, NATO RTO conference on Tactical communications, Prague, April 2008. IST-083. Page 4-4.

[i.7] On Workload in an SCA-Based System, with Varying Component and Data Packet Sizes Ulversøy, T.; Olavsson Neset, J, NATO RTO conference on Tactical communications, Prague, April 2008. IST-083.

[i.8] Spectrum Management for the 21st century. The president's spectrum policy initiative second annual progress report. U.S. DEPARTMENT OF COMMERCE. October 2007.

[i.9] J. Zhao, H. Zheng, G.H. Yang, Distributed coordination in dynamic spectrum allocation networks, in: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 259-268, November 8-11, 2005.

[i.10] Lili Cao and Haitao Zheng, "Distributed spectrum allocation via local bargaining", in Proc. of Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, (Secon), Sept. 2005, pp. 475-486.

[i.11] H. Zheng, L. Cao, "Device-centric spectrum management", in Proc. of IEEE DySPAN 2005, Nov. 2005, pp. 56-65.

[i.12] J. So and N. H. Vaidya, "Multi-channel MAC for ad hoc networks: Handling multi-channel hidden terminals using a single transceiver", in Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing, (Mobihoc), May 2004, pp. 222-233.

[i.13] ETSI TR 102 653: "Project MESA; Technical Specification Group - System; System and Network Architecture".

[i.14] European Radio Office (ERO).

NOTE: Available at www.ero.dk. Last accessed 26/06/2009.

[i.15] ECC REPORT 102: "Public protection and disaster relief spectrum requirements", Helsinki, January 2007.

[i.16] Press Release: "European Commission paves the way for European mobile satellite services".

NOTE: Available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/770&format=HTML&aged=0&language=EN&guiLanguage=en. Last Accessed 31/07/2009.

[i.17] APCO 25.

NOTE: Available at http://www.project25.org/. Last accessed 26/05/2009.

[i.18] US Department of Homeland Security. Multi-band Radio Project.

NOTE: Available at http://www.safecomprogram.gov/SAFECOM/currentprojects/mbr. Last accessed 31/07/2009.

[i.19] The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress. CRS Report for Congress. November 17, 2005.

[i.20] "TETRA versus GSM for Public Safety".

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

[i.21] ETSI TR 122 950: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Priority service feasibility study (3GPP TR 22.950)".

[i.22] "TETRA serving Public Safety in Europe".

NOTE: Available in the reports section at www.tetramou.com.

[i.23] "Best practices regarding the use of spectrum by some public sectors". EC DG INFSO/B4/RSPG. 11 February 2009.

NOTE: Available at http://rspg.groups.eu.int/.

[i.24] ETSI TR 102 683: "Reconfigurable Radio Systems (RRS); Cognitive Pilot Channel (CPC)".

[i.25] ETSI TR 102 682: "Reconfigurable Radio Systems (RRS); Functional Architecture (FA) for the Management and Control of Reconfigurable Radio Systems".

[i.26] ETSI TR 102 476: "Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities".

[i.27] ETSI TR 102 445: "Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness".

[i.28] ETSI TR 170 012 (V3.1.1): "Project MESA; Technical Specification Group - System; System Overview".

[i.29] ETSI TR 102 745: "Reconfigurable Radio Systems (RRS); User Requirements for Public Safety".

[i.30] ETSI TR 122 952: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Priority service guide (3GPP TR 22.952)".

[i.31] ETSI TR 122 953: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Multimedia priority service feasibility study (3GPP TR 22.953)".

[i.32] ETSI TS 122 153: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Multimedia priority service (3GPP TS 22.153)".

[i.33] ETSI TR 102 839: "Reconfigurable Radio Systems (RRS); Multiradio Interface for Software Defined Radio (SDR) Mobile Device Architecture and Services".

[i.34] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)".

[i.35] ETSI TS 170 016: "Project MESA; Technical Specification Group - System; Functional Requirements Definition".

[i.36] D2.1:"Report on ICT Research and Technology Development status for public safety".

[i.37] ETSI TR 170 002: "Project MESA; Service Specification Group - Services and Applications; Definitions, symbols and abbreviations".

[i.38] ETSI TR 170 003: "Project MESA; Service Specification Group - Services and Applications; Basic requirements".

[i.39] SAFECOM: "Public Safety Radio Frequency Spectrum: A Comparison of Multiple Access Techniques".

[i.40] SAFECOM: "Public Safety Architecture Framework Volume I and II and Trial Report".

[i.41] CHORIST: "Reports on improvements to existing legacy PMR and broadband systems".

[i.42] CHORIST: "Report on Wideband network definition and design".

[i.43] CHORIST: "Report on Broadband network definition and design".

[i.44] IEEE 802.16e: "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands".

# 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.

**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

NOTE: As an example, non-RRS network node is a conventional wireless communications systems based on TETRA Release 1 [i.22].

**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

## 3.2 Abbreviations

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

| | |
|---|---|
| AP | Access Point |
| APCO | Association of Public-Safety Communications Officials International |
| API | Application Program Interface |
| BER | Bit Error Rate |
| CALM | Communications, Air-interface, Long and Medium range |
| CCM | Cognitive Control Manager |
| CDMA | Code Division Multiple Access |
| CEPT | European Conference of Postal and Telecommunications Administrations |
| CPC | Cognitive Pilot Channel |
| CQPSK | Compatible differential offset Quadrature Phase Shift Keying |

NOTE: QPSK-C to be changed to CQPSK in the document.

| | |
|---|---|
| CR | Cognitive Radio |
| CRS | Cognitive Radio System |
| CS | Circuit Switched |
| DMO | Direct Mode of Operation |
| DoS | Denial of Service |
| DSM | Dynamic Spectrum Management |
| DSP | Digital Signal Processor |
| E2R | End-to-End Reconfigurability |
| EAN | Extended Area Network |
| ECC | Electronic Communications Committee |
| EDA | European Defence Agency |
| ESRA | European Software Radio Architecture |
| ESRAB | European Security Research Advisory Board |
| ESRIF | European Security Research and Innovation Forum |
| EVM | Error Vector Magnitude |
| FDMA | Frequency Division Multiple Access |
| FM | Frequency Management |
| FPGA | Field Programmable Gate Array |
| GPP | General Purpose Processor |
| GSM | Global System for Mobile communications |
| HF | High Frequency |
| HSD | High Speed Data |
| HSDPA | High Speed Downlink Packet Access |
| HSPA | High Speed Packet Access |
| HSUPA | High Speed Uplink Packet Access |
| HW | Hard Ware |
| IAN | Incident Area Network |
| ICT | Information and Communication Technology |
| IDIS | Intra-Device Interface Standard |
| IDL | Interface Definition Language |
| ITS | Intelligent Transportation System |
| JAN | Jurisdiction Area Network |
| LS | Liaison Statement |
| MF | Medium Frequency |
| MSP | Multilevel Security Path |
| MSS | Mobile Satellite Services |
| MTSS | Mobile Terminal Semi-Stationary |
| NATO | North Atlantic Treaty Organization |
| NIAG | NATO Industrial Advisory Group |
| NNEC | NATO Network Enabled Capability |

NOTE: This is a NATO term and it does not appear in ETSI.

| | |
|---|---|
| OMG | Object Management Group |
| PAMR | Public Access Mobile Radio |

| | |
|---|---|
| PER | Packet Error Rate |

NOTE: This term is not in TEDDI but it is common knowledge.

| | |
|---|---|
| PMR | Professional Mobile Radio |
| PPDR | Public Protection and Disaster Relief |
| PSCD | Public Safety Communication Device |
| QoS | Quality of Service |
| RAT | Radio Access Technologies |
| RF | Radio Frequency |
| RFI | Request From Information |
| RRS | Reconfigurable Radio Systems |
| RSPG | Radio Spectrum Policy Group |

NOTE: This term is not in TEDDI but the acronym is already defined in the document.

| | |
|---|---|
| RTOS | Real Time Operating System |
| SCA | Software Communications Architecture |
| SCM | Self Cognitive Module |
| SCV | Spectrum Conformance Validator |
| SDA | Software Download Authentication |
| SDD | Software Download Distributor |
| SDR | Software Defined Radio |
| SDRF | Software Defined Radio Forum |
| SoR | Statement of Requirements |
| SW | Soft Ware |
| SW | Soft Ware |
| TDMA | Time Division Multiple Access |
| TETRA | TErrestrial Trunked Radio |
| TIA | Telecommunications Industry Association |
| UAV | Unmanned Arial Vehicle |
| UHF | Ultra High Frequency |
| UMTS | Universal Mobile Telecommunications System |
| VHF | Very High Frequency |
| WCDMA | Wide band Code Division Multiple Access |
| WF | WaveForm |

# 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 Association of Public-Safety Communications Officials International (APCO)

"The Association of Public-Safety Communications Officials International (APCO) is a member driven association of communications professionals that provides leadership; influences public safety communications decisions of government and industry; promotes professional development; and, fosters the development and use of technology for the benefit of the public" (from APCO web site, http://www.apcointl.org/. Last Accessed 4 September 2008).

APCO has been responsible for the definition of Project 25 suite of standards, which are mostly used by federal, state/province and local public safety agencies in North America to enable them to communicate with other agencies and mutual aid response teams in emergencies. The evolution for Broadband communication was APCO Project 34, the North American predecessor of Project MESA, q.v.

The following inputs are relevant for requirements definition:

- Technical reports produced by P25 User needs committee.

### 4.1.2 European Commission DG INFSO

In EC DG INFSO, the following entities are responsible for Radio Spectrum:

- Radio Spectrum Policy Group:
  - The RSPG set up in 2002 gathers high-level governmental experts from member States and helps the Commission developing general radio spectrum policy at Community level.
- Radio Spectrum Committee:
  - The RSC, created under the Radio Spectrum Decision in accordance with comitology rules, assists the Commission for the adoption of technical implementing measures in support of Community policies.

The following documents are relevant for system and technology aspects:

- PSC-Europe/RD/016. Status of Radio Spectrum Harmonization for the Emergency Services in the European Union.

### 4.1.3 ECC

The Electronic Communications Committee (ECC) is part of the CEPT (European Conference of Postal and Telecommunications Administrations).

ECC is responsible for (from [i.14]):

1) considering and developing policies on electronic communications and activities in a European context, taking account of European and international legislation and regulations;

2) develop European common positions and proposals, as appropriate, for use in the framework of international and regional bodies;

3) forward plan and harmonize within Europe the efficient use of the radio spectrum, satellite orbits and numbering resources, so as to satisfy the requirements of users and industry;

4) take decisions on the management of the work of the ECC.

The following documents are relevant for system and technology aspects, especially in relation to spectrum usage by the public safety domain:

- ECC REPORT 102 [i.15].

### 4.1.4 ETSI EMTEL

The activities of TC EMTEL will follow the broad areas of:

- preparation of ETSI deliverables used to describe requirements for Users, Network Architectures, Network Resilience, Contingency planning, Priority Communications, Priority Access Technologies (e.g. Twisted Pair, Cable/ HFC, Satellite, Radio Frequencies/ fixed and mobile, new solutions) and Network management;

- studies of the issues related to National Security and Public Protection and Disaster Relief (PPDR).

The following documents are relevant for system and technology aspects:

- TR 102 476 [i.26];

- TR 102 445 [i.27]. The scope will also encompass the resiliency of mobile radio and/or other forms of emergency communications to/from the emergency responding units. The effort will address the resiliency of emergency communications, the availability of adequate capacity during periods of network component/facility failure or periods of high capacity demands due to disasters, terrorism or similar events, and expedited restoration during major service interruptions.

### 4.1.5 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 following documents are relevant for system and technology aspects:

- Liaison Statement (LS) from ETSI TETRA TC to ETSI RRS TC regarding Digital Dividend Spectrum Cognitive Radio (CR). TETRA31 (08) 22.

### 4.1.6 Intelligent Transportation System

The Intelligent Transportation System (ITS) refers to the set of information and communication technologies used to improve the transport infrastructure and vehicles to improve safety, efficiency and reduce vehicle wear and fuel consumption.

ITS is related to the public safety domain because many of the proposed ITS systems may involve surveillance of the roadways. ITS can also support the resolution of emergency crisis by improving the effort of mass evacuation or by increasing the operational speed and efficiency of the first responders.

ITS can take advantage of RRS technology to provide mobile equipment, which is re-configurable when moving among relevant regulatory jurisdictions. Furthermore ITS equipment should minimize spectrum interference with other standardized regional radio units and RRS technology could be used to this purpose.

In relation to the telecommunication domain, the CALM (Communications, Air-interface, Long and Medium range) is an important element to consider. CALM has been started by ISO TC 204/Working Group 16 to define a set of wireless communication protocols and air interfaces for a variety of communication scenarios spanning multiple modes of communications and multiple methods of transmissions in Intelligent Transportation System (ITS).

The documents produced by the following working groups are relevant for RRS system and technology aspects in Public Safety domain:

- SWG 16.0 Architecture.
- SWG 16.5 Emergency Communications.
- SWG 16.7 Security and Lawful Intercept.

### 4.1.7 NATO

The NATO C3 Organization (NC3O) was created in 1996 to ensure the provision of a NATO-wide cost-effective, interoperable and secure C3 capability, meeting the NATO users' requirements by making use of common funded, multinational and national assets.

The following documents are relevant for system and technology aspects:

NOTE: Some documents may be of restricted access and they may not be used directly.

- Framework for sharing common waveforms [i.2].
- NATO Industrial Advisory Group (NIAG) study on SDR [i.3].
- Software defined radio to enable NNEC: technical challenges and opportunities for NATO by Michael Street (see [i.4]).

### 4.1.8 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 system and technology aspects:

- D2.1 - "Report on ICT Research and Technology Development status for public safety" [i.36]. The purpose of the present document is to provide a list of background technical material of relevance for public safety communication.

### 4.1.9 Project MESA

Project MESA is an international partnership producing globally applicable technical specifications for digital mobile broadband technology, aimed initially at the sectors of public safety and disaster response.

The following documents are relevant for system and technology aspects:

- Service Specification Group - Services and Applications - Statement of Requirements (SoR) (TS 170 001 [i.34]).
- Service Specification Group - Services and Applications - Definitions, symbols and abbreviations (SoR) (TR 170 002 [i.37]).
- Service Specification Group - Services and Applications - Basic requirements (SoR) (TR 170 003 [i.38]).
- Technical Specification Group - System Overview (TR 170 012 [i.28]).
- Technical Specification Group - System and Network Architecture (TR 102 653 [i.13]).
- Technical Specification Group - Functional Requirements Definition (TS 170 016 [i.35])..

### 4.1.10 SAFECOM

SAFECOM is an US communications program of the Department of Homeland Security. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies.

The following documents are relevant for system and technology aspects:

- "Public Safety Radio Frequency Spectrum: A Comparison of Multiple Access Techniques" [i.39]. The present document discusses the functionality of each access method (FDMA, TDMA and CDMA), the advantages and disadvantages of each technology, and various forms of implementation for each technology.

- "Public Safety Architecture Framework Volume I and II and Trial Report" [i.40].

### 4.1.11 SDR Forum

The 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 system and technology aspects:

- Software Defined Radio Technology for Public Safety. Working Document SDRF-06-W-0001-1 (see [i.1]). The document provides an exhaustive study of the application of SDR to the Public Safety domain. The study is complemented by results from RFI (Request From Information) on this topic sent to relevant end-user, industry and regulation organizations.

[i.1] provides important information and recommendations, which should be taken in consideration in the present document:

- Clause 4.1 provides deployment and implementation considerations. The answers from RFIs indicate that software definable gateway should be one of the highest priorities as they would ease the integration of various network infrastructures. The clause provides also indications on the tradeoffs between a SDR base station approach and a network based on non-SDR base stations and terminals capable of interfacing with various air-interfaces.

- Clause 4.2 provides a discussion on what is the role of standardization and what should be standardized. The main choice is about the standardization of the internal interfaces of the radio device or Intra-Device Interface Standard (IDIS) as it is called in [i.1] or the standardization of the network interfaces between the radio devices and other elements of the network like the air-interface. If the standardization of the IDIS is addressed, the main question is whether adopt the SCA architecture as a reference for the IDIS standardization. In the document, it is noted that SCA was created on the basis of military requirements which are similar but more severe than public safety requirements. Cost, performance or power consumption are important factors to be considered in the definition of IDIS. Non-SCA IDIS like the ones from the commercial domain should also be considered even if they may not meet the needed public safety requirements. If the standardization of the IDIS is not addressed, [i.1] specifies the standardization of the software download functionality as a main area to address.

- Clause 4.3 describes the role of cognitive applications. Cognitive techniques can be used to increment the operational capabilities of public safety responders to be more aware of the RF environment, automatically reconfigure and connect, use additionally spectrum resources if needed. A main area of concern is if spectrum sharing can be allowed or is too risky for public safety applications. Furthermore, the question is whether "cognitive capability can be included in the same box as SDR for all potential applications and techniques or whether a separate box with a well-defined standard interface is required in some uses for at least the near future in order to avoid additional size, weight, cost and power concerns".

## 4.2 Projects

### 4.2.1 Project CHORIST

Project CHORIST (integrating communications for enhanced environmental risk management and citizens safety) is a 3-year project (June 2006 to May 2009), funded by the European Commission, which addresses Environmental Risk Management in relation to natural hazards and industrial accidents.

CHORIST will propose solutions to increase rapidity and effectiveness of interventions following a major natural and/or industrial disaster in order to enhance citizens' safety and communications between rescue actors.

The following documents are relevant for system and technology aspects.

Deliverables of CHORIST SP4 (Emergency telecommunication systems on crisis site) including:

- Reports on improvements to existing legacy PMR and broadband systems (SP4.D3) [i.41].
- Report on Wideband network definition and design (SP4.D4) [i.42].
- Report on Broadband network definition and design (SP4.D5) [i.43].

### 4.2.2 E2R

The End-to-End Reconfigurability (E2R) project aims at bringing full benefits of the valuable diversity within the Radio Eco-Space, composed of wide range of systems such as Cellular, Wireless Local Area and Broadcast. The key objective of the E2R project is to devise, develop and trial architectural design of reconfigurable devices and supporting system functions to offer an expanded set of operational choices to the users, applications and service providers, operators, regulators in the context of heterogeneous mobile radio systems.

The following deliverables are relevant for system and technology aspects.

- D1.4: E2E ReconfigurabilityManagementSystem-level Architecture;
- D3.3: Reconfiguration ManagementPlane and Designof NetworkSupportFunctionsand Signalling;
- D4.3: Functional Physical Layer Architecture.

### 4.2.3 ESSOR

The ESSOR study is a Cat B program under the auspices of the EDA which will address the following main objectives in order to give European industry the capability to develop interoperable SDR in the period from 2010 to 2015.

These include:

1) Developing, in a relationship with the United States, the normative referential required for development and production of software radios in Europe.

2) Setting up a common security basis to increase interoperability between European forces as well as with the United States.

3) Stimulating a balanced transatlantic relationship on SDR.

This project may develop an architecture as described in [i.6].

### 4.2.4 EULER

This project aims to leverage software defined radio (i.e. a fully programmable radio conforming to some embedded software standard allowing radio applications to be ported from platform to platform) to bring novel efficient interoperability capabilities to wireless systems used by European P&GS forces when confronted to joint operations in crisis situations (from EULER Description of Work).

The following deliverables may be relevant for system and technology aspects:

- Deliverables of WP3: P&GS communication system open architecture.
- Deliverables of WP4: Software defined radio standard and platforms.
- Deliverables of WP5: ESRA waveforms and related components.

### 4.2.5 WIDENS

Wireless DEployable Network System (WIDENS) Project WIDENS was a two-year co-operative Research and Development project involving European industries and universities. The project was supported by the European Commission under the IST Framework Programme 6. It ended in January 2006. The overall objective of the WIDENS project was to design, prototype and validate a high data-rate, rapidly deployable and scalable wireless ad-hoc communication system for future public safety, emergency and disaster applications.

The following documents are relevant for system and technology aspects:

- D2.2 "System Aspects".

### 4.2.6 WINTSEC

With the support of a User Group involving emergency and security End-Users from 6 EU nations, taking into account daily operations, along with complex interventions at national or multinational level, WINTSEC explores a mix of complementary solutions to overcome the barriers for wireless interoperability across different security agencies, taking into account the constraints of the security services and the legacy base (from WINTSEC Description of Work).

The following documents are relevant for system and technology aspects:

- Deliverables of WP 2, 3 and 4 for System Architecture for Interoperability - Core Network Layer, System Architecture for Interoperability - Impact of SDR and Information Assurance Architecture for Interoperability.

### 4.2.7 WISECOM

The WISECOM project is co-funded by the European Commission. It studies, develops, and validates by live trials candidate rapidly deployable lightweight communications infrastructures for emergency conditions (after a natural or industrial hazard).

The system integrates terrestrial mobile radio networks - comprising GSM, UMTS, WiFi, and optionally WiMAX and TETRA - over satellite, using Inmarsat BGAN and DVB-RCS systems.

The following documents are relevant for system and technology aspects:

- D2.1-1: "Terrestrial and Satellite Systems for Emergency Situations".
- D2.2-1: "Overall System Architecture Definition". This is currently a confidential document and it may not be available for this study.

# 5 Current communication systems in Public Safety

This clause has the purpose to describe the existing wireless communication systems used by Public Safety organizations.

The list, in alphabetical order, includes technologies also used in the commercial domain or defence domain. Such diversity can generated interoperability issues during the resolution of an emergency crisis.

The application of RRS technologies to the Public Safety domain may be based on the evolution of one or more technologies presented in this clause.

Both analog and digital systems do coexist in the Public Safety domain even if the current trend is for a wider deployment of digital systems.

The use and deployment of a wireless communication technology may depend on the type of operational scenarios. For this reason, the clause provides a table to map the existing wireless communications systems to the most common Public Safety environment scenarios like Urban, Rural, Remote Areas, Coast, Ports and so on, which are defined in TR 102 745 [i.29].

## 5.1 Analog PMR

Professional Mobile Radio (PMR), also known like Private Mobile Radio or Land Mobile Radio, is an analog radio communication system used by Public Safety organizations. Before the introduction of digital systems like TETRA or APCO 25 [i.17], analog PMR was the main type of wireless communications used by Public Safety organizations.

Analog PMR usually use UHF and VHF bands.

The first Professional Mobile Radio (PMR) were simple systems composed by a single base station, which provided communication to a number of mobiles. In time, more sophisticated architectures were defined.

## 5.2 APCO 25

APCO 25 [i.17] is a standard for digital wireless communication for Public Safety domain. APCO is the acronym of Association of Public-Safety Communications Officials. APCO 25 is mostly used in the USA. The standards have been developed together with the Telecommunications Industry Association (TIA).

Four key objectives guided the steering committee in the definition of the standards:

- provide enhanced functionality with equipment and capabilities focused on public safety needs;
- improve spectrum efficiency;
- ensure competition among multiple vendors through Open Systems Architecture;
- allow effective, efficient, and reliable intra-agency and inter-agency communications.

APCO 25 [i.17] is based on the FDMA access method and QPSK-C modulation. Data rate communications are supported to a maximum of 9,6 Kbits/s. An evolution of APCO 25 [i.17] is currently under development to provide broadband connectivity. Further details are in [i.17].

## 5.3 Commercial cellular networks GSM/GPRS/UMTS/3G

Commercial cellular wireless communication systems like GSM/GPRS and UMTS have not been designed for Public Safety purposes as they lack the level of reliability, availability, responsiveness and security requested by Public Safety organizations. Nevertheless, there are public safety organizations in the world, which do use commercial cellular wireless system because of lack of alternatives in the area, where they operate. In comparison to commercial networks, public safety organizations have a high cost per subscriber in the dedicated public safety network because the overall number of subscribers is small in comparison to the cost of the network. Obviously public safety networks are designed for the protection of the citizen or the nation and not on business requirements.

The recent evolution of commercial cellular networks has resulted in high spectrum efficiency and increase bandwidth. Cellular networks have started to become an option for public safety users to reduce the cost per subscriber. An important advantage of modern cellular networks is represented by the capability to provide high data rate communications. The High Speed Packet Access (HSPA) is a collection of two mobile telephony protocols High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), which extend the performance of existing WCDMA protocols.

The main issue with the applications of these technologies is that they are not designed on the basis of the Public Safety requirements. Further details on this issue are in [i.20].

Furthermore, public safety networks and commercial networks should be internetworking and interoperable to share network resources. An important functionality, which was missing in commercial networks until few years ago, is the prioritization of the network resources. Recently, the 3GPP standardization body has produced a feasibility study on the providing priority access to radio channels for voice and data (see [i.21]). More details in clause 6.6.

## 5.4 TETRA

TETRA (TErrestrial Trunked Radio) is an open digital trunked radio standard defined by the ETSI (European Telecommunications Standards Institute) to meet the needs of Public Safety organizations and other professional mobile radio users involved in critical applications.

TETRA uses TDMA technology with 4 timeslots at a bandwidth of 25 kHz per carrier. The standard defines the air interface, the peripheral interface and the inter-system interface but not the architecture within the system infrastructure. TETRA provides data rate channels at 9,6 Kbits/s, but an evolution of TETRA is being defined to provide higher data connectivity.

TETRA is wide deployed in Europe and other countries around the world (see [i.22]). Because of the dominant role of this technology, the application of RRS to the Public Safety domain may be strongly related to the evolution of TETRA.

The original Voice plus Data standard is known as TETRA Release 1. The recent evolution of TETRA is TETRA release 2, which includes the new TETRA High Speed Data (HSD) service using different RF channel bandwidths and data rates for flexible use of PMR frequency bands.

## 5.5 TETRAPOL

Tetrapol has been developed for Public Safety usage on the requirement of the French police forces. Even though the name of the product is similar to TETRA, Tetrapol is quite different from the ETSI TETRA standard. Tetrapol is a proprietary solution from EADS Telecom (former Matra) and has never been accepted as an ETSI standard.

Tetrapol uses FDMA technology providing one speech or control channel per 12,5 kHz carrier. Tetrapol solutions are mostly adapt in networks with few users covering a large area, which is typically the case in single agency networks.

## 5.6 Satellite Networks

The main advantage of satellite networks for Public Safety organizations is that they do not need an existing terrestrial infrastructure. Satellite networks can transmit in a number of frequency bands (C-Band, Ku Band) depending on the coverage provided by the satellite network. The main deployment costs of a satellite network are the satellites themselves.

Mobile Satellite Services (MSS) are satellite systems based on portable terrestrial terminals. MSS terminals can be installed on trucks, automobiles, ships or even airplanes. MSS terminals can be an important asset in the public safety domain by providing almost full coverage and the benefit of mobility.

MSS will have a wide deployment in Europe as described in [i.16].

## 5.7 WiFi/WiMAX

Like GSM/GPRS/UMTS, WiFi and WiMAX are commercial systems, which have not been designed for Public Safety purposes. WiFi has very short coverage (200 meters to 300 meters), while WiMAX has much larger coverage. Both systems have been designed to be an extension of the fixed network to provide broadband connectivity. Lack of support for mobility is an issue for both systems, even if more recent versions of WiMAX (802.16e [i.44]) improve the limits for mobility.

WiFi and WiMAX are currently investigated, in the Public Safety domain, to implement ad-hoc or mesh wireless networks in the area of the emergency crisis, where they could provide the needed broadband connectivity.

## 5.8 Marine Communications

This category includes all the different types of communications used by marine public safety organizations like coastal guards. Marine Communications are usually based on MF/HF or VHF channels for ship-to-shore or ship-to-ship communications. Marine public safety organizations may also use satellite networks (especially MSS) and GSM/UMTS. The most common radio communication is VHF around in the 150 MHz to 160 MHz band, which is an almost line-of-sight (around 30 Kms to 40 Kms). Communication beyond the horizon is done using MF and HF bands.

## 5.9 Avionics communication

This category includes the communication used by aircraft like airplane and helicopters, which may participate to public safety scenarios like the resolutions of a natural disaster or a large fire. Avionics are usually in the VHF band from 118 MHz to 137 MHz. In the future, mobile radio links at higher frequencies could be used to guide and receive information from Unmanned Arial Vehicle (UAV) used in border security operations.

## 5.10 Mapping Table

Table 1 provides an indication of usage (High, Medium and Low) of the different types of communication systems in various types of scenarios. The indication is based on the current level of deployment and they may change in the future.

**Table 1: Use of communications in Public Safety scenarios**

| | Urban | Rural | Coast | Border | Port |
|---|---|---|---|---|---|
| **Digital PMR (APCO 25, TETRA, TETRAPOL)** | High | Medium | Low | Medium | Medium |
| **Satellite Networks** | Low | High | Low | Low | Low |
| **PMR (Non-Tetra)** | High | High | Medium | Medium | Medium |
| **GSM/UMTS** | High | Medium | Medium | Medium | Medium |
| **WiFi/WiMAX** | Medium | Low | Low | Low | Low |
| **Marine Communications** | Low | Low | High | Medium | High |
| **Avionics Communications** | Medium | High | Medium | Medium | Low |

An important element to consider is the deployment cost of each technology in the various operational contexts. Below is a qualitative estimate of the deployment costs. The costs are based on the typical usage of telecommunications by public safety organizations, which is higher in urban areas and lesser in rural areas. Table 2 is based on the questionnaire results described in TR 102 745 [i.29].

Satellite Networks are a special case, as the deployment costs are mostly based on the satellite itself and it is independent on the context.

**Table 2: Deployment cost of communications in Public Safety scenarios**

| | Urban | Rural | Coast | Border | Port |
|---|---|---|---|---|---|
| **Digital PMR (APCO 25, TETRA, TETRAPOL)** | High | Medium | Medium | Medium | Medium |
| **Satellite Networks** | N/A | N/A | N/A | N/A | N/A |
| **PMR (Non-Tetra)** | High | Low | Low | Medium | Medium |
| **GSM/UMTS** | High | Medium | Medium | Medium | Medium |
| **WiFi/WiMAX** | High | Medium | Medium | Medium | High |
| **Marine Communications** | Low | Low | Medium | Low | Medium |
| **Avionics Communications** | Low | Low | Low | Medium | Low |

# 6 Overall System Design

## 6.1 Introduction

Today the overall Public Safety communication infrastructures are a complex system composed by a heterogeneous set of networks and ICT systems developed by the various Public Safety organizations. In time, each Public Safety organization has developed its own "vertical" ICT system to satisfy its needs and requirements. Furthermore, Public Safety organizations of the same type may have different systems in different nations across Europe. This diversity can cause problems of communication and lack of interoperability in trans-national operational scenarios like border security or when a large emergency crisis involve more than one public safety organization.

In many cases, the development of public safety telecommunication standards like TETRA has mitigated this problem by providing a single infrastructure and a single type of communication. However, its deployment has not included all the public safety organizations in Europe yet. Interoperability is still a Public Safety challenge, which could be resolved or mitigated by radio systems, which have the capability to provide connectivity to the various communication systems present in the emergency area. RRS could be used to create "bridges" across different public safety communication systems or to provide the capability to a handheld used by public safety officer to "talk" to various radio systems. More details on interoperability are in clause 6.6.

Interoperability is not the only capability that the deployment of RRS technologies can deliver.

Public Safety operations are usually unplanned in response to emergency crisis or natural disasters, which destroys critical facilities in the area and endanger human lives. RRS technologies can provide the necessary flexibility to cope with unplanned events or conditions, which a non-RRS radio system would not be able to provide.

EXAMPLE 1: An increased communication bandwidth may be needed to transmit images, video or information on the plan of a building.

The flexibility is also necessary to increase the robustness and reliability of the network to respond to external interferences or disturbances. RRS technology can be used to change, in real time, transmission parameters like power, frequency, and modulation and so on. This capability can be used to increase the communication efficiency and lower battery consumption but also to implement operational procedures for specific scenarios.

EXAMPLE 2: A Public Safety user can set a communication mode for high data capacity and low power efficiency in a scenario or high power efficiency and voice narrowband communications only in another scenario.

Some of these capabilities are already present in the communication systems and standards presented in clause 5. RRS technologies can be used to augment these capabilities or be part of the evolution of the described communication standards.

The main challenge, for the deployment of RRS technology in the Public Safety domain, is to provide the same level of reliability, responsiveness and availability provided by existing public safety wireless communication systems like TETRA otherwise they will not accepted by Public Safety end-users, who have severe acceptance criteria for their equipment and communication networks.

Finally, security plays an important role in Public Safety communication. The data distributed across a Public Safety communication network is high sensitive or the networks are connected to ICT infrastructures with high levels of security. Public Safety organizations have different levels of security. From one extreme, we have military and defence organization, which participates to the resolution of large emergency crisis or natural disasters; on another extreme we have volunteer organizations with very low level of security. In the between, we have police, fire-fighters, emergency health services with various level of security. Data should be protected without impacting the quality of the communication or the interoperability.

System aspects are related to the types of contexts where the Public Safety organizations may operate. An emergency crisis may be limited to a local area, where an ad-hoc wireless network is able to provide the needed connectivity or it may extend to an entire region, where one or more communication infrastructures are needed, including fixed networks. In the present document, we will use the contexts defined in Project MESA (see clause 4.1.9). In Project MESA, the term network is actually used to describe the context and a network hierarchy is defined.

These definitions will be used in the present document as well (extracted from [i.13]):

- Incident Area Network (IAN):

  The Incident Area Network (IAN) is generally dedicated to a single incident or event. A key public safety requirement is the ability for peer-to-peer and peer-to-multiple peers in the lack of any supporting infrastructure. The IAN can be pre-deployed for a planned event, such as a sporting or "nationally significant" event, or it could be dynamically deployed for an unplanned event or incident (all-hazards). Possible unplanned events range from a local law enforcement situation to relief efforts in a natural disaster area. Depending on the affected situational area and agencies engaged, interoperability, inter-connection and resource management become more critical. Note that an unplanned incident can involve fluid and challenging geographic and infrastructure scenarios that can affect initial staging operations and overall communication capabilities (i.e. terrorist attack or major hurricane/tsunami).

- Jurisdictional Area Network (JAN):

  The Jurisdiction Area Network (JAN) is designed to provide specific agency or shared access coverage over a wide area that may include such geographic boundaries as a city, county or country. The design and deployed placement of JAN infrastructure elements are well planned to ensure complete coverage and sufficient bandwidth, a high QoS level and reliability factor that corresponds to the nature of this mission-critical user group. The JAN's infrastructure utilizes powerful communication towers and other two-way broadcast infrastructure elements to provide for the capabilities mentioned above and the communications coverage required meeting public safety and public protections service agency needs. These towers or communication link points can vary in both shape and size, depending on planning and coverage needs. Some are designed for placement on hill tops while others are much smaller and are designed for use inside buildings and tunnels.

- Extended Area Network (EAN):

  The Extended Area Network (EAN) is mainly a network designed to provide connectivity between various JANs it can also include traditional backend networks.

## 6.2 Input from other TC RRS working groups

TR 102 682 [i.25] describes functional architecture of cognitive radio wireless networks in the commercial domain. The document describes the building blocks to provide Dynamic Spectrum Management functionality. Some concepts and architecture elements can be adapted to the Public Safety domain if they validate the user requirements described in TR 102 745 [i.29].

TR 102 683 [i.24] describes the design approaches for cognitive pilot channel in the commercial domain. Some of the design solutions presented in the document can be adapted to the Public Safety domain if they validate the user requirements described in TR 102 745 [i.29].

## 6.3 Functional architecture and interfaces

The present document will reuse some of the concepts described in [i.13] for the definition of the main functional architecture and interfaces.

Two views of the functional architecture and main interfaces are described in this clause. The first view provides the functional architecture of non-RRS Public Safety radio systems. The second view describes the introduction of RRS elements and the related interfaces.

The first view is presented in figure 1.

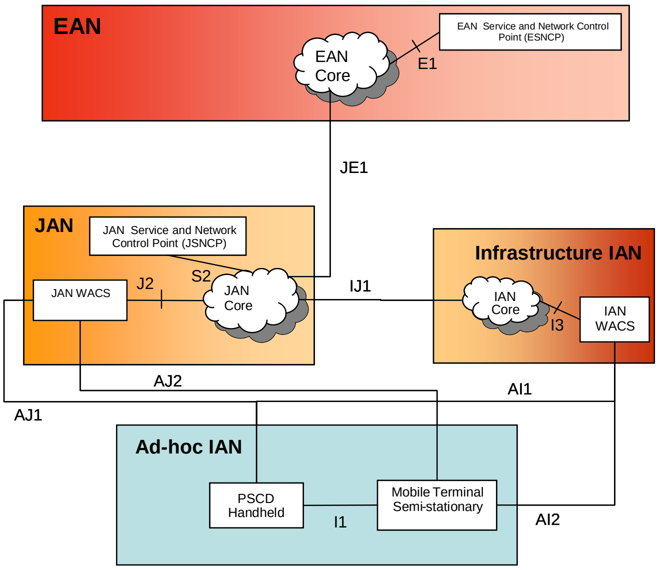

EAN
EAN Service and Network Control Point (ESNCP)
EAN Core
E1
JE1
JAN
JAN Service and Network Control Point (JSNCP)
JAN WACS
J2
S2
JAN Core
IJ1
Infrastructure IAN
IAN Core
I3
IAN WACS
AJ2
AI1
AJ1
Ad-hoc IAN
PSCD Handheld
I1
Mobile Terminal Semi-stationary
AI2

**Figure 1: Networks and interfaces (existing public safety communication systems)**

The following nodes are defined:

- Public Safety Communication Device (PSCD) is a handheld terminal or mobile device to be carried by Public Safety officers. It can be used to support a mobile or fixed sensor device (radar, video-camera). The performance of a PSCD is usually limited in comparison to the other nodes because of its limited sized and power capabilities. Nevertheless, PSCD is the main form of communication for Public Safety officers and it represents a significant part of the Public Safety communication infrastructures in terms of numbers and budget impact.
- Mobile Terminal Semi-Stationary (MTSS) is a terminal installed on a vehicle or a device installed in a specific location to be used as a sensor. Because MTSS has access to power sources either provided by the vehicle or installed together with the sensor, it can provide improved performances and functionalities in comparison to a PSCD. Usually MTSS are also used to implement Access Point (AP) for local ad-hoc wireless network composed by PSCDs. For example, this is the case of TETRA vehicular terminal, which can provide a limited coverage area to PSCD through TETRA Direct Mode of Operation (DMO).
- IAN WACS represents the wireless access point of the fixed wireless infrastructure, which provides wireless connectivity in the IAN context. For example, a TETRA base station or an analog PMR wireless radio station. IAN WACS provide coverage to a specific area and they support the traffic of a specific number of terminals.
- JAN WACS represents the wireless access point of the fixed wireless infrastructure, which provides wireless connectivity in the JAN context.

EXAMPLE: A maritime HF wireless radio station, which provides coverage to a wide coastal or maritime region.

- IAN Core represents the core network of the fixed wireless infrastructure in the IAN context.
- JAN Core represents the core network of the fixed wireless infrastructure in the JAN context. It is used to connect IAN Core elements.
- EAN Core represents the core network of the fixed wireless infrastructure in the JAN context. It is used to connect JAN Core elements.

The following interfaces are defined:

- Interface I1. This is an interface between PSCD and the Mobile Terminal Semi-stationary. This interface supports communications from one PSCD to one or more PSCDs or Mobile terminals, in the absence of any fixed or transportable infrastructure. An example is the Direct Mode of Operation (DMO) between a TETRA handheld terminal and a TETRA vehicular terminal.
- Interface AI1. This is an interface between the PSCD and the IAN WACS. An example is the air-interface connection between a TETRA handheld terminal and a TETRA base station.
- Interface AI2. This is an interface between the MTSS and the IAN WACS. An example is the air-interface connection between a TETRA vehicular terminal and a TETRA base station.
- AJ1. This is an interface between the MTSS and the JAN WACS. An example is the long range connection between an HF or VHF vehicular terminal used by Public Safety and a HF or VHF radio station, whose coverage spans a JAN.
- AJ2. This is an interface between the PSCD and the JAN WACS. An example is the long range connection between an HF or VHF terminal used by Public Safety and a HF or VHF radio station, whose coverage spans a JAN.
- I3. This is an interface between the IAN WACS and the IAN Core. It may be a fixed connection (e.g. cable) or a radio link. Usually it is a high data rate connection. An example is the connection between a TETRA base station and an entry point (switch or add drop multiplexer) of the TETRA infrastructure.
- IJ1. This is an interface between IAN Core and JAN Core. It is usually a high data rate fixed connection like an IP connection based on fibre optic cable.

- J2. This is an interface between JAN WACS and JAN Core. It may be a fixed connection (e.g. cable) or a radio link. Usually it is a high data rate connection. An example is the connection between an HF radio station and a control centre of the Public Safety organization.

- S2. This is an interface between JAN WACS and JAN SNCP. The JAN SCNCP contains the dispatch office for the jurisdiction. In addition the JAN SNCP handles interfacing between an established EAN and the JAN. It may be a fixed connection (e.g. cable) or a radio link. Usually it is a high data rate connection.

- JE1. This is an interface between the JAN Core and EAN Core. It is usually a high data rate fixed connection like an IP connection based on fibre optic cable.

- E1. This is the interface between the EAN cores EAN SNCP for dispatching purpose.

The application of RRS technology introduces additional nodes and interfaces. Terminals and base stations based on RRS technology coexist with equipment which does not have these capabilities.

In the rest of the clause, we identify with the term RRS, the terminals and base stations, which has cognitive radio capabilities or which are based on software defined radio (see clause 3.1).

With the term non-RRS, we identify conventional wireless communication systems, which do not have cognitive radio capabilities or they are not based on software defined radio (see clause 3.1).

RRS terminals and base stations have the capability to communication both to other RRS nodes but also to conventional radio equipment.

In a RRS enabled network, the following new nodes and interfaces will be present.

NOTE 1: To simplify the schema the previous interfaces have not been represented again.

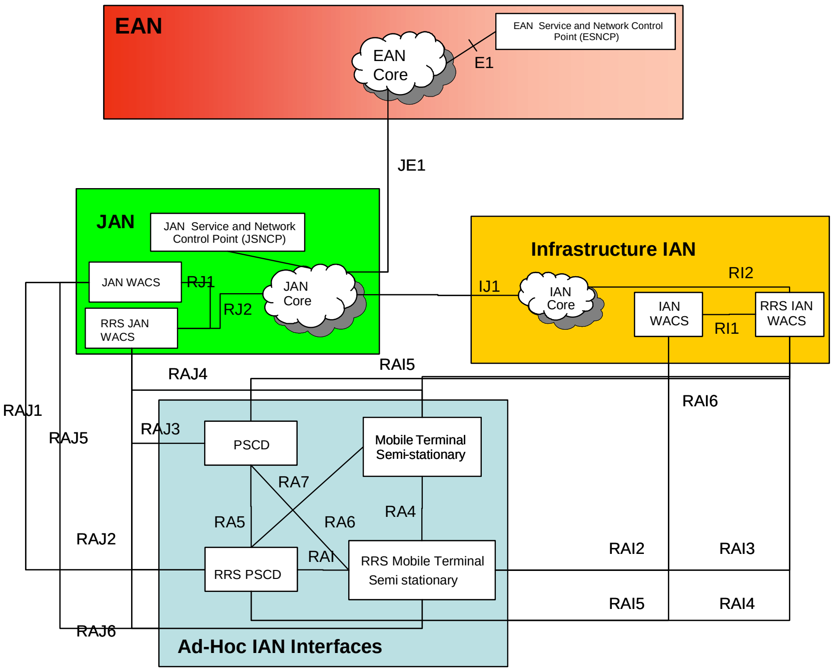


**Figure 2: Networks and interfaces (RRS enabled public safety communication systems)**

The following additional nodes are defined:

- RRS Public Safety Communication Device (PSCD) is a handheld terminal or mobile device with RRS capability. It can be used to support a mobile or fixed sensor device (radar, video-camera). Such node is able to connect with all the non-RRS nodes described in the previous schema including PSCD, MTSS, IAN WACS and JAN WACS (support for interoperability). It has cognitive radio capability (support for dynamic spectrum management) and is able to collaborate with the other RRS nodes present in the network. Power consumption will still be a limitation for RRS PSCD. Cognitive Radio and reconfigurability could require more processing capabilities and faster consumption, but it could also increase the overall efficiency.

- RRS Mobile Terminal Semi-stationary (MTSS) is a terminal installed on a vehicle or a device installed in a specific location to be used as a sensor with RRS capability. Such node is able to connect with all the non-RRS nodes described in the previous schema including PSCD, MTSS, IAN WACS and JAN WACS (support for interoperability). It has cognitive radio capability (support for dynamic spectrum management, beyond the capabilities of today's trunked radios) and is able to collaborate with the other RRS nodes present in the network.

- RRS IAN WACS represents the wireless access point of the fixed wireless infrastructure with RRS capability. RRS IAN WACS is able to connect to non-RRS nodes (PSCD, MTTS) and RRS nodes. RRS IAN WACS may provide the capability of "bridging" that is to provide interoperability between two different radio systems presents in the area. For example a RRS IAN WACS could have two air interfaces to TETRA and to Analog PMR and able to create a connection between their respective terminals. RRS IAN WACS should be able to provide cognitive radio capability. If a centralized cognitive radio approach is chosen, the RRS IAN WACS will act as a control node in the IAN network. It may cooperate with RRS JAN WACS nodes.

- RRS JAN WACS represents the wireless access point of the fixed wireless infrastructure with RRS capability. RRS JAN WACS is able to connect to non-RRS nodes (PSCD, MTTS) and RRS nodes. RRS JAN WACS may provide the capability of "bridging", that is to provide interoperability between two different radio access technologies existing in the area. RRS JAN WACS should be able to provide cognitive radio capability. If a centralized cognitive radio approach is chosen, the RRS JAN WACS will act as a control node in the JAN network and cooperate with the RRS IAN WACS nodes.

- RRS IAN CORE represents the core network of the fixed wireless infrastructure in the IAN context, with RRS capabilities. Apart from interoperability which other RRS core networks (IAN, JAN), RRS IAN CORE will have the function to operate as gateway with non-RRS IAN or JAN core networks.

- RRS JAN CORE represents the core network of the fixed wireless infrastructure in the JAN context, with RRS capabilities. Apart from interoperability which other RRS core networks (IAN, JAN), RRS JAN CORE will have the function to operate as gateway with non-RRS IAN, JAN or EAN core networks.

The following new interfaces are defined:

- Interface RA1. This is an interface between RRS PSCD and the RRS MTSS. Because both elements are RRS-based, this interface may not be based on existing telecommunication standards. The interface is one of the building blocks to define RRS-based ad-hoc wireless local networks based on the cognitive radio concept.

- Interface RA4. This is an interface between non-RRS MTSS and the RRS MTSS. It should be based on standards supported by the non-RRS terminal like TETRA DMO.

- Interface RA5. This is an interface between non-RRS PSCD and the RRS PSCD. It should be based on standards supported by the non-RRS terminal like TETRA DMO.

- Interface RA6. This is an interface between RRS PSCD and the non-RRS MTSS. It should be based on standards supported by the non-RRS terminal like TETRA DMO.

- Interface RA7. This is an interface between non-RRS PSCD and the RRS MTSS. It should be based on standards supported by the non-RRS terminal like TETRA DMO.

- Interface RAI2. This is an interface between non-RRS IAN WACS and the RRS MTSS. It should be based on standards supported by the non-RRS IAN WACS like TETRA.

- Interface RAI3. This is an interface between RRS IAN WACS and RRS MTSS. Because both elements are RRS-based, this interface may not be based on existing telecommunication standards. The interface is one of the building blocks to define RRS-based local networks based on the cognitive radio concept.

- Interface RAI4. This is an interface between RRS PSCD and RRS IAN WACS. Because both elements are RRS-based, this interface may not be based on existing telecommunication standards. The interface is one of the building blocks to define RRS-based local networks based on the cognitive radio concept.

- Interface RAI5. This is an interface between RRS PSCD and non-RRS IAN WACS. It should be based on standards supported by non-RRS base stations.

- Interface RAI6. This is an interface between non-RRS MTSS and RRS IAN WACS. It should be based on standards supported by non-RRS terminals.

- Interface RAI7. This is an interface between non-RRS MTSS and RRS IAN WACS. It should be based on standards supported by non-RRS terminals.
- Interface RAJ1. This is an interface between RRS PSCD and non-RRS JAN WACS. It should be based on standards supported by non-RRS base stations.
- Interface RAJ2. This is an interface between RRS PSCD and RRS JAN WACS. Because both elements are RRS-based, this interface may not be based on existing telecommunication standards. The interface is one of the building blocks to define RRS-based cognitive wireless networks.
- Interface RAJ3. This is an interface between non-RRS PSCD and RRS JAN WACS. It should be based on standards supported by non-RRS terminals.
- Interface RAJ4. This is an interface between non-RRS MTSS and RRS JAN WACS. It should be based on standards supported by non-RRS terminals.
- Interface RAJ5. This is an interface between RRS MTSS and non-RRS JAN WACS. It should be based on standards supported by non-RRS base stations.
- Interface RAJ6. This is an interface between RRS MTSS and RRS JAN WACS. Because both elements are RRS-based, this interface may not be based on existing telecommunication standards. The interface is one of the building blocks to define RRS-based cognitive wireless networks.
- Interface RI1. This is an interface between the IAN WACS and the RRS IAN WACS. This interface will be used for internetworking between RRS Base stations and non-RRS base stations in the local emergency network. It should be based on standards supported by non-RRS base stations.
- Interface RI2. This is an interface between the RRS IAN WACS and the RRS IAN CORE. This interface will be used for the RRS base stations to interoperate with the RRS Core network in the local emergency network.
- Interface RJ1. This is an interface between the JAN WACS and the RRS JAN WACS. This interface will be used for internetworking between RRS Base stations and non-RRS base stations in the infrastructure network.
- Interface RJ2. This is an interface between the RRS IAN WACS and the RRS IAN CORE. This interface will be used for the RRS base stations to interoperate with the RRS Core network in the infrastructure network.

NOTE 2: RRS CORE Networks element will support non-RRS IAN and JAN through the same interface and standards already defined in J2 and I3.

## 6.4 Spectrum Management

### 6.4.1 Current status of Spectrum Policy for Public Safety

The objective of this clause is to provide the current status of spectrum policies for Public Safety in Europe.

It is generally understood that spectrum availability for emergency communications should be given a high priority by regulatory authorities. Furthermore, the national and regional security dictates a permanent harmonized band, which could be effectively utilized across national boundaries at times of calamity.

So far the only harmonized public safety band available to European users is 380 MHz to 385 MHz and 390 MHz to 395 MHz in which (narrow-band) TETRA technology is the dominant user. However this band is now so highly congested in a number of European countries that it is not possible to add wide-band TETRA channels.

The Public Safety community realizes that, within a couple of years, mobile broadband data is needed for their operational tasks, both for normal daily work as for major events and disaster relief.

As done in the past with TETRA, the goal is to have a harmonized solution; this means a common choice for the technology and a harmonized frequency band.

For the technology it is logic to ask ETSI to define the standard (like it has been done with TETRA). The purpose is not to create a complete new technology but to evolve existing wideband and broadband mobile data solutions, which validates the specific Public Safety requirements like security, reliability, fast group communication and others, which are described in TR 102 745 [i.29], User Requirements in Public Safety.

One important aspect is the allocation and use of the radio frequency spectrum.

The claim for a harmonized frequency band has been made clear during 2008, regarding the Digital Dividend debate, because it looks like a perfect solution to allocate a frequency band below 1 GHz for Public Safety broadband mobile data. However the spectrum regulatory bodies have doubts if such an allocation is realistic to happen. They prefer an allocation of the spectrum for Public Safety in other bands.

The CEPT Frequency Management (FM) working group had got the task to come with a suggestion where to find frequencies for PS/PPDR use. In CEPT FM, FM38 is working hard to get a result for Public Safety. The goal is to identify a harmonized frequency band for data applications in the EU.

The survey conducted by FM38 in early 2009 received a large number of responses from the public safety sector. FM38 supports the wishes of the Public Safety sector. Because there are multiple claims for the Digital Dividend section in the 800 MHz to 900 MHz, FM38 has also looked at other parts of the spectrum including spectrum bands used by the Defence domain. The public safety sector only uses a small fraction of the overall allocated spectrum.

FM38 has advised to investigate the 300 MHz to 400 MHz band to see if it is possible to create room in this band that is open for use throughout Europe. Point of concern: this is a NATO band and the question is if defence organizations are prepared to cooperate to such an investigation?
In the June 2009 FM meeting, the FM38 recommendation for the 300 MHz to 400 MHz band has not been adopted. Early 2010 there will be a workshop to find a harmonized frequency band where all options will still be open.

Despite the non-positive feedback on Digital Dividend the decision is made not to give up on the presented claims for the public safety sector. Interoperability and mobile broadband data (spectrum) is on the political agenda.
Very important in that matter is the recommendation of Police Cooperation: the recommendation (on EU minister level!) is focused on mobile broadband data: the ECC is asked to look for a harmonized frequency band for broadband data; such a broad and high political support is unique for a request for frequency bands. For further details, see [i.23].

Interoperability is one of three fundamental requirements of the Public Safety services; the other two are the special user requirements (like reliability and availability) and the need for competition.

In a quest for a more-efficient spectrum utilization the Wireless Access Platform for Electronic Communications Services (WAPECS) concept is currently under serious consideration by European regulators. WAPECS is defined as "a framework for the provision of electronic communications services (ECS) within a set of frequency bands to be identified and agreed between European Union Member States in which a range of ECS may be offered on a technology and service neutral basis, provided that certain technical requirements to avoid interference are met, to ensure the effective and efficient use of the spectrum, and the authorization conditions do not distort competition". However, the EU Radio Spectrum Policy Group (RSPG) recognized that "The use of bands by services pursuing particular general interest objectives (e.g. Service of General Economic Interest, safety-of-life services, etc.) requires special consideration. Member states may have to fulfil some obligations relating to such services, even when they fall under the WAPECS scope and to safeguard some spectrum for them".

## 6.4.2 Dynamic Spectrum Management

### 6.4.2.1 Introduction

One of the limit of the current spectrum allocation regime based on fixed blocks of spectrum is that portions of the allocated spectrum are used in certain geographical areas and there are some portions of the assigned spectrum that are used only for brief periods of time. Studies have shown that an order of magnitude increase in capacity could be achieved if this "wasted" spectrum is utilized [i.8].

In Fixed Spectrum Management, RF spectrum is divided into frequency bands, in which specific channels are licensed to specific users for specific services. These frequency bands are subject to explicit usage rules governing the designated RF service or transmission type.

Dynamic Spectrum Management is a set of techniques for sharing radio spectrum among various users as a function of time, space, and context.

In comparison to Fixed Spectrum Management, Dynamic Spectrum Management presents (at least) the following potential advantages and disadvantages:

**Advantages:**

- Potential to improve the overall spectrum utilization
- Greater flexibility in matching spectrum availability to the user needs

**Disadvantages:**

- More complex system utilization
- Challenging regulatory and management environment
- Increased risk of wireless interferences

There are various ways of managing radio spectrum:

- **Underlay** where the signal strength is under a specified emission power limit to avoid interference with primary service. An example is Ultra Wideband.
- **Overlay** where the use of spectrum is reallocated dynamically in an opportunistic or cooperative way.
- **Equal rights** where the use of spectrum is shared by various wireless services on equal rights.

For Public Safety, we are going to focus on Overlay because Underlay has severe range or bandwidth limitations.

Overlay can be:

- Opportunistic: where spectrum is used whenever the licensee does not use it.
- Cooperative: where frequencies are allocated centrally based on real-time negotiation with the licensee.
- Mixed: where sharing is cooperative when possible and opportunistically otherwise.

Because of its high degree of reconfigurability and easiness to program, RRS is a technology enabler for Cognitive Radio (CR). Cognitive radio is a radio or wireless communication that is able to change dynamically its transmission or reception parameters by using the information collected or sensed on the external environment. The advanced flexibility, reconfigurability, learning and awareness features of cognitive radios implemented in RRS based technologies can greatly benefit public safety communications systems. Cognitive Radios is an essential enabler for Dynamic Spectrum Management.

A network based on overlay spectrum requires a higher computing power and more complexity from its components including base stations, terminals and switches. On another side, networks would be able to use the radio's cognitive abilities to achieve new levels of flexibility and reconfigurability, which can provide important advantages not only related to the improvement of spectrum efficiency but also to the overall reliability and capability of the wireless communication system.

EXAMPLE: Specific cooperation algorithms could be implemented on the cognitive radios to support operational procedures for Public Safety responders.

Cognitive Radios can also be used in the implementation of mobile ad-hoc networks to support the resolution of local emergency crisis.

### 6.4.2.2 DSM design in Public Safety domain

In cognitive radio networks, the cognitive tasks in order to enable the dynamic spectrum management are: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility.

To execute these tasks, cognitive radios may also demand control message exchanges to enhance the accuracy of spectrum sensing, reduce interference, increase network capacity and overall network robustness.

The Dynamic Spectrum Management section in TR 102 682 [i.25] (from clause 6.2), describes the Dynamic Spectrum Management (DSM) responsibilities and functions defined for the commercial domain.

Some of the described concepts can be applied to the Public Safety domain with slight modifications.

The main DSM responsibilities are:

a) Knowledge on the policies for the spectrum assignment.
These policies include the regulatory framework for the spectrum usage. In the public safety domain, there is the additional consideration that the policies may be different across national borders because the spectrum allocation is not uniform.

b) Knowledge on the current spectrum assignments.
DSM should know the current allocation and usage of spectrum bands. An issue in the public safety domain is how large is the area where DSM should have this knowledge. With reference to clause 6.3, the area could be IAN, JAN or EAN. The more the area is extended and the more difficult is to validate this responsibility. The recommendation is to limit the DSM knowledge to the IAN in a first deployment phase.

c) Provision of a spectrum framework (available amount of spectrum) to RATs, based on evaluation of spectrum occupancy and system-level parameters. Public Safety domain has a limited number of potential RATs in comparison to the commercial domain and one of them will be TETRA.

d) Knowledge on available spectrum bands for trading. In this case, public safety organizations may have higher authority and priority than commercial operators to use spectrum bands in case of emergency (see the two layers approach described in clause 6.4.2.3). Spectrum bands used by Defence may not be available in any conditions.

e) Capability to trade available spectrum bands with other DSM instances e.g. belonging to another operator. In the public safety domain this term can be widened to include public safety organizations responsible for a network or a spectrum band or operators in the commercial domain.
A major issue is if regulators will allow the trading of available spectrum among public safety organizations and commercial operators. Even if this will be allowed, another challenge is how to provide the resource management capability to trade spectrum bands among public safety and commercial domain networks.

Still with reference to TR 102 682 [i.25], the envisaged functions that are in line with the aforementioned DSM responsibilities include:

(i) the measurement collecting entity, responsible of collecting the measurements from the different nodes (i.e. terminals and cells) and existing in the heterogeneous environment;

(ii) the DSM trigger entity, responsible of detecting the relevant changes in the traffic distribution and to decide the instant when the allocation algorithm should be executed; and finally

(iii) the spectrum assignment entity, responsible of deciding on the spectrum framework to be suggested to the various RATs during the reconfiguration process.

Each of these responsibilities requires the design and implementation of sophisticated capabilities. The main one is the capability of exchanging DSM control messages (also called cognitive control messages).

The design of the best mechanism to exchange control messages has significant challenges because of the highly dynamic nature of cognitive radio wireless networks. One challenge is that cognitive radio nodes, which just enter into the network, have a limited knowledge of the environment and they have to exchange a large number of control messages to perform adequately. Another challenge is that the nodes of the wireless network need to exchange control messages if the users have high mobility or the surrounding radio environment changes frequently.

If the network is geographically wide, control messages are transmitted with medium or long transmission range. This requirement may conflict with the need for energy efficiency (low battery consumption) and low interference with traffic channels.

Two choices are possible:

- The wireless network implements a self organization scheme to allocate spectrum resources or to adjust transmission/reception parameters.

- A pre-defined control channel is used to transmit control messages among the nodes of the wireless network.

The first choice of self organizations schemes has been investigated and presented in a number of research papers.

A distributed coordination scheme was presented in [i.9]. In [i.10], the authors formulated the spectrum allocation problem as a graph multi-colouring problem. They proposed a protocol that uses a distributed local bargaining algorithm to maximize the network throughput. In [i.11], the authors propose a spectrum management scheme in which users observe local interference patterns and act independently according to a set of rules that define the trade-off relationship between performance and complexity. Self organization schemes may not respond timely enough if the radio spectrum environment or the network changes frequently.

The second choice requires the definition of a control channel where the cognitive radio nodes can exchange control messages.

As described in clause 6.2, TC RRS WG3 is investigating the application of Cognitive Pilot Channel, which is one channel or a group of channels, which are dedicated to transport control messages.

Control channels can improve the coordination of the cognitive radio network, but there are trade-offs and challenges. For example, the control channel saturation problem described in [i.12].

The design of a dedicated control channel can be roughly classified in two main categories: the in-band control channel and the out-of-band control channel.

In the in-band control channel design, the control messaging occurs in the licensed channels used for data transfer of an existing RAT. For example: the data channels of TETRA could be used to provide in-band control channel.

In the out-of-band control channel design, the control messaging occurs in a separate channel, which does not overlap with unlicensed channels. There may be the need to allocate a separate spectrum band from existing licensed bands.

The out-of-band control channel is easier to implement but it reduces the available bandwidth for traffic. Furthermore, the spectrum regulators should guarantee the allocation of the spectrum band for the control channel. This is especially challenging in Europe, where it is already difficult to harmonize the bands used by Public Safety agencies among the various nations.

The in-band control channel approach introduces lower overhead and it does not need a separate spectrum band.

The design of Cognitive Pilot Channels can also use both approaches in different phases. The E2R project (clause 4.2.2) uses a hybrid approach for the Cognitive Pilot Channel, where out-band is used in the start-up phase of the wireless network, while in-band is used in the subsequent phases.

If the control channel approach is proposed for the use of RRS and Cognitive Radio in Public Safety, WG4 should investigate in-band, out-of-band or a hybrid approach for the cognitive pilot channel.

The design of Dynamic Spectrum Management of cognitive radio in the Public Safety domain should consider, at least the following requirements:

1) Availability of communication services including control channel or exchange of control messages. Public Safety users require that a higher level of availability in comparison to commercial networks.

2) Call setup-up or service activation setup time. Public Safety communication systems have specific requirements on the maximum time needed to setup a call or activate a specific communication service.

3) Interoperability with legacy systems. An emergency situation may see the participation of various communication systems including legacy networks or terminals, which will not have cognitive radio capabilities. The design of cognitive networks for Public Safety should consider this aspect as well.

4) Availability of bands for cognitive control channels. The current situation is that there are no bands available even for data traffic (broadband connectivity).

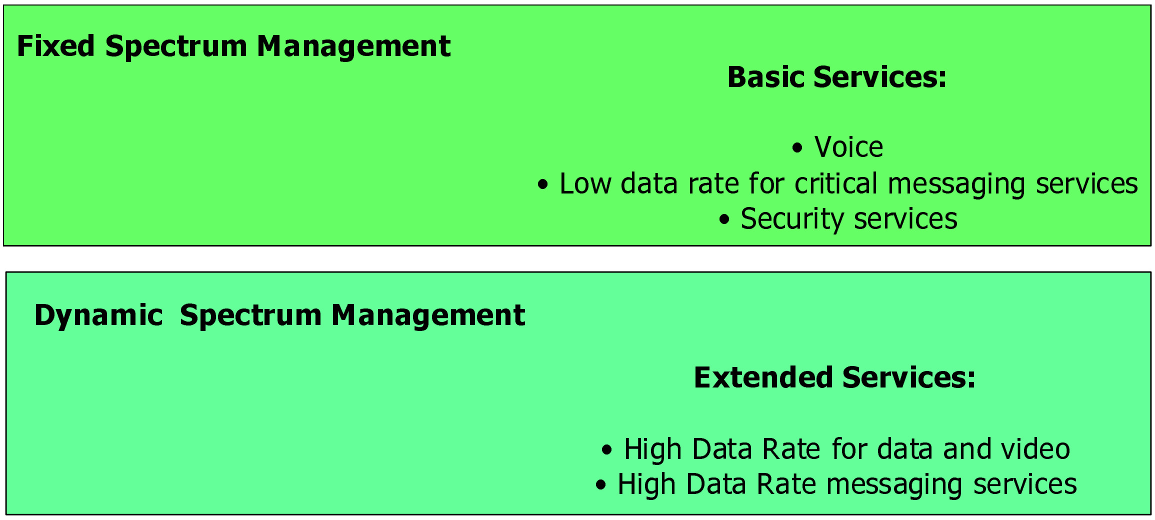
#### 6.4.2.3 DSM two-layers approach in Public Safety domain

Research has not proven yet that DSM can satisfy the public safety requirements listed above. Further investigation is needed in this field. To date, the applicability of Dynamic Spectrum Allocation to Public Safety communications with their specific requirements regarding availability, access time, reliability, etc. has not yet been sufficiently verified. Some technical obstacles, like e.g. the hidden node problem, still have to be overcome.

Therefore, it is likely that, in an evolutionary approach, cognitive radio concepts will initially be used for other, less complex functions like for example Public Safety coverage enhancements.

A preliminary proposal for the application of CR and DSM to Public Safety could be based on two layers approach.

- A static allocation of the spectrum is used for basic services like voice and low data rate communication and messaging.
- A dynamic allocation of the spectrum is used instead to provide broadband connectivity. Dynamic spectrum allocation can be based on the concept of spectrum sharing with commercial providers. In case of emergency.



**Fixed Spectrum Management**

**Basic Services:**

- Voice
- Low data rate for critical messaging services
- Security services

**Dynamic Spectrum Management**

**Extended Services:**

- High Data Rate for data and video
- High Data Rate messaging services

**Figure 3: Two layers approach for spectrum management in Public Safety**

Dynamic spectrum allocation can be based on the concept of spectrum sharing with commercial providers. In case of emergency, commercial providers will shut down their communication systems and free their spectrum bands. Public Safety RRS nodes will be able communicate and transmit in these spectrum bands for the duration of the emergency crisis.

There are a number of issues with this approach:

- Some public safety organizations may consider basic services event high data messaging services, as they would be essential for their activities.
- Who will guarantee that commercial providers will promptly shut down their networks in case of emergency? The risk is that some commercial providers will still transmit in the shared spectrum bands and they will create interference to RRS public safety communication systems.
- Emergency telecommunications as described in the TRs produced by ETSI EMTEL (see clause 4.1.4), shows that commercial networks are still needed in case of emergency crisis to alert the population through broadcast communication and messages. Commercial networks like GSM/UMTS are also used by volunteer organizations.
- Ad-hoc Cognitive radio networks do still present a number of technical challenges to be resolved to validate the requirements of reliability and time described in TR 102 745 [i.29].

### 6.4.3 Architectures for Dynamic Spectrum Management

The following architectures provide the alternatives for the design of DSM in the public safety domain.

Each architecture will be compared to the functional architecture and interfaces described in clause 6.3.

This clause reuse some of the concepts described in TR 102 683 [i.24] Cognitive Pilot Channel (see clause 6.2).

In the final clause each architecture is compared against the requirements defined in TR 102 745 [i.29].

### 6.4.3.1 Centralized architecture, Out-of-band channel

In this architecture, a single Cognitive Control Manager (CCM) is used to define the spectrum bands, which are used by the base stations and terminals in the network. CCM is responsible for sending the cognitive control messages to the base stations in the cognitive radio network.

Figure 4 describes this architecture.

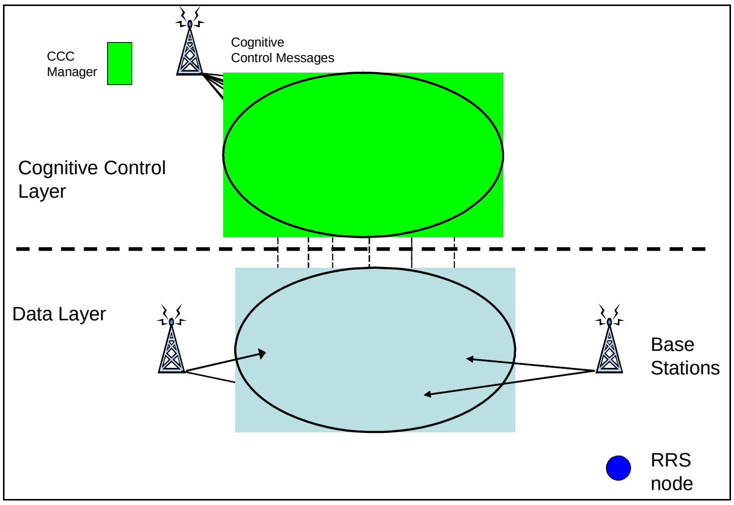


**Figure 4: Centralized Out-of-band architecture**

An Out-of-band channel is used for the distribution of cognitive control messages.

For a specific scenario, the allocation of the spectrum bands can be set on:

1) a predefined assignment agreed among public safety organizations regulators and eventually commercial operators;

2) the knowledge of the policies for the spectrum assignment;

3) the knowledge on the current spectrum assignments in the area;

4) the knowledge on the current licensed non-RRS networks or services present in the area.

In cases 3 and 4, the Cognitive Pilot Channel (CPC) is bidirectional and it can be used by RRS nodes to "sense" the spectrum usage in the area and provide the feedback information to the CCM.

In this architecture, RRS nodes cannot arbitrarily decide the usage of the spectrum by they should conform to the messages received by the CCM through the CPC unless these are against spectrum policies already defined (see clause 6.5).

Case 4 described above is included to avoid the generation of non-RRS wireless interference with licensed non-RRS networks operating in the scenario.

Licensed non-RRS public safety networks can be:

- non-RRS public safety networks (like Analog PMR);
- non-RRS commercial networks, which are still operating during the scenario. For example to broadcast emergency messages to the people;
- military networks.

In this architecture, the RRS nodes (like terminals or base stations) will adopt the following operational procedure (similar to what is described in TR 102 683 [i.24]):

1) CCM transmits the information on the available spectrum bands through the CPC to all RRS nodes (PSCD, MTSS, RRS IAN WACS, RRS JAN WACS) in the area.

2) RRS nodes detects CPC.

3) the RRS nodes receive the information on the available spectrum bands through the CPC. The information received is checked (see clause 6).

4) RRS nodes start to communicate with other RRS and non-RRS networks in the area.

5) If the CPC is bidirectional, RRS nodes perform spectrum sensing in the area and provide feedback information to the CCM through the CPC.

6) On the basis of the received information, CCM may update the information on available spectrum bands.

Figure 5 provides a description of this architecture in relation to the overall functional architecture and interfaces described in clause 6.3.

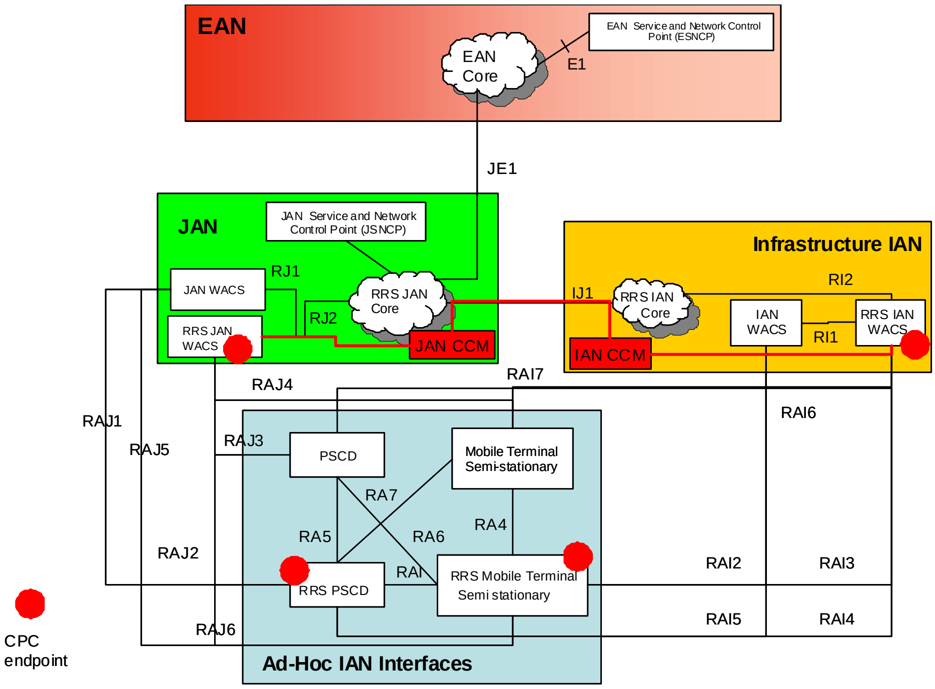


**Figure 5: CCM and CPC endpoints**

The main CCM is at JAN level. If there are IANs in the operational scenario, each IAN has a specific CCM, which is subordinate to the JAN CCM. In this architecture, an EAN CCM is not included, because EAN can span very large geographical areas and it would be difficult to organize a complete spectrum allocation.

The CPC endpoints are located at all RRS nodes (PSCD, MTSS, JAN WACS and IAN WACS). The CPC endpoint at RRS IAN WACS is connected to the IAN CCM through the RI2 interface. The CPC endpoint at RRS JAN WACS is connected to the JAN CCM through the RJ2 interface.

IAN CCM are connected to the JAN CCM through the IJ1 interface.

CPC is included in the definition of all the air-interfaces among RRS nodes: RA1, RAI3, RAI4, RAJ2 and RAJ6.

Only the data layer and the cognitive control layer are presented in this clause. Other layers (management layer or security layer) may also be present.

This architecture has the benefit of simplifying the cognitive radio network development and deployment but it has the disadvantage of introducing a single point of failure represented by the CCM. Furthermore the CCM can become a bottleneck from a performance point of view.

In this architecture, an Out-of-Band CPC is used. The design of the Out-of-band CPC should take in consideration the requirements of resilience defined in TR 102 745 [i.29].

For example, Out-of-band CPC could use more than one frequency band to increase the resistance to jamming attacks.

An issue is the definition of a spectrum band by regulators for Out-of-band CPC. The identified band should be harmonized across all the European countries.

The amount of data exchanged on the CPC is proportional to the dynamicity of operational scenario and the amount of users, but in this centralized architecture, it should be relatively small. Therefore, the CPC frequency band can be relatively narrow.

The estimate of the maximum amount of traffic in public safety operational scenario should be one of the activities of a standardization effort for the definition of CPC.

A variation of the centralized architecture is the hierarchical architecture where a large network or operational context is divided in clusters. For example a large JAN can be divided in smaller JANs or IANs. This architecture provides the benefit of decreasing the amount of CPC data to be exchanged in the network.

### 6.4.3.2 Centralized architecture, In-band channel

As in the previous architecture, a single Cognitive Control Manager (CCM) is used to define the spectrum bands, which are used by the base stations and terminals in the network. CCM is responsible for sending the cognitive control messages to the base stations in the cognitive radio network.

In this architecture, an in-band channel is used. In the in-band solution, the CPC is implemented using specific channels of an existing radio access technology. The in-band CPC can provide both downlink as well as uplink information transfer.

Because of the wide deployment of TETRA communication networks in public safety domain, the most logical solution is that CPC is implemented using a TETRA data channel. Where TETRA networks are not available, other digital PMR could be used like TETRAPOL or APCO 25.

The benefit in comparison to the previous architecture is that no additional channel and spectrum allocation is needed. On the other side, an additional interface are defined and implemented between RRS and TETRA networks.

Figure 6 describes this architecture.

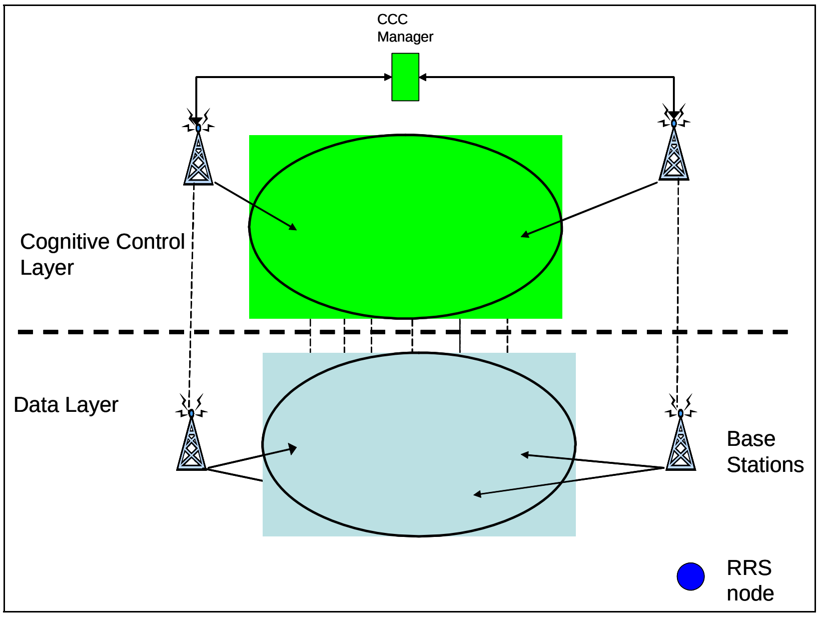


**Figure 6: Centralized In-band architecture**

The base stations in figures 7 and 8 can be TETRA base stations or RRS base stations, which are conformant to TETRA standard to implement the CPC through TETRA.

Most of the considerations, which have been presented in clause 6.4.3.2, can also be applied to this architecture, including the allocation of spectrum bands and operational procedure.

The representation of this architecture in relation to the overall functional architecture and interfaces described in clause 6.3 is slightly different from what is presented in clause 6.4.3.2.

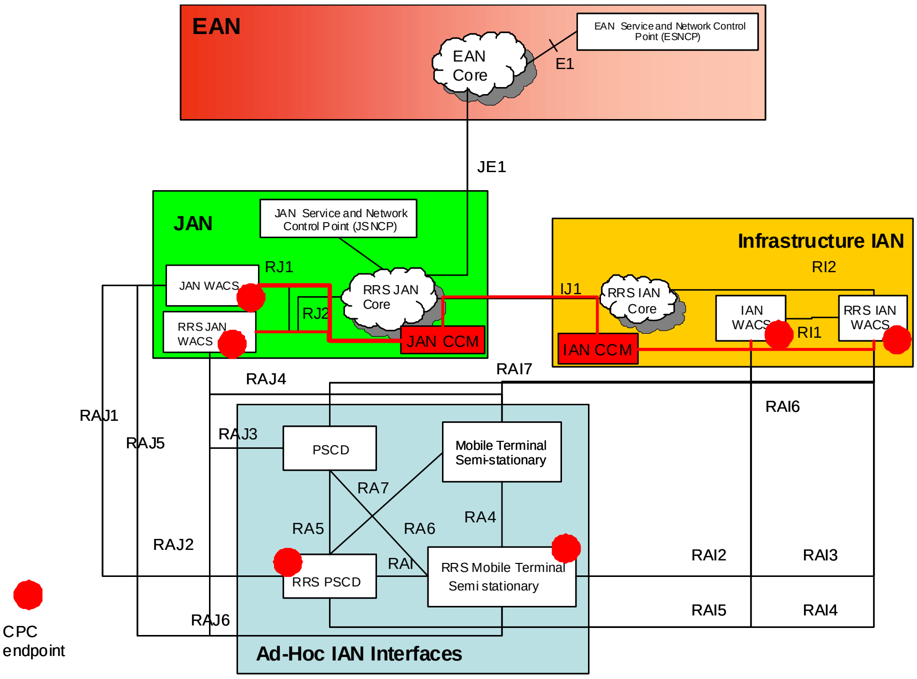


**Figure 7: CCM and CPC endpoints**

The main CCM is at JAN level. If there are IANs in the operational scenario, each IAN has a specific CCM, which is subordinate to the JAN CCM. In this architecture, an EAN CCM is not included, because EAN can span very large geographical areas and it would be difficult to organize a complete spectrum allocation.

The CPC endpoints are located at all RRS nodes (PSCD, MTSS, JAN WACS and IAN WACS) but also at the non-RRS base stations (JAN WACS and IAN WACS) which are used to transmit the CPC data The CPC endpoint at RRS IAN WACS is connected to the IAN CCM through the RI2 interface. The CPC endpoint at non-RRS IAN WACS is connected to the non-RRS IAN CCM through the RI1 interface. The CPC endpoint at RRS JAN WACS is connected to the JAN CCM through the RJ2 interface. The CPC endpoint at RRS JAN WACS is connected to the JAN CCM through the RJ1 interface.

IAN CCM are connected to the JAN CCM through the IJ1 interface.

CPC is included in the definition of all the air-interfaces among RRS nodes and non-RRS base stations: RA1, RAI2, RAI3, RAI4, RAI5, RAJ1, RAJ2, RAJ5 and RAJ6.

The implementation of the In-band CPC should not require modification of the non-RRS terminals or other non-RRS base stations which are not used to carry the CPC channel. CPC deployment should only require minimal modifications to RRS terminals and base stations. This is one issue to be investigated and resolved with TETRA standardization organization (or other digital PMR organizations bodies like TETRAPOL or APCO25).

Only the data layer and the cognitive control layer are presented in this clause. Other layers (management layer or security layer) may also be present.

### 6.4.3.3 De-centralized architecture

In this architecture, there is no single Cognitive Control Manager (CCM). Each node is responsible for sending the cognitive control messages and defining the best spectrum management policy. An In-band channel (for example a TETRA data channel) or out-of-band channel can be used.

This architecture gives more freedom to define and deploy the cognitive radio network. It is not dependent on an existing base stations infrastructure.

The architecture is based on cooperative (or collaborative) behaviour where each RRS node considers the effect of the node's communication on other nodes. In other words, the spectrum measurements of each node are shared among other nodes.

This type of architecture can be used when an existing network infrastructure is missing and only ad-hoc IAN can be established. This is the typical case of the Natural Disaster described in TR 102 745 [i.29].

A de-centralized architecture present numerous challenges in comparison to the centralized architectures presented in clauses 6.4.3.1 and 6.4.3.2:

- A de-centralized architecture converges very slowly in comparison to a centralized architecture to identify the correct allocation of spectrum bands. As a consequence, this architecture may not validate the timing requirements defined in TR 102 745 [i.29].
- This architecture may present "hidden node" problem, where an RRS node (node A) may not be able to detect the emission from another RRS node (node B) because their mutual distance is too great for the sensitivity of the node A. The consequence is that node A may start transmission with a power level, with will create harmful interference to node B. Cooperative sensing among RRS nodes may be able to mitigate this problem but cooperative algorithms may be slow to converge and the degradation of the transmission may not be considered acceptable by Public Safety organizations.
- RRS nodes, which have a primary function in maintaining the cognitive networks, may lose connectivity with the rest of the network if a natural or man-made obstacle is present.
- The complexity of the design and implementation of RRS nodes may increase their price in comparison to the centralized architecture.

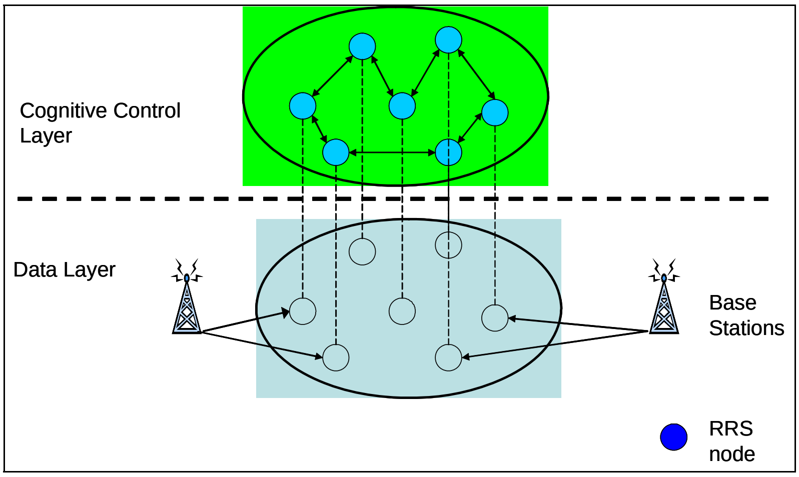


**Figure 8: De-Centralized architecture**

Figure 9 provides a representation of the de-centralized architecture in relation to the overall functional architecture and interfaces described in clause 6.3.

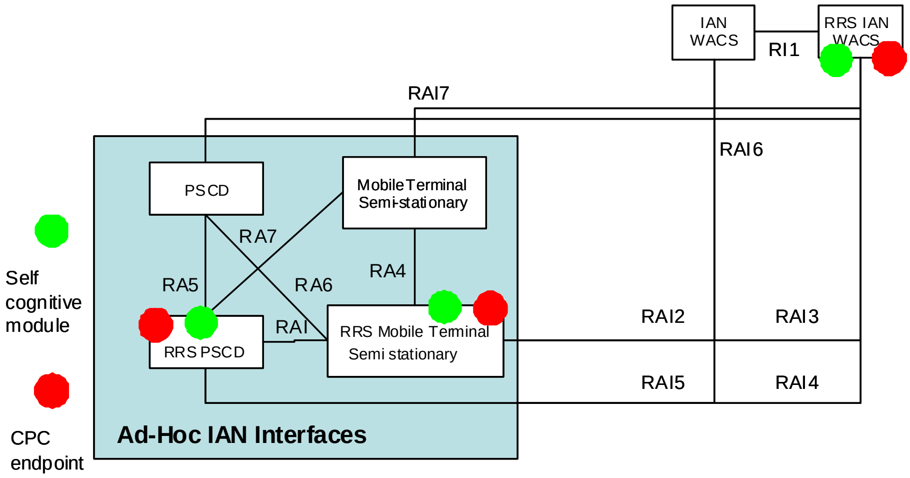


**Figure 9: SCM and CPC endpoints**

In this architecture RRS nodes have a Self Cognitive Module (SCM), which is responsible for:

- The knowledge of the current available spectrum bands, as part of the "spectrum sensing" capability.
- Decide what is the best allocation of spectrum bands on the basis of the cognitive control messages received from other RRS nodes through the CPC.
- Implement spectrum policies relevant to the area of operation and the operational context.

The CPC endpoints are still needed to transmit the cognitive control messages across the network.

#### 6.4.3.4 Evaluation of DSM architectures against requirements

This clause provides considerations on the architectures presented in the previous clauses against the requirements identified in TR 102 745 [i.29].

**Table 3**

| | Centralized architecture, Out-of-band channel | Centralized architecture, In-band channel | De-centralized |
|---|---|---|---|
| **Interoperability** | RRS should be aware of the spectrum allocation and usage of other Radio Access Technologies (RAT) in the area. | RRS should be aware of the spectrum allocation and usage of other radio access technologies in the area. Interfaces should be defined with the RAT used for In-band channel. | RRS should be aware of the spectrum allocation and usage of other radio access technologies in the area. Because a fixed infrastructure is not present, this task can be difficult to achieve. |
| **Spectrum Usage** | A centralized architecture with a bi-directional CPC can satisfy the requirements with a relatively simple design.<br>A harmonized spectrum band for Out-of-band CPC may be difficult to define at regulatory level. | A centralized architecture with a bi-directional CPC can satisfy the requirements with a relatively simple design. | A de-centralized architecture presents a number of challenges to satisfy the requirements (see clause 6.4.3.3). |
| **Security** | It is easier to implement network security with a centralized architecture. The out-of-band CPC can be vulnerable to jamming or other security attacks. | It is easier to implement network security with a centralized architecture. An in-band CPC can reuse the security mechanism already defined in the RAT (e.g. TETRA). | Network security protection usually needs a central entity (e.g. certification authority), which may be difficult to implement in this architecture. |
| **Resilience** | A centralized architecture is more resilient against internal failure or external attacks. | A centralized architecture is more resilient against internal failure or external attacks. | A de-centralized architecture has significant challenges to provide the needed resilience. |
| **Scalability** | A centralized architecture may be less flexible to support scalability. A hierarchical centralized architecture could be used for large networks. | A centralized architecture may be less flexible to support scalability. A hierarchical centralized architecture could be used for large networks. | The algorithms for the allocation of spectrum bands can take a long time to converge. |
| **Resource Management** | A centralized architecture can satisfy resource management requirements like prioritization or timing constraints in a better way than a de-centralized architecture. | A centralized architecture can satisfy resource management requirements like prioritization or timing constraints in a better way than a de-centralized architecture. | A de-centralized architecture can satisfy resource management requirements like self configuration and self optimization but prioritization or timing constraints could be difficult to validate. |
| **Operational support and Usability** | A centralized architecture is more aligned with the organizational structures of public safety organizations. | A centralized architecture is more aligned with the organizational structures of public safety organizations. | A de-centralized architecture could be more appropriate when the fixed infrastructure is destroyed or degraded. |

### 6.4.4 Modelling and simulation of Cognitive Wireless networks in Public Safety

As described in the previous clauses, there are a number of different approaches and design alternatives to implement a cognitive wireless network.

The purpose of this clause is to present the various design alternatives and to describe models to evaluate their performance against metrics defined by the Public Safety requirements.

Following is a view of the adopted methodology.

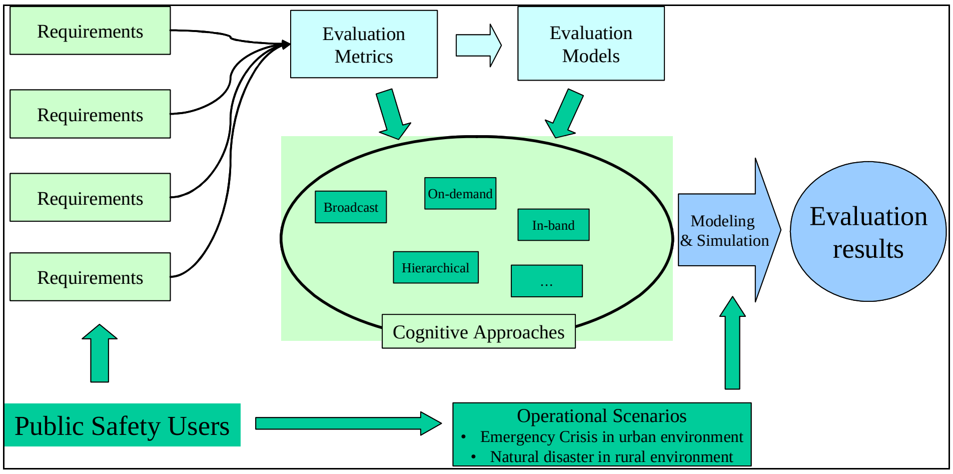


**Figure 10: Methodology for modelling and evaluation of cognitive approaches in Public Safety**

From TR 102 745 [i.29], User Requirements, the requirements are defined and extracted. The requirements will be used to define the metrics by which, the performance of the cognitive wireless systems will be evaluated.

The following metrics have been identified:

- Connection Setup Time.
- Timeliness of the cognitive control messages.
- Minimization of the dropped connections.
- Robustness against external interferences or security attacks.
- Data throughput in relation to the number of users.
- Power Consumption.
- Implementation complexity.
- Coverage.
- Ability to manage hidden nodes.

An activity of standardization could use models based on the architectures presented in clause 6.4.3 to evaluate the best design solutions for Dynamic Spectrum Management in Public Safety against the operational scenarios identified in TR 102 745 [i.29].

## 6.5 Security

As described in TR 102 745 [i.29], Public Safety domain has a unique set of requirements for wireless communications in comparison to the consumer domain.

In comparison to the consumer domain, Public Safety has more severe security requirements. Public Safety ICT systems store critical information on people and assets to be protected. The safety of the human beings is dependent on the security and performance of wireless communications, which guarantee integrity of the data being transmitted and robustness against security attacks. Security is also an important requirement in the consumer domain, but other drivers like price of the equipment and a uniform set of customers play a more important role.

While Public Safety domain has similar operational requirements to the Defence domain, it also presents unique challenges due to the broader range of participants (fire-fighters, medical support, volunteer organizations, etc.), each with its own set of security requirements.

The activity of research and standardization of RRS security present resolve a broad range of issues, which spans from software assurance, to conformance to spectrum regulations and certification.

As a general rule, communication systems based on RRS technologies should validate the communication security requirements of non-RRS communication systems like Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization. This is a consequence of the general conformance to standards and regulations already defined for the wireless communication systems, with which RRS will interoperate. For example, communication systems based on RRS technologies could support the type 1 security requirements defined in the TETRA standard.

As a consequence, a network based on RRS should provide the following categories of security services:

**Registration, Authentication and Authorization Services**

- Registration: The process by which the users and their devices are provided with a credential (e.g. an identity such as a user name or certificate) to use for subsequent authentication. During registration the potential user will be required to supply proof of his "real world identity".
- Authentication: The process by which the electronic identity of the user (as represented by the credential obtained in the registration process) is validated by the system.

EXAMPLE 1: Authentication checks (e.g. by means of a password or biometric or digital certificate, etc.) that the user of the virtual identity is the true owner of the credential supplied in the registration process.

- Authorization and Access Control: Authorization is the granting of rights to use the service. Access control is the process by which only Authorized users may use the service and to control under what conditions access can occur. Access control also includes accounting for the use of the service.

**Data Confidentiality and Privacy**

- "Confidentiality" is aimed at preventing the disclosure of sensitive information to individuals not authorized to see it normally in accordance with national security laws.
- "Privacy" is aimed at preventing the disclosure of the private data of an individual (e.g. medical or financial) in accordance with data protection legislation.

In general the measures adopted to address confidentiality and privacy concerns are similar.

**Trust Services**

- Data Integrity: The aim of Data Integrity is to provide proof that the content of an electronic communication received by the recipient is identical with that sent by the originator and has not been modified deliberately or accidentally en route. (Note I do not think you can *prevent* modification, you can only detect that it has occurred between the originator and the recipient).
- Non Repudiation: The aim of non-repudiation is to provide proof that the originator created and sent a communication and that the recipient received and read the content of the communication.

**Availability**

- Service Availability: The aim of service availability is to ensure that access to the applications and wireless network infrastructure is available and usable by authorized users.
- Information Availability: The aim of Information Availability is to ensure that access to the information carried by the wireless network is available to those users authorized to see the information.

All these services are implemented/supported by security measures in the wireless communication system.

Security measures include:

- Key generation, Key management and Key distribution including Over the Air (OTAR).
- End-to-end encryption across network boundaries.
- Digital signatures.

- Audit.
- Support for multiple encryption algorithms.
- Data Management.

Beyond the support and validation of generic communication security requirements, RRS-based networks present specific challenges.

The ability of RRS to reconfigure radio functionality through software instead of hardware can offer various benefits but it can also introduce new security problems in comparison to conventional radio systems.

RRS terminals or base stations could theoretically be able to download new configuration profiles or software modules from the air interface or from a direct link (in case of base stations). The new profile or software module can be used to set transmission parameters like frequency, power and modulation types or even implement a communication standard (i.e. waveform). This functionality is not completely new as the "software download" functionality has been present in cellular networks (like GSM) for a long time, enabling the replacement or upgrade of software modules in base stations. In the case of conventional (non-RRS) systems, the change of the software had a limited impact because the hardware architecture was always the same. In case of RRS systems, this functionality is much more powerful as many of the traditional communication functionalities are implemented in software and they can be changed more easily.

As a consequence, an attacker can download a malicious software module or profile to an RRS terminal to alter dramatically its transmission behaviour and provoke harmful interference to the communication systems (RRS or non-RRS) present in the area or implement other security attacks like eavesdropping and spoofing.

Another difference with non-RRS systems is the mechanism for software download. In non-RRS systems, the links (wireless or wireline) to base stations are defined and they can be controlled. The terminal firmware can be changed only in a controlled way.

RRS nodes can download the software through the same air interface used to communicate. As a consequence, an attacker can download a malicious software module or profile to all the RRS terminals in the coverage area. In this sense, RRS can be vulnerable to the same type of attacks of personal computers connected to the Internet including virus, worms and other Malware, with the effect that malicious software can propagate more easily.

To ensure a secure and reliable software download, the following issues are identified:

- Who guarantees that the downloaded profile or software module comes from a trusted source and can be activated on the RRS terminal?
- Who guarantees that the downloaded profile or software module will behave as expected?

To resolve these, issues, RRSs should be designed with similar mechanisms to the ones adopted to guarantee Software Assurance in Information Technology.

Software Assurance for RRS requires:

- A secure download mechanism, which guarantees the authenticity of the downloaded software.
- RRS components, which are capable to verify the trustworthiness of the downloaded software.
- A secure execution environment in the RRS to guarantee that only trusted software can be activated and executed.
- A RRS component to ensure that spectrum regulations will be validated regardless of the software modules running on the RRS terminal.
- An overall certification processes to guarantee that the software modules to be downloaded and activated will behave as expected.
- An overall security process with certification authority and other entities.

An essential phase in the standardization effort for RRS is to adapt software assurance techniques and best practices to RRS technology.

Another area where security is a paramount importance is the use of RRS as an enabler of cognitive radio networks. Non-RRS communication systems can only change their transmission parameters and use the RF spectrum bands in the limits, which have been defined by predefined standards and spectrum regulations. These limits are implemented in their hardware and firmware architecture and they cannot be changed at runtime. On the other side, a RRS does not have this limit as it is theoretically designed to communicate in a wide range of spectrum bands and with the capability to change its transmission parameters at runtime.

Cognitive radio networks can implement innovative approaches to spectrum management like Dynamic Spectrum Management (DSM), where the allocation of spectrum bands to communication services can change in time or space. Cognitive radio networks can present security challenges as well. A cognitive radio, which has been taken over by an attacker, can break the DSM mechanism by implementing spectrum mis-usage or a selfish behaviour.

EXAMPLE 2: It can transmit in not-assigned bands or it can ignore the cognitive messages sent by the other elements of the cognitive radio network.

EXAMPLE 3: The Byzantine threat, where a cognitive radio node may use his privileges to implement misuse of the network or malicious behaviour is a likely threat in cognitive radio networks based on a distributed architecture

A security analysis of cognitive radio networks could address, at least, the following issues:

- What are the potential threats to cognitive radio networks ? Threats of non-cognitive radio networks may be different or non existing in cognitive radio networks, while new threats may be identified. What is the likelihood of these threats ?

- What type of attacks could be implemented against cognitive radio networks ? Are attacks already identified in non-cognitive radio networks also valid for cognitive radio networks ? Which new attacks could be implemented against cognitive radio networks ? What are the potential consequences of these attacks ?

Once that threats and attacks are identified, mitigation solutions could be designed to counter such attacks.

Cognitive radio networks are likely to be based on exchange of information on the radio spectrum environment, the capabilities of the participating cognitive radio nodes and networks and the available spectrum bands to be used. The exchange of information is needed to construct a common understanding and agreement on the available spectrum resources. Such exchange of information (e.g. cognitive control messages) is one area where threats and attacks are possible.

Malicious attackers can insert false information to influence the common understanding of the cognitive radio network for their own advantage (e.g. allocation of wider spectrum bands) or just to undermine the reliability of the network. Security solution are likely to be based on the authentication of the source and the content of the exchanged information. The cognitive radio network needs assurance that the cognitive control message are indeed from trusted cognitive radio nodes and that their content has not been altered.

There are similarities between this area and research activity to ensure secure exchanges of information in mobile ad-hoc networks. Security solutions designed for mobile ad-hoc networks could be adapted to cognitive radio networks, especially in relation to the de-centralized cognitive radio network architectures described in clause 6.4.3.3.

A specific research area is related to the security analysis of cognitive radio networks based on a Cognitive Pilot Channel (see clause 6.2), which is responsible for distributing the cognitive control messages to coordinate the overall cognitive network. The Cognitive Pilot Channel (CPC) can become a vulnerability point by attacks like Denial of Service (through jamming) or through traffic overload. A malicious cognitive node can transmit in the same frequency of the CPC or can overload the channel by sending a large number of cognitive control messages. These types of Denial of Service (DoS) attacks have already been analyzed in wireless telecommunications and adequate solutions could be defined. Overflow of cognitive control messages can be controlled through algorithms implemented in the cognitive radio nodes to analyze repetition of cognitive control messages, while jamming of CPC can be mitigated by selecting a number of potential CPC bands.

As in the case of secure download and software assurance, protection and mitigation techniques can be applied to increase the robustness of CPC or to ensure that cognitive radio networks based on RRS respect the Dynamic Spectrum Management rules of conduct.

The implementation of such solutions are absolutely necessary if we want to guarantee the same level of security provided by non-RRS public safety communication systems like TETRA. While in the commercial domain, security solutions could be adopted through a gradual approach, in other application domains, security solutions are absolutely necessary from day one. The design and deployment of mitigation solutions to ensure security should consider the risk of adding complexity to the overall architecture or increase the overall cost of the cognitive radio networks and the related terminals.

The trade-off of the implementation and deployment of security solutions is the additional cost and increased complexity of RRS-based network.

A final consideration is based on the capability of RRS technology to remove or mitigate the interoperability barriers among the organizations involved in emergency crisis or natural disasters. This application of RRS was evaluated in the FP7 EULER and WINTSEC projects (clauses 4.2.4 and 4.2.6). Using the capability of RRS technology to communicate with different RAT (Radio Access Technologies) using the same platform, it is theoretically possible to create interoperable "bridges" across public safety organizations, which use different communication systems.

EXAMPLE 4: A handheld can communicate to TETRA and analog PMR systems. More details on the interoperability capability of RRS are in clause 6.6.

Military and public safety organizations operate with various levels of security. This wide range of entities includes volunteer organizations and citizens from one side (lowest level of security) to military organizations (highest level of security) to the other side of the security spectrum. Wireless communication systems and terminals based on RRS should guarantee interoperability without sacrificing the security of data in each network. This is the concept of "multi-level" security where the RRS-based networks can provide various levels of security across the network and on the RRS nodes.

The implementation and deployment of "multi-level" security presents even more challenges than the software assurance solutions presented before. The cost impact could be quite high for a public safety organization.

Figure 11 has the purpose to provide a simplified overview of the potential implementation of a secure RRS network, with a description of the main components.

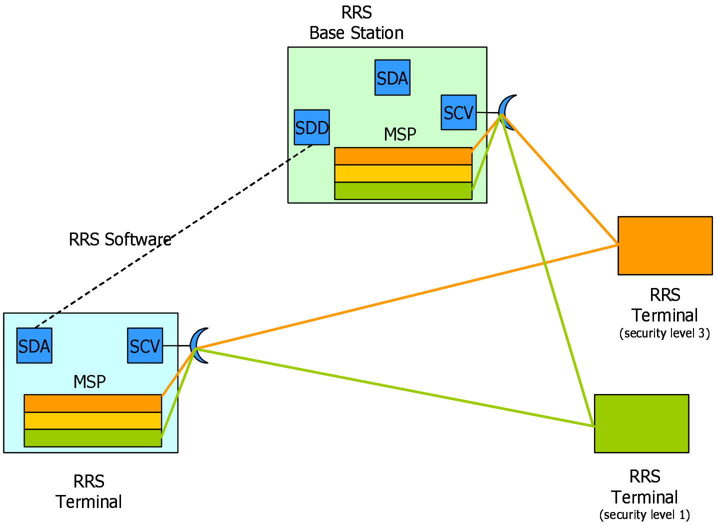


**Figure 11: Security elements**

The following components are present:

1) SDA is the Software Download Authentication (SDA), which has the tasks to:

- guarantee the security of the link used to download the RRS software from a trusted source;
- validate and verify the received RRS software;
- verify the execution of the activated RRS software.

2) SDD is the Software Download Distributor (SDD), which has the task to:

- manage the different releases of trusted RRS software to be distributed;
- guarantee the security of the link used to distribute the RRS software;
- ensure that the RRS software is distributed to the trusted target.

3) SCV is the Spectrum Conformance Validator (SCV), which has the task to ensure the conformance to spectrum regulations for the software waveform activated on the RRS platform (terminal or base station).

4) MSP is the Multilevel Security Path controller to provide different communication paths for each level of security.

## 6.6 Interoperability

As described in the previous clauses, the Public Safety domain is characterized by a number of heterogeneous networks. Some of these networks have been described in clause 5.

One of potential capabilities offered by RRS is to provide interoperability among the various systems.

The European FP6 WINTSEC project (described in clause 4.2.6) has the main objective to investigate the use of RRS (called SDR in the project) to remove the interoperability barriers in the public safety domain.

RRS can act as a bridge at the points in the network:

- At the level of the network infrastructure as a gateway among two or more network interfaces.
- At the level of base stations to create a bridge among two or more wireless communications systems (standards).
- At the level of user terminal, which provide an interface to one or more wireless communication systems (standards)?

Figure 12 describes the possible options.

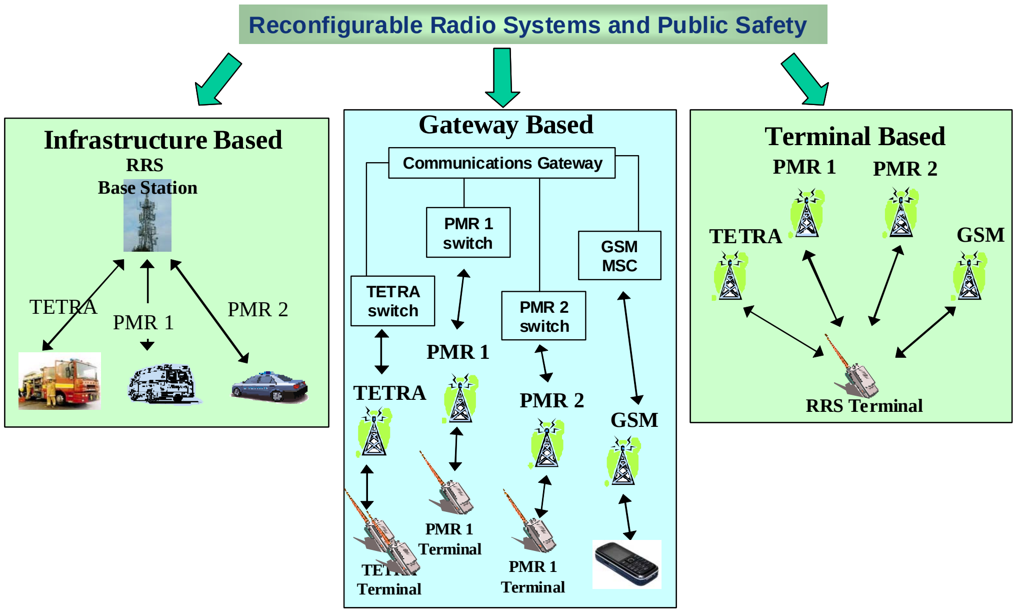


**Figure 12: Use of RRS to mitigate technical interoperability barriers in Public Safety**

NOTE: The interoperability barriers described in this clause are only at the technical level. Interoperability barriers at organizations and processes level are not considered in this clause even if they are equally important.

Each solution has its own advantages or disadvantages:

- The RRS terminal based solutions would require a more complex architecture of the terminal to support a number of different air interfaces. This would increase the cost of the terminal. On the other side, the technology is mature as multi-mode public safety radios have been used for several years in the USA, and recently multi-band radios have been introduced as well (see [i.18]). There is also concern on the increase power consumption, which will have an impact on the life of the batteries. Considering the number of terminals used by Public Safety users, this solution may not be feasible for hand-held terminals. Terminal based solutions could be adopted for vehicular terminal, where the cost of the equipment is less meaningful. A typical Public Safety vehicle like a police or fire-fighter vehicles cost in excess of 60 000 Euro, so more sophisticated and costly vehicular terminals will not have a significant impact on the budget of a Public Safety organization. A topic for standardization could be the definition of the internal architecture and interfaces of a vehicular terminal. This approach has the risk of creating strong constraints on the implementation by the various manufacturers.

- The base station solution would have a minor economic impact on the upgrade of the Public Safety network infrastructure in comparison to the terminal based solution. On the other side, RRS base stations will be more expensive than non-RRS base stations as multi-mode/multi-frequencies base stations do operate simultaneously on all modes and frequencies. A technically more challenging situation than with a terminal, which only needs to operate on one at a time. Because emergency crisis are usually unexpected, it would be difficult to design the base stations with all the needed air interfaces standards. The capability of downloading in real-time the needed waveforms could become an important asset in this context. A specific aspect of Public Safety communications is that base stations are often designed to be transportable by a vehicle in the area of emergency crisis.

- The gateway based is the most cost effective solution as the impact on the existing infrastructures is minimized in comparison to the previous approaches. The disadvantage is the impact of the responsiveness of the systems and a minor level of reconfigurability in comparison to the previous approaches. The definition of the gateway interfaces among the types of wireless communication system used by the Public Safety described in clause 5, could be a topic for standardization.

Each solution is also related to the type of Public Safety scenarios where the solution could be applied.

An important area to evaluate is the sharing of networks resource with commercial networks like the ones described in clause 5. Apart from spectrum sharing already described in clause 6.4, "network sharing" could be also a solution to provide additional capability to public safety responders during an emergency crisis.

Public Safety organizations use commercial networks when public safety networks are not available because of the consequences of the natural disasters or because they operate in remote areas like in Search and Rescue operations. The use of commercial networks is also evident from the results of the questionnaire presented in TR 102 745 [i.29].

As described in clause 5.3, commercial networks are also evaluated by Public Safety organizations to have access to broadband connectivity.

The use of commercial networks by Public Safety organizations and sharing of network resources has the following challenges:

- Commercial networks are not designed on the basis of public safety requirements.

- Telecom providers have done large investments in the implementation and deployment of commercial networks and they would be resistant to hand over the control of such networks to public safety organizations during a long emergency crisis or natural disaster.

- In case of a natural disaster, the commercial networks could be seriously degraded or destroyed. Usually only the operators of the commercial networks have the knowledge to restore the network to an operating status.

- Commercial networks are also used for emergency broadcast communication to the population in case of a natural disaster (see deliverables of ETSI EMTEL, clause 4.1.4).

- Sharing of network resources or "network sharing" among public safety and commercial networks can be quite complex. Standards and technologies like gateways are still be defined for shared resource management.

- Commercial networks are usually sized up to specific amount of traffic capacity and number of users. In emergency crisis, panic conditions may increase the amount of traffic to be carried by the network.

- Commercial networks need prioritization access mechanism to ensure that public safety organization have dedicated resources.

The 3GPP standardization body has defined a Priority service for Circuit Switched (CS) in Release-6 through the TR 122 950 [i.21], Priority service feasibility study and the TR 122 952 [i.30], Priority service guide. In Release-7, a similar work has been done for multimedia services like VoIP, video, Push-to-Talk, email, instant messaging and file transfer in TR 122 953 [i.31], Multimedia priority service feasibility study and TS 122 153 [i.32], Multimedia priority service requirements.

The recommendation is that the standardization activity for the application of RRS technology to Public Safety domain should consider the TRs described above.

"Network sharing" requires a joint management of radio resources between public safety networks and commercial networks. TR 102 682 [i.25] defines a block called JRRM (Joint Management of radio resources across heterogeneous radio access technologies), which is distributed between the terminal and access network.

A similar block can be defined for joint resource management between public safety networks and commercial networks.

In the centralized architecture described in clause 6.4.3.2, JRRM could be a block of the CCM or related to it as in figure 13.

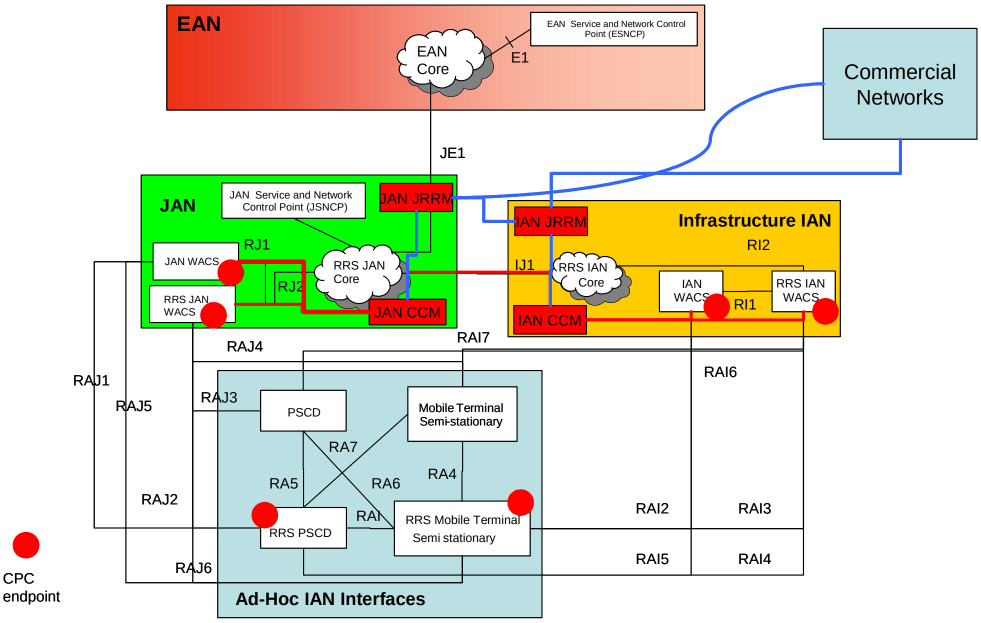


**Figure 13: Joint Resource Management among Public Safety and Commercial networks**

In this architecture, the JRRM blocks at JAN and IAN level are responsible for sharing resources with commercial networks in the area. Each JRRM block coordinates the allocation of resources with the CCM. The IAN JRRM are subordinate to the JAN JRRM. The standardization activity should define the interfaces between JRRM and commercial networks and JRRM/CCM.

# 6.7 Policy Framework

In comparison to the static allocation of the spectrum, Cognitive Radio and Dynamic Spectrum Management may increase the risk for mistakes or instabilities in the use of the spectrum. Spectrum may be allocated in the wrong way or at the wrong time during an operational scenario due to lack of common semantics or a well defined protocol to exchange information.

Public Safety scenarios usually demand a mechanism for expressing and enforcing access control policies for any type of resources. In the case of the spectrum resource, there is a need to define what are the available resources (e.g. transmission/reception bandwidths), what are the parties that are allowed to access them and under what conditions. This is especially true in "spectrum sharing" scenarios where various parties compete for the same spectrum.

Furthermore, DSM introduces many more "degrees of freedom" in comparison to a fixed approach for the spectrum. The deployment of DSM may have a large number of operating dimensions including frequencies, waveforms, power levels, and so forth.

There is the need to define an access control or policy framework, which allows the benefits of DSM while ensuring the conformance to regulatory policies and rules of conduct among Public Safety organizations. The policy framework could be an important tool for regulatory bodies as well to define some basic rules for sharing the spectrum.

The definition of the policy framework is out of scope of this clause, but we can identify some basic features for such framework:

- The presence of a language to describe the policies for spectrum management, including the range of frequency, which can be used, the geographical area or region where the policy applies, the capabilities requested to the cognitive radio device to implement the policy. The language should have simple and unambiguous semantics to be used by regulators to define the rules and behaviour for spectrum emission and transmission. A declarative language is recommended as the objective is to describe "what" are the spectrum policies and constraints and not "how" they could be implemented.

- A mechanism to deploy the agreed policies to the nodes of the cognitive radio networks, which implement DSM. Not only static deployment but also dynamic deployment could be envisaged. In a static deployment, the network nodes receive the policies before they become operational; for example when the terminals are distributed to the public safety officers. In a dynamic deployment, the policies could be changed or distributed during the operational scenario. Obviously a coordination mechanism should be implemented to ensure that all the cognitive network nodes are aligned to the same policies in any moment.

- The capability to describe constraints in the access of spectrum resources on the basis of the context (i.e. operational scenario).

- The extensibility to define new policies or to extend the expressiveness of the language for new application domains.

- Public Safety operational scenarios are characterized by many organizations with different levels of authority and priority in the access to any resource (i.e. energy, water or communications). Generally military have the highest authority, then police and volunteers organizations. The priority depends also on the type of operational scenario. The policy framework should have the capability of describing the different levels of priority in using the spectrum resources on the basis of the type of operational organization and the type of operational scenario.

# 7 Terminal Architecture

## 7.1 Introduction

This clause gives an overview of SDR based terminal architectures which could be defined in the public safety domain. Other terminal architectures for RRS or Software Defined Radio have been defined in other fora like the SDR Forum (see clause 4.1.11) and JTRS program (see [i.19]).

## 7.2 ETSI TC RRS SDR Architecture for Mobile Devices

In TR 102 839 [i.33] SDR Reference Architecture for Mobile Device, is presented a possible architecture for terminals in the commercial domain. Requirements and a reference architecture with the definition of the interface is presented. A terminal architecture defined for the commercial mass market may provide benefits like decreased cost of the equipment and "state of art" technological sophistication. On the other side, public safety requirements may be difficult to validate in a commercial architecture. Further analysis is needed to evaluate the use of the reference architecture defined in TR 102 839 [i.33] for the public safety domain.

## 7.3 Software architecture

Currently, in general wording, Software Defined Radio (SDR) means a radio platform able to provide as far as possible its functions and related reconfiguration by means of SW use. This approach is implemented by SW reprogramming of digital components able to perform signal processing and analog components command and control. With this model, for example a sub-system configuration for a Multi-Band Transmitter could be defined as in figure 14.

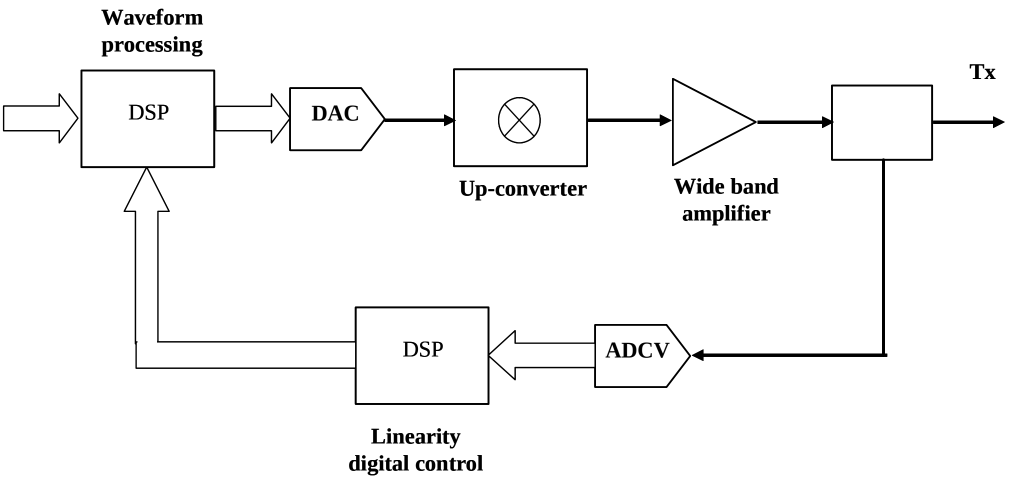


**Figure 14: Digital signal processing for waveform and multi band transmitter**

Here, from now on, the DSP function is for Digital Signal Processing performed by DSP Processor, or General Purpose Processor (GPP) or Field Programmable Gate Array (FPGA). DSP function is shared by:

- signal processing for waveform modulation;
- digital pre-distortion (linearity digital control).

In a legacy solution, then not SDR defined, the HW/SW architecture can be depicted as in figure 15. In this figure is shown the direct management provided by DSP SW.

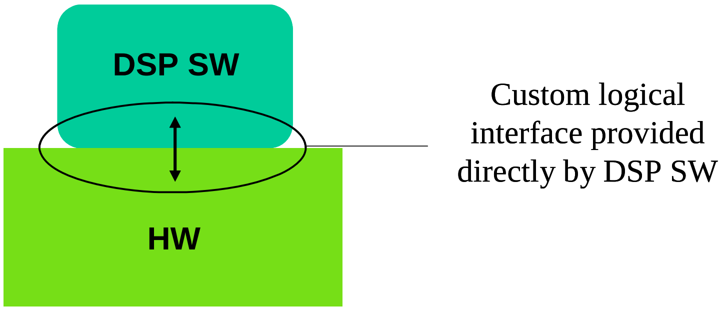


**Figure 15: Legacy terminal architecture**

The use of SW for reconfiguration can be performed at different levels in order to reach different levels of SW portability. Apart from the SW structure which any algorithm can be implemented with, at the minimum the DSP SW should be developed with:

- high level language as C/C++ for DSP or GPP and VHDL for FPGA;
- a specific subset of Application Program Interface (APIs).

The APIs definition is the typical approach to obtain at the minimum the functional set-up communality. As far as the above multiband transmitter application concerns an APIs subset could include for example:

- power amplifier APIs including operations as "modulate envelope", "output power", "operating frequency set-up", "linearization data" and "gain control";
- configuration APIs including operations as "SW install";
- fault management including operations as "Run BIT (Built in Test)" and "get BIT result".

Figure 16 depicts the SW structure based on a common Real Time Operating System (RTOS) at which the DSP SW for waveform and transmitter elaborate on delegates the platform HW access.

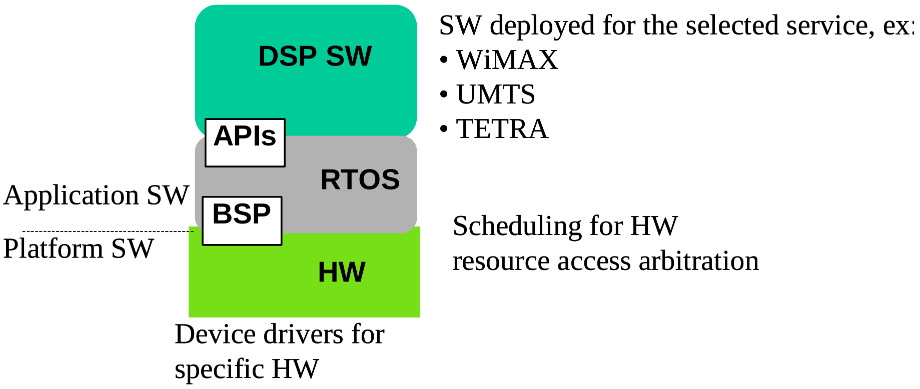


**Figure 16: DSP SW architecture based on RTOS**

The SW architecture depicted in figure 16 is the typical solution applied to integrate SW components in a SDR platform. In addition, by means its APIs subset the SW architecture provides the minimum level of SW application abstraction from the HW or better it provides the level of abstraction from application SW and the specific HW and transport protocol features of the platform. Small RTOS kernel requiring reduced royalties' payment can be the effective solution for current commercial radio communication solution.

The situation for the professional market, that's Public Safety, sees already now the need to update gradually the radio communication capabilities both in term of bandwidth performances and in term of new access technologies. In addition, the life cycle of a public safety radio terminal or base station is at intermediate level between commercial and military applications. It can be appealing both from an operative and economic point of view to propose radios able to be reconfigured and updated by means of new waveforms SW installation. It is probable the reconfiguration will be allowable for base stations so as to make it a cheaper solution to the future access technology insertion need.

The operational need of a lot of professional users in Europe have been developed by means of specific EC funded R and D projects in turn responding to calls defined by Governments level boards like European Security Research Advisory Board (ESRAB). PASR and FPx programs (Framework Program), like WINTSEC, have defined solutions based on reconfigurable radios able to integrate different and heterogeneous access technologies like V/UHF, GSM/UMTS and TETRA aiming to satisfy interoperable need occurring on crisis management. A leading initiative addressing SDR at European level is ESRI/ESRA. ESRIF is an open initiative addressing the European Cross Domains Interoperability challenges. ESRI/ESRA target is:

- Consider "Cross-Domains Interoperability" as a key element for Homeland Security and Peace Keeping operations, based on combined solutions.
- Bring a comprehensive architectural approach integrating Commercial, Public Safety and Military network at "Core Network" level.
- Consider standardized SDR architecture as an essential enabler to achieve the Interoperability goal.
- Leverage and Bridge Industry, National and EC investments on the above topics.

In addition, already now, the FP7 "Future Internet" ICT theme is fostering the development of solutions able to integrate multi access technologies and architecture for seamless ubiquitous broadband services, integrating wired and wireless, fixed and mobile technologies in hybrid access network. The main target of ICT environment is to enable support for service portability and continuity across composite networks through the service-network interface, with ubiquitous access from any network, from any technological and administrative domain, from any location and with a variety of access devices.

All the above considerations make foreseeable next generation terminals and base stations that will have their SW architecture very oriented to reconfiguration and new access technology insertion capabilities. Then a SW architecture with a higher level of SW abstraction with respect the current ones until now applied may be adopted.

Further analysis is needed to define a complete business model for the design of RRS based terminal and base stations in the Public Safety domain.

The following elements should be part of the analysis:

- A business model based on portable SW waveforms could also present the risk of a complex and costly certification process, which is an unavoidable phase in the deployment of wireless communication systems in the Public Safety domain. See clause 8.3.1 for details.
- The technological evolution of terminals in the commercial domain and the promise of reconfigurability could bring important benefits for the lifecycle of public safety equipment, but not at the cost of jeopardizing the conformance to public safety requirements. Furthermore the market size of commercial terminals is one-two orders of magnitude larger than the market size of public safety terminals.
- The business model should include all the stakeholders involved in the deployment of public safety equipment including manufacturers, public safety organizations, regulators, certification bodies and telecom providers.
- The different functionalities and price considerations of handheld terminals, vehicular terminals and base stations should be taken in consideration in the analysis. Vehicular terminals are usually 3 to 4 times more expensive than handheld terminals and they usually have increased capabilities in terms of radio coverage and signal processing.

### 7.3.1 Software Communications Architecture (SCA)

The SW architecture depicted in figure 16 is the typical solution applied to integrate SW component in a SDR platform. Currently the SDR world covers many applications spreading from consumer to private communications and military applications. From this latter environment the need for SW reuse and portability have conveyed to the Software Communications Architecture (SCA) definition that allows the SW reuse by means of extreme abstraction from platform HW. The SCA is depicted in figure 17.

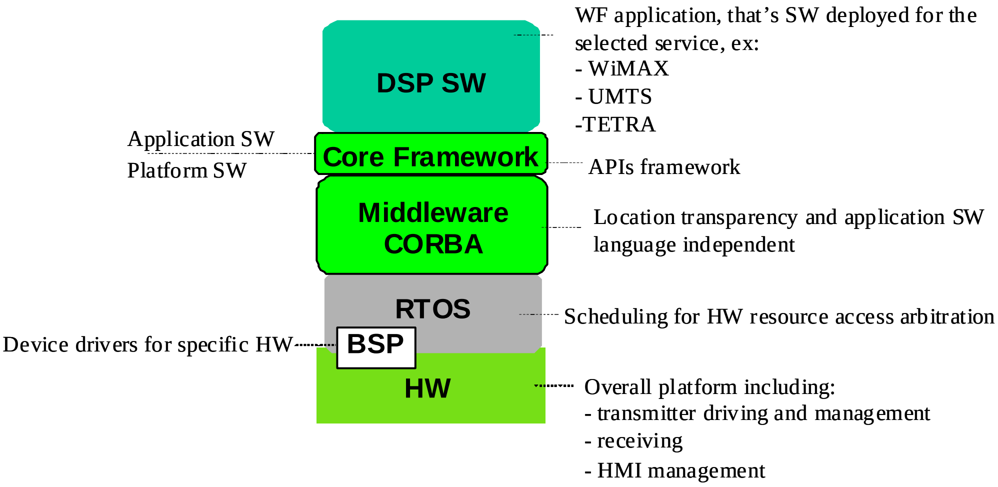

WF application, that's SW deployed for the selected service, ex:
- WiMAX
- UMTS
-TETRA
DSP SW
Application SW
Platform SW
Core Framework
APIs framework
Middleware CORBA
Location transparency and application SW language independent
RTOS
Scheduling for HW resource access arbitration
Device drivers for specific HW
BSP
HW
Overall platform including:
- transmitter driving and management
- receiving
- HMI management

**Figure 17: Software Communications Architecture (SCA)**

The components providing the SW abstraction level of the above architecture are the CORBA middleware and its Interface Definition Language (IDL) defined APIs. The middleware adoption does not require to paying royalties to the current CORBA implementation suppliers. Then, commercial and professional market wireless devices suppliers, currently reject the adoption of a SCA like solution only because don't see today an actual business chance to adopt a new SW architecture requiring additional processing resources in order to overcome the overhead required by the additional CORBA components. However, current technology state of the art is providing DSP devices more and more performance efficient. Nor the rejection is due to new SW development in that the additional SW to include in order to performing CORBA APIs is a very low percentage with respect the DSP SW common to all the above architectures (business logic).

The main lesson learned until now provided is to not concentrate the effort on the complete definition or standardization of a SW architecture. Instead now we should concentrate our effort in order to develop the conditions making cost effective new business model where new access technologies insertion can be provided with reconfigurable radio systems. This also will foster the business of SW waveform and applications for heterogeneous users. The recommendation is to focus the standardization efforts on defining the upper interfaces of the terminal and base station (figure 18) instead of defining the internal interfaces and architecture.

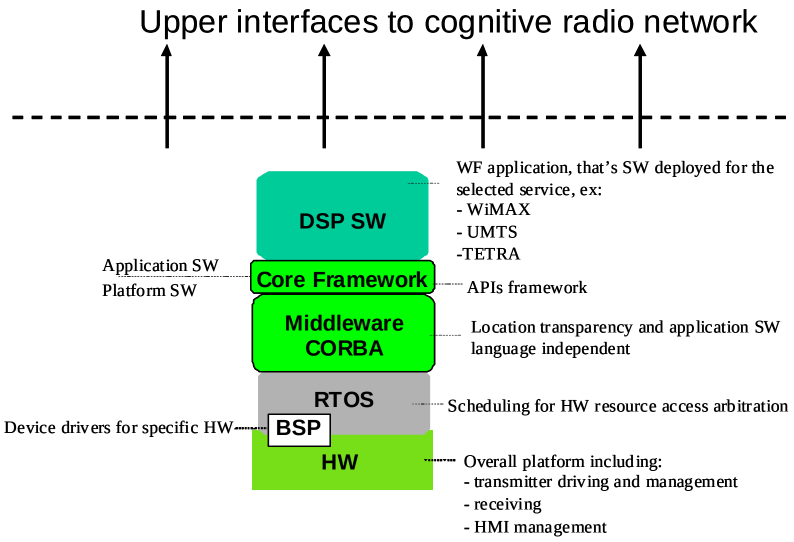

Upper interfaces to cognitive radio network
DSP SW
WF application, that's SW deployed for the selected service, ex:
- WiMAX
- UMTS
-TETRA
Application SW
Platform SW
Core Framework
APIs framework
Middleware CORBA
Location transparency and application SW language independent
RTOS
Scheduling for HW resource access arbitration
Device drivers for specific HW
BSP
HW
Overall platform including:
- transmitter driving and management
- receiving
- HMI management

**Figure 18: Upper interfaces of software defined radio**

## 7.3.2 The European Software Radio Architecture (ESRA)

The WINTSEC (see clause 4.2.6) project conducted an analysis of the European Software Radio Architecture (ESRA) against Public Safety requirements. Deliverable D7.1 of WINTSEC describes the ESRA Framework Core, while deliverable D3.2 provides an analysis and maturity Assessment for ESRA. Deliverable D3.2 provides a compliance matrix against the Public Safety requirements described in deliverable D3.1 of WINTSEC.

The activity of definition and analysis of ESRA framework is still continuing in the FP7 EULER project (see clause 4.2.4) project.

As the ESRA framework is mostly focused on the definition of the architecture of the SDR platform (terminal and base stations), this activity is not strongly related to the present document, which is focused on the system aspects. However, the definition of the external interfaces and behaviour of the RRS platform should be consistent with the System Aspects defined during the standardization phase.

The recommendation is that a future standardization process for the application of RRS to the Public Safety domain should be aligned with the ESRA definition and the activities of the FP7 EULER project.

## 7.4 Conclusions

The previous clauses have given a high level overview of possible SDR-based terminal architecture for Public Safety Domain. Although the Software Communications Architecture (SCA) is the most prominent architecture for Software Defined Radio, it is not yet clear whether or not this architecture is applicable to the Public Safety domain as it was developed for a business case which may be not applicable to the public safety market. References [i.4] and [i.7] provide some guidance on the impact of using the SCA and the benefits it brings. This is also the case for the SDR architecture for mobile devices [i.34] whose applicability to the Public Safety domain requires further investigations due to the different public safety requirements with respect to the commercial ones. As for the ESRA, activities are continuing under the EULER project. As such it is recommended that a future standardization process for the application of RRS to the Public Safety domain should take into account the ESRA definition and the activities of the ongoing FP7 EULER project.

# 8 Investigation on Deployment/Integration/Evolution/Migration from current infrastructures and equipment

## 8.1 Cost considerations (lifecycle/terminal price/software portability/deployment)

In the present document some references are made to software portability meaning the capability a SW radio architecture based RRS should proven so as to allow the integration of third parties' libraries with a limited effort. This aspect is also a matter of internal SW architecture already managed by bodies like SDR Forum and OMG. Instead the present document refers to SW portability in order to investigate trade-off related to cost of the equipments provided both from operational and functional requirements (system aspects) and from other economic topics provided by life cycle and business model considerations.

### 8.1.1 Introduction

The reconfiguration capability of a Radio System, being a terminal or a base station, a handheld or a vehicular version, it sets the system not as the current radio devices tailored for a specific radio communication standard (e.g. TETRA) or for a set of homogenous standards (ex. GMS/UMTS multi band), but it requires the system be able to change network (NET), link (MAC) and physical (PHY) level functionalities so as to adapting to specific operational conditions. The combination of NET-MAC-PHY functions provides the behaviour of the WavefForm (or WF from now on).

Here we refer to "waveform" as the set of SW modules developed in order to be comply with the functionalities specified by a radio communication profile that it can be an official international level standard or however it has to be a common adopted interoperable profile.

The SW modules once installed on the RRS make it able to perform the above functionalities.

The reconfiguration capability requires a waveforms set (operative and functional modes according to a standard) that they can be selected and installed according to operative needs.

An operator already owning a RRS can get later one or more waveforms in order to update the RRS's functionalities so as to be ready for a next forthcoming operative need. In addition, a new waveform can be provided as a consequence of new standard.

The reconfiguration capability is not performed only by new waveforms activation but it performed also by means of the execution of new Policies, that's the rules and parameters set ruling the operational condition. These are for example applied on the network setting:

- Identifying peer radios and determining their connectivity status.
- Authenticating compatible reconfigurable radios.
- Adjusting the network topology.

- Reconfiguring transmission parameters including frequency, transmission rate, etc.

The above rules can be considered as an upper protocol relying on the lower NET/MAC/PHY waveform levels. This protocol could be applied in order to be compliance with national or cross-border policy.

All the above matters have a real connection with all the topics referred by this clause and here listed:

- terminal price;
- deployment;
- software portability and related business model;
- lifecycle.

### 8.1.2 Terminal price

The price of a terminal able to reconfigure its capabilities by means of the activation of new waveforms and policies functionality is constrained by the related technical issues and by the potential features the RRS can offer. The technical issue consists of the additional SW architecture components necessary to perform and manage the reconfiguration itself. The potential features are the system capabilities a RRS offers adapting to different network conditions and policies. In addition, a potential feature is for a customer the chance to be not tied up to the RRS supplier for the following waveform updating. This also raises some business model topics.

### 8.1.3 Deployment

Terminal deployment topic can be faced in the present document referring both operative and functional requirements. The operational need can require deploying for fast response on crisis emergency some terminals able to re-establish radio communications on area hit by natural disaster or terrorist attack. The radio coverage condition can be foreseen but it can change during the emergency so as the terminal has to adapt to the new conditions. Like in military environment, also for Public Safety the operational condition can require a reconfiguration capability of the network based on more terminals and base stations. In addition, the "Network Centric" approach, already known in military side, could be applied on Public Safety in order to allow information transfer in a multi users heterogeneous environment. An example of this approach is a multi access technologies gateway able to manage V/UHF, GSM/UMTS, TETRA and broadband links in order to allow interoperability among Public Safety users like fire department and Policy and monitoring and warning agencies.

Other situation could require a reconfiguration of terminals or base stations already deployed on areas where new services have to be broadcasted. For example for Digital Divide overcome scenario the base stations already deployed for GSM/UMTS coverage could be reconfigured so as to perform additional services like broadband communications and support for Public Users operations.

### 8.1.4 SW Portability and related business model

In Europe some EC and EDA funded programs are working both on a common RRS (or SDR) architecture and on the definition of a common European perspective toward the WF portability (see clause 7.3.2) while the ETSI is working on RRS system functionalities and future standardization.

However, the SW portability is a topic involving all the above bodies because it is closely related to some matters due to the reconfiguration capability. Among these matters, that common ones are the rules set governing the WF libraries definition and documentation and certification and the business model that can be applied to make all that feasible from an economical point of view.

The business of WF portability could derive from the potentials of creating several libraries filled by WFs developed by a large number of companies that will also produce the WF documentation to be shared among the users. Each item in the library has be tested, the expected functionalities verified, it has be certified, with given APIs, etc.

Usually in the military domain the exchange of WFs is based on commercial agreements between different countries, within specific programs launched for instance by the EDA. Indeed, the EDA usually supports the development of WFs that are shared between the involved partners.

Both for military and not the business can be made on the usage of the WF by parties that did not participate in the development but decide to use the WF and purchase them, along with the support for the portability. Once a nation has developed a WF, and once it has been authorized to commercialize it to third parties, it becomes a matter of vendor-client relationship. A foreign nation purchases the WF, the assistance, the support for the portability and then proceeds to the integration within the platform.

The business is generated as soon as new companies are involved on and/or spin-off are created, that gives the necessary support for the WF portability.

The above process has to be integrated with the Certification process that still requires the terminal be complying with the requirements of the radio communication standard the waveform performs.

The stakeholders involved in the business model for WF portability in the military domain are:

- The military customer of various nations.
- The WF providers.
- In the middle, as mediator between the defence agency and the industries, we have the European Defence Agency (EDA).

As far as the Public Safety concerning, the stakeholders involved in the business model for WF portability are:

- End users of various nations.
- The WF providers.
- in the middle, as mediator between the end users and the industries, we could have an European body like ETSI.
- RRS terminal and infrastructure manufacturer.

The WF providers offer the WF, but also guarantee the required support for the integration and for the portability of such WFs together with the other stakeholders. In this scenario, a number of Nations could be organized in a consortium to develop the WFs. Of course, this process can rely on certified companies. Once the WF library is developed, it can be sold (distribution phase) then, it should be updated according to the new standards and new services can be offered, like porting and on-site support. This kind of services will be offered by industries or spin-off that can be certified. Furthermore, the portability requires a joint effort between the WF provider and the RRS platform provider, in order to integrate a different WF on a specific platform. This could become an important issue as both the WF provider and the RRS platform provider should share the economical benefits of RRS commercialization.

A business and organizational model can also identify for which domains the WF portability may be applied. There are three different domains where the WF services can be provided, as shown in figure 19. For each domain, the main drivers/benefits and challenges are identified.

| Defence domain | Public Safety domain | Commercial domain |
|---|---|---|
| Interoperability for Joint/Coalition operations | Interoperability of Local/National/Regional levels | Multi-standard handover |
| Many military WF | Large number of WF but still less than the Defence domain | Increasing number of WF |
| Strong security requirements | Strong/Medium security requirements | Low security requirements |
| Long Life Cycle | Long/Medium Life Cycle | Medium/Short Life Cycle |
| Large customer budget | Medium customer budget | Medium/Low customer budget |
| Strong certification process | Strong/Medium certification process | Weak certification process |
| Medium number of users/terminals | Medium number of users/terminals | Very large number of users/terminals |

**Figure 19: Market Constraints and Business Models for RRS/SDR**

A certified Waveform Provider may be able to provide the following essential data and/or services to Industry and end users:

- Ability to be part of a Contractual Arrangement with industry and /or end users in order to provide the relevant data and services.
- Ability to protect the relevant IPRs.

- To maintain and upgrade the waveform software, according to bug fixing or standard/specification evolutions, including its documentation.

- Ability to provide efficient engineering support for porting Waveform software onto the compatible RRS.

- To take into account the National constraint and requirements.

The definition and setting up of such a process and organization could be quite ambittious and difficult to achieve in a single phase. A gradual approach may be needed.

An analysis on the portability of WF and the related model cannot be complete without cost considerations. A software architecture, which supports software portability and the related business/organizational model described in this clause, may have a high cost on the production and deployment of RRS terminals and infrastructure. Even if RRS technology and portability can provide clear benefits, these additional costs may be difficult to accept by Public Safety organizations.

Additionally, an RRS architecture, which provides full software portability, may have also an impact on the power consumption or battery usage of the RRS terminals. Such architecture may not validate the power consumption requirements defined in TR 102 745 [i.29].

### 8.1.5 Lifecycle

The RRS concept moves the lifecycle application from the overall terminal to the waveform. The lifecycle concept for the RRS terminal can be applied only from technological point of view in order to increase processing performances or to manage the obsolescence.

RRS means an overall performance that can be provided with different SW architectures able to perform a minimum level of reconfiguration and SW portability. This latter capability is closely related the application of a specific SW architecture allowing a proper level of hardware abstraction. The adoption of a better candidate of SW architecture as future standard constraints the lifecycle that the future RRS will have on the market. Currently the best known candidate for a SW architecture standard seems the SCA currently under managing by bodies like SDR Forum and OMG. The SCA, as it is or with some adaptations to specific markets seem today a valid solution for a RRS's SW architecture.

## 8.2 Impact to organizational structures and procedures

In time, Public Safety organizations have established consolidated operational procedures based on the experience of resolving many different types of emergency crisis.

One of the main risks in the adoption of a new technology is the impact on the operational procedures, organizations structure and processes. This impact should be minimized otherwise there is the risk of rejection or underutilization of the new technology.

This is especially the case with an innovative technology like Reconfigurable Radio Systems.

RRS technology will be quite complex to design and deploy. Such complexity should be hidden to the Public Safety responders, for a number of reasons:

- Emergency crisis are characterized by very fast reaction times. If the terminal is difficult to operate and it has a low usability, this will negatively impact the operational efficiency.

- Organizational structures and procedures have been defined in Public Safety domain as a result of many years of facing and resolving difficult and dangerous scenarios. There is a strong resistance to change by Public Safety organizations. New technologies like RRS should adapt to the existing organizational structures and procedures. Changes are still possible only when a benefit has been clearly identified (e.g. larger bandwidth).

- While some Public Safety organizations receive a high level of training, some others (e.g. volunteers organizations) may not have the preparation to use, in the proper way, sophisticated technologies.

The conclusion is that a standardization effort for the application of RRS technology to Public Safety domain should include an evaluation on the impact to the Public Safety organizational structures and procedures.

## 8.3 Considerations for evaluation and testing

### 8.3.1 Certification

To fully exploit RRS technology and to ensure that its proper use by Public Safety organizations, regulatory changes will be required that accommodate new models of certification.

The certification cost of a complex technology as RRS can be so high that it can block adoption of this technology.

An additional issue is that regulatory policies and Public Safety procedures are different in each nation of Europe, so there may be more than one certification process in Europe for RRS technology.

The recommendation is that Public safety agencies should begin considering the needed changes for their certification and approval procedures to take advantage of the capabilities of RRS technology.

### 8.3.2 Measurements and testing of wireless interferences

RRS technology and dynamic spectrum management can increase significantly the risk of wireless interference in comparison to the traditional "static" approach of assigning spectrum bands to licensed users.

This is an important area to investigate as wireless interference and the consequent degradation of the Quality of Service (QoS) may not be acceptable by Public Safety organizations.

Wireless interferences may due to a number of causes including:

- A "hidden RRS node" may transmit with a power level, which causes harmful interference.
- The reallocation of spectrum bands during an emergency crisis may not be immediate. The transient phase may cause harmful wireless interference.
- If "spectrum sharing" with the commercial domain is adopted during an emergency crisis, wireless interference may be generated by commercial networks, which have not been shut down.
- Security attacks by criminals, who would like to disrupt the public safety communication systems. This threat is obviously present even in non-RRS networks.

The recommendation is to evaluate the impact of dynamic spectrum management in terms of "interference noise" and parameters of Quality of Service like EVM, BER and PER. The evaluation could be conducted through simulation (see also clause 6.4.4) and measurement campaigns.

Spectrum sensing has an essential role in RRS networks to detect and eventually locate source of wireless interference.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | March 2010 | Publication |
| | | |
| | | |
| | | |
| | | |